Федеральное государственное автономное образовательное учреждение высшего образования
"Национальный исследовательский университет "Высшая школа экономики"

Факультет компьютерных наук
Департамент программной инженерии

Рабочая программа дисциплины
Формальные методы программной инженерии
(на английском языке)

для образовательной программы «Системная и программная инженерия»
направления подготовки 09.04.04 «Программная инженерия»
уровень - магистр

Разработчик программы
Ломазова И.А., д.ф.-м.н., профессор, ilomazova@hse.ru

Одобрена на заседании департамента программной инженерии «___»_____ 2017 г.
Руководитель департамента Авдошин С.М. _____

Утверждена Академическим советом образовательной программы
«___»_____ 2017 г., № протокола_____

Академический руководитель образовательной программы
Александров Д.В. _____

Москва, 2017

1 The field of use and normative references

This syllabus of the “Formal methods in software engineering” course states knowledge and skills prerequisites and determines content and forms of control for the course.

The syllabus is intended for instructors of the course, teaching assistants, and students of the direction 09.04.04 "Software engineering", that take master program “System and software engineering”, specializations “Software development management” and the course "Formal methods in software engineering".

The syllabus is developed in accordance with:

- Educational standard of Federal state autonomous educational institution of higher professional education "National Research University - Higher School of Economics" for the direction 09.04.04 "Software engineering" of master training ;
- Educational program of the direction 09.04.04 "Software engineering" of master training;
- Curriculum of the university for the direction 09.04.04 "Software engineering" of master training, specializations “ Software development management”, approved in 2017.

Abstract

In computer science and software engineering, **formal methods** are a particular kind of mathematically-based techniques for the specification, development and verification of software and hardware systems. The use of formal methods for software and hardware design is motivated by the fact that, as in other engineering disciplines, performing appropriate mathematical analysis can contribute to the reliability and robustness of a design.

Formal methods are best described as the application of a fairly broad variety of theoretical computer science fundamentals, in particular logic calculi, formal languages, automata theory, and program semantics, but also type systems and algebraic data types to problems in software and hardware specification and verification.

Formal methods can:

- Be a foundation for describing complex systems.
- Be a foundation for reasoning about systems.
- Provide support for program development.

In contrast to other system design approaches, formal methods use mathematical proof as a complement to system testing in order to ensure correct behavior. As systems become more complicated, and safety becomes a more important issue, the formal approach to system design offers another level of insurance.

Formal methods differ from other design methods by the use of formal verification schemes, the basic principles of the system must be proven correct before they are accepted. Traditional system design uses extensive testing to verify behavior, but testing is capable of only finite conclusions. E. Dijkstra and others have demonstrated that tests can help to find fails and bugs, but cannot guarantee their absence. In contrast, once a theorem is proven true it remains true.

It is very important to note that formal verification does not obviate the need for testing. Formal verification cannot fix bad assumptions in the design, but it can help identify errors in reasoning which would otherwise be left unverified. In several cases, engineers have reported finding flaws in systems once they reviewed their designs formally.

Roughly speaking, formal design can be seen as a three step process, following the outline given here:

1. Formal Specification: During the formal specification phase, the engineer rigorously defines a system using a modeling language. Modeling languages are special formalisms which allow users to model complex structures out of predefined types. This process of formal specification is similar to the process of converting a word problem into algebraic notation.

In many ways, this step of the formal design process is similar to the formal software engineering technique developed by Rumbaugh, Booch and others. At the minimum, both techniques help engineers to clearly define their problems, goals and solutions. However, formal modeling languages are more rigorously defined. And the clarity that this stage produces is a benefit in itself.

2. Verification: As stated above, formal methods differ from other specification systems by their heavy emphasis on provability and correctness. By building a system using a formal specification, the designer is actually developing a set of theorems about his/her system.

   Verification is a difficult process, largely because even a very simple system usually has several dozen theorems, each of which has to be proven. Even a traditional mathematical proof is a complex affair. Given the demands of complexity, almost all formal systems use an automated theorem proving tool of some form. These tools can prove simple theorems, verify the semantics of theorems, and provide assistance for verifying more complicated proofs.

3. Implementation: Once the model has been specified and verified, it is implemented by converting the specification into code. As the difference between software and hardware design grows narrower, formal methods for developing embedded systems have been developed. LARCH, for example, has a VHDL implementation.

Formal methods offer additional benefits outside of provability, and these benefits do deserve some mention.

- **Discipline**: By virtue of their rigor, formal systems require an engineer to think out his design in a more thorough fashion. In particular, a formal proof of correctness is going to require a rigorous specification of goals, not just operation. This thorough approach can help identify faulty reasoning far earlier than in traditional design.

  The discipline involved in formal specification has proved useful even on already existing systems. Engineers using the PVS system, for example, reported identifying several microcode errors in one of their microprocessor designs.

- **Precision**: Traditionally, disciplines have moved into jargons and formal notation as the weaknesses of natural language descriptions become more glaringly obvious. There is no reason that systems engineering should differ, and there are several formal methods which are used almost exclusively for notation.

For engineers designing safety-critical systems, the benefits of formal methods lie in their clarity. Unlike many other design approaches, the formal verification requires very clearly defined goals and approaches. In a safety critical system, ambiguity can be extremely dangerous, and one of the primary benefits of the formal approach is the elimination of ambiguity.

The purpose of this course is to learn how to specify behavior of systems and to experience the design of a system where you can prove that the behavior is correct. Students will learn how to formally specify requirements and to prove (or disprove) them on the behavior. The behavior of systems will be represented by such formalisms as

- finite state machines;
- process algebras;
- Petri nets;
- temporal logics.

With a practical assignment students will experience how to apply the techniques in practice.

The first part of this course focuses on the study of the semantics of a variety of programming language constructs. We will study structural operational semantics as a way to formalize the intended execution and implementation of languages, axiomatic semantics, useful in developing as well as verifying programs, and denotational semantics, whose deep mathematical underpinnings make it the most versatile of all.

Then the special emphasis will be put on parallel and distributed systems modeling, specification and analysis. We consider two basic approaches to concurrent systems specification and analysis: process algebras and Petri nets.

Process algebra is a mathematical framework in which system behavior is expressed in the form of algebraic terms, enhancing the available techniques for manipulation. Fundamental to process algebra is a parallel operator, to break down systems into their concurrent components. A set of equations is imposed to derive whether two terms are behaviorally equivalent. In this framework, non-trivial properties of systems can be established in an elegant fashion. For example, it may be possible to equate an implementation to the specification of its required input/output relation. In recent years a variety of automated tools have been developed to facilitate the derivation of such properties.

Applications of process algebra exist in diverse fields such as safety critical systems, network protocols, and biology. In the educational vein, process algebra has been recognized to teach skills to deal with complex concurrent systems, by representing and reasoning about such systems in a mathematically clear and precise manner.

Petri nets is another popular formalism for modeling, analyzing and verifying reactive and distributed systems. Their strength are their simple but precise semantics, their clear graphical notation, and many methods and algorithms for analysis and verification.

The course introduces Petri nets and their theory by the help of examples from different application domains. The focus, however, will be on traditional Petri net theory, in particular on Place/Transition-Systems and on concepts such as place and transition invariants, deadlocks and traps, and the coverability tree. The course also covers different versions and variants of Petri nets as well as different modeling and analysis techniques for particular application areas. Thus we consider an urgent topic of modeling and analysis of workflow processes in more details.

The forth module covers a prominent verification technique that has emerged in the last thirty years – model checking. This approach is based on systematical check whether a model of a given system satisfies a property such as deadlock freedom, invariants, or request-response. This automated technique for verification and debugging has developed into a mature and widely-used industrial approach with many applications in software and hardware. It is used (and further developed) by companies and institutes such as IBM, Intel, NASA, Cadence, Microsoft, and Siemens, to mention a few, and has culminated in a series of mostly freely downloadable software tools that allow the automated verification of, for instance, C#-programs or combinational hardware circuits.

Subtle errors, for instance, due to multi-threading that remained undiscovered using simulation or peer reviewing can potentially be revealed using model checking. Model checking is thus an effective technique to expose potential design errors and improve software and hardware reliability.

This course provides an introduction to the theory of model checking and its theoretical complexity. We introduce transition systems, safety, liveness and fairness properties, as well as omega-regular automata. We then cover the temporal logics LTL, CTL and CTL*, compare them, and treat their model-checking algorithms. Techniques to combat the state-space explosion problem are at the heart of the success of model checking.

We will show that model checking is based on well-known paradigms from automata theory, graph algorithms, logic, and data structures. Its complexity is analyzed using standard techniques from complexity theory.

2 Course Objective

The objective of the Formal methods in software engineering course delivery is to train students to treat the specification of software as a very important stage of software development, and also to appreciate the advantages and problems associated with this approach for future projects.

One of the important aspects of formal methods is that, even for quite simple problems, they force the students to think very carefully about the specification, and not to get involved in the coding

too quickly. Even for students who have done a lot of programming before the ideas behind formal methods are likely to be completely new, and can draw their attention to problems of program correctness and reliability.

Another very important reason for teaching formal methods is that they are gradually being used in more industrial projects, and thus students should be familiar with at least the ideas associated with the approach, even if they have not learnt the specific formal specification language that their particular industry may require.

3 Training Objectives

During the course, the students will:

- Study the basic principles of using formal methods for specification and analysis of software systems;
- Study basic notions and modes of formal semantics for sequential and concurrent programs.
- Study formalism, such as process algebras and Petri nets, and methods for modeling and analysis of concurrent and distributed systems.
- Study methods and algorithms for model checking of concurrent systems;
- Master methods and tools of software specification, analysis and verification;
- Acquire practical skills in design, specification and analysis of model distributed systems examples.

Upon completion of this course, students should be able to:

- understand the language of studied formalisms;
- model various classes of systems using these formalisms;
- apply specific analytical techniques;
- prove properties of discrete systems using process algebras, Petri nets and appropriate specification formalisms.

4 The position of the course in the structure of the educational program

The course is given to the students of the Master Program “System and Software Engineering”, Faculty of Computer Science, the National Research University - Higher School of Economics/HSE.

It is a part of general scientific curricula unit, and it is delivered in modules 1-4 of the first academic year. The course length is 128 academic hours of audience classes divided into 48 lecture hours and 80 seminar hours and 252 academic hours for students’ self-study.

The covered number of credits is 10. Academic control forms are one home assignment, one written exam after module 2, and one written exam after module 4.

Prerequisites of the course:

- Informatics, mathematical logics, and theory of computation
- Discrete mathematics
- Software programming

The main notions and concepts of the course are to be utilized in the courses on software system development.

5 Topic-Wise Curricula Plan

№	Topic name	Course hours, total	Audience hours		Self-study
			Lectures	Practical studies	
	Module 1 (80 hrs.)				
1.	Formal methods as a basis for software reliability.	8	2	2	4
2.	Floyd method for verification of sequential programs. Hoare axiomatic semantics for sequential and parallel programs.	32	4	8	20
3.	Finite state machines (FSMs): basic definitions, operational semantics. Categories of FSMs. Extended FSMs. Modeling concurrent systems with communicating FSMs.	22	2	4	16
4.	Petri nets: basic notions, definitions and classification. Modeling distributed systems with Petri nets.	30	4	6	20
	Module 1, totally:	92	12	20	60
	Module 2 (80 hrs.)				
5.	Petri nets analysis. Checking structural and behavioral properties.	24	4	6	14
6.	High-level Petri nets. Colored Petri nets and CPN-Tools.	22	2	4	16
7.	Modeling distributed and concurrent system with process algebras. Structured operational semantics and its formalization (SOS). Algebra CCS: syntax, semantics, modeling technique.	30	4	6	20
8.	The notion and properties of bisimilarity relation.	16	2	4	10
	Module 2, totally:	92	12	20	60
	Module 3 (100 hrs.)				
9.	Verifying reactive concurrent systems with CCS. Hennesy-Milner logic and temporal properties. The notion of fixed point and Tarski’s fixed point theorem.	20	4	4	12
10.	Transition systems and program graphs. Nondeterminism, parallelism and communication. Peterson algorithm.	16	4	2	10
11.	Specifying distributed systems with Promela. Spin model checker.	30	2	8	20
12.	Temporal logics LTL and CTL for specification of behavioral properties of reactive systems.	26	4	4	18
	Module 3, totally:	92	14	18	60
	Module 4 (100 hrs.)				
13.	Automata-based approach for verification of LTL formulae.	74	6	16	52
14.	Model checking algorithm for verification of CTL formulae.	30	4	6	20
	Module 4, totally:	104	10	22	72
	TOTAL:	380	48	80	252

6 Education control forms

Type of control	Control form	1 year				Settings **
		1	2	3	4	
Interme-diate	Exam		*			Written test; 80 minutes
Mid-term (week)	Home as-signment				*	Written report; two weeks; minimal size of a report is 5 pages.
Total	Exam				*	5 days for an assessment

6.1 Knowledge and skills evaluation criteria

Exam, intermediate control (module 2):

A computer-based testing assessment on the topics covered in the first term.
Students should demonstrate:

- understanding of the basic formalisms and notions learnt in first two modules (communicating finite automata, Petri nets, coloured Petri nets, process algebra CCS);
- skills of modeling and analysis (reachability graph, coverability graph, S- and T- invariants, traps, siphons, strong/weak bisimulation, etc.) of distributed and parallel systems with the studied formalisms and algorithms.

Home assignment (module 4):

The home task deals with constructing a formal model and verifying it. Given a concrete distributed system (a communication protocol, a system of interacting agents, a resource producing/consuming system etc.) students should complete the following tasks:

- Develop a Petri net model of a given distributed system.
- Describe basic behavioral properties of the constructed model.
- Classify the behavioral properties and chose appropriate methods and/or tools for specifying and verifying these properties.
- Verify the behavior of the constructed system.

Students should demonstrate:

- skills of modeling complex distributed systems in PROMELA modeling language;
- skills of using SPIN verification system to debug and conduct model checking of models constructed in PROMELA;
- ability to argument the suggested solution;
- ability to analyze advantages and disadvantages of the proposed solution;
- ability to propose further improvements of the solution;
- ability to find alternative solutions of the given assignment.

Evaluation criteria:

- correctness of the suggested solution;
- completeness of the solution (whether all of the possible problems concerning correctness and performance are taken into account);
- analysis of the suggested solution (recognition of shortages and benefits of the suggested solution; diagnosis of the solution performance bottlenecks, or explanation, why the solution is free of them);
- argumentation of the suggested solution correctness;
- suggested alternative solutions and comparison of them with the submitted solution;

- accuracy of the submitted report.

When submitting an assignment, students are expected to answer questions in class to demonstrate understanding of the content of the assignment and course material, to present and explain their own solutions, to answer questions. If a student is not able to answer or argue the question, then the grade may be reduced. After an assignment is graded, the topic is discussed in class. The assignment explanation takes about 15 minutes of the class time.

Exam, final control (module 4):
A computer-based testing assessment on the topics covered in the course.

An official means of communicating with students is e-mail. Students can ask their questions about assignments and theoretical issues in classrooms, as well as by e-mail.

6.2 Grading system

The evaluation is based on a ten-point scale.

Student class work is evaluated via quick tests and assignments given in the classroom. Each assignment is weighted in points. The amount of assignment points depends on the assignment complexity. The points of an assignment are given in the assignment description. Some of assignments are expected to be solved and submitted at the seminar on the day of their distribution. If such an assignment was not submitted on the day of its issue, but was submitted till the next seminar it is accepted with the coefficient 0.75 and considered as self-study. Other assignment must be submitted till the seminar next to the seminar of distribution.

%%%%%These assignments form grade $O_{\text{ауд+сам i}}$, where i – is a number of the current module.

Evaluation criteria:

- completeness of the solution (if all of the potential problems with correctness and performance are taken into account);
- analysis of the suggested solution (recognition of shortages and benefits of the suggested solution; diagnosis of the solution performance bottlenecks, or explanation, why the solution is free of them);
- argumentation of the suggested solution correctness;

In addition an instructor evaluate proactive attitude of students in a class:

- proactive attitude of a student in solving offered assignments:
  - suggesting alternative solutions and comparison of them with the submitted solution;
  - demonstrating erudition in the field of study (in-depth knowledge beyond the bounds of the course).
  - demonstrating erudition in adjacent fields of knowledge;
- ability to find defects in the submitted solution;
- be fluent in applying learned methods and algorithms.

Grades for practical and self-study work are written down in a worksheet. Cumulative grade for practical work or self-study is calculated at the end of each module before intermediate or final control.

The result grade after the 1st term is calculated by the formula:

$$O_{\text{term 1}} = 0{,}5\ O_{\text{accum1}} + 0{,}5\ O_{\text{exam1}}$$

where O_{accum1} is the accumulated grade composed of grades for the current work (quick tests, assignments, work in the classroom) during modules 1 and 2; O_{exam1} is the grade for the intermediate exam. Rounding is done by "round half up" rule.

The final course grade is calculated by the formulas:

$$O_{accum\ 2} = 0{,}5\ O_{current2} + 0{,}3\ O_{h\_task} + 0{,}2\ O_{term1}$$
$$O_{final} = 0{,}6\ O_{accum2} + 0{,}4\ O_{exam2}$$

where $O_{current2}$ is the grade for the current work (quick tests, assignments, work in the classroom) during modules 1 and 2; O_{h_task} is the grade for the home task, O_{term1} is the result grade after the 1st term, and O_{exam2} is the grade for the exam after module 4. Rounding is done by "round half up" rule.

7 Detailed course content

Topic 1: Formal methods as a basis for software reliability.

- *Topic outline:*
  - Why formal methods.
  - Formal methods and software/hardware reliability.
  - Formal methods: historical overview.
  - How logic helps computer scientists.
  - Formal methods vs. simulation and testing.
  - Course overview.
- *Main references/books/reading:*
  1. D. Peled: Software Reliability Methods, Springer-Verlag 2001. (pp. 1-11)
  2. Карпов Ю.Г. MODEL CHECKING. Верификация параллельных и распределенных программ и систем. СПб.: БХВ-Петербург, 2010. – 560 с. (pp. 1-42)
  3. Jonathan P., Bowen and Mike Hinchey "Ten Commandments of Formal Methods ... Ten Years Later", IEEE Computer, 39(1):40-48, January 2006.
- *Additional references/books/reading:*
  1. Грис Д. Наука программирования. – М.: Мир, 1984. – 416 с.
  2. Formal methods. In: Wikipedia, http://en.wikipedia.org/wiki/Formal_methods
  3. Michael R. A. Huth, Mark D. Ryan. *Logic in Computer Science – modelling and reasoning about systems.* – Cambridge University Press, 2004, 427 pages.
  4. J. Rutten, M. Kwiatkowska, G. Norman and D. Parker: Mathematical Techniques for Analyzing Concurrent and Probabilistic Systems, Volume 23 of CRM Monograph Series. American Mathematical Society, P. Panangaden and F. van Breugel (eds.), March 2004.

  Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

Topic 2. Floyd method for verification of sequential programs. Hoare axiomatic semantics for sequential and parallel programs.

- *Topic outline:*
  - Partial and total correctness assertions.

- Floyd method for proving partial program correctness. The notion of invariant.
- The axiomatic approach for proving program correctness
- Hoare's assertion language: syntax and semantics.
- Partial correctness properties.
- Hoare's logic. Soundness and relative completeness of Hoare's logic.
- Weakest preconditions and their properties.
- Proving total program correctness. Soundness and relative completeness of total correctness.
- Equivalence of axiomatic and denotational/operational semantics.
- Hoare's logic for parallel programs. Semantics of parallel constructions. Rules for partial correctness assertions.

♦ *Main references/books/reading:*

1. Nielson H. R. and Nielson F. Semantics with Applications: An Appetizer. Springer-Verlag, 2007- 274 p.
2. Грис Д. Наука программирования. – М.: Мир, 1984. – 416 с.

♦ *Additional references/books/reading:*

1. Rajeev Alur, Tom Henzinger. Invariant verification. Chapter II in manuscript "Computer-aided verification". http://mtc.epfl.ch/courses/CAV2006/Notes/2.pdf
2. Matthew Parkinson. Course materials *Software Verification* (University of Cambridge). http://www.cl.cam.ac.uk/teaching/0910/L19/

Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

Topic 3. Finite state machines (FSMs): basic definitions, operational semantics. Categories of FSMs. Extended FSMs. Modeling concurrent systems with communicating FSMs.

♦ *Topic outline:*

- Finite state machines (FSMs): informal introduction, formal definitions, case study.
- State transition diagrams.
- Deterministic and nondeterministic FSMs.
- Extended FSMs.
- Communicating mechanisms for concurrent systems. Specifying distributed systems with interacting automata.
- Proving protocol correctness with communicating FSMs.

♦ *Main references/books/reading:*

1. Hopcroft, John E.; Motwani, Rajeev; Ullman, Jeffrey D. (2006). Introduction to Automata Theory, Languages, and Computation (3rd ed.). Addison-Wesley. ISBN 81-7808-347-7. (In russian: Хопкрофт Дж., Мотвани Р., Ульман Дж. Введение в теорию автоматов, языков и вычислений: Пер. с англ. - М.: Издательский дом "Вильямс", 2008. 528 с. (pp. 1-101, a lot of material can be omitted, as if a student is familiar with it).
2. Карпов Ю.Г. Теория автоматов. – СПб., Питер, 2003. – 208 с. (pp. 95-146).
3. Book chapter: "Calculi and Automata for Modelling Untimed and Timed Concurrent Systems" (pp. 233-254) from the book by Howard Bowman and Rodolfo Gomez, "Concurrency Theory",

2006. DOI 10.1007/1-84628-336-1, ISBN 978-1-85233-895-4 (Print) 978-1-84628-336-9 (Online) (available through HSE digital library).

- *Additional references/books/reading:*

1. Yuri Gurevich, *Sequential Abstract State Machines Capture Sequential Algorithms*, ACM Transactions on Computational Logic, vl. 1, no. 1 (July 2000), pages 77–111. http://research.microsoft.com/~gurevich/Opera/141.pdf
2. Дехтярь М.И. Лекции по дискретной математике. / М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2007.
3. Boerger E., Staerk R. Abstract state machines. A method for high-level system design and analysis. - Springer, 2003. 448 p.
4. Wagner, F., "Modeling Software with Finite State Machines: A Practical Approach", Auerbach Publications. - CRC Press, 2006. 302 p.

Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

Topic 4. Petri nets: basic notions, definitions and classification. Modeling distributed systems with Petri nets.

- *Topic outline:*
  - Motivation and informal introduction. Net formalisms for modeling distributed systems. Examples from different areas.
  - Place/Transition systems: basic concepts. Places, transition, linear algebraic representation.
  - Firing rule, interleaving semantics, occurrence graph, unboundedness.
  - Variants of Petri nets: condition/event systems, contact-free nets, high-level Petri nets, colored Petri nets, nested Petri nets.
  - Modeling basic control constructs with Petri nets: sequencing, nondeterministic choice, concurrency.
  - Modeling causality relations and resource dependencies with Petri nets.
- *Main references/books/reading:*

1. Wolfgang Reisig, Understanding Petri Nets. Modeling Techniques, Analysis Methods, Case Studies, 2013, 230 p. ISBN 978-3-642-33278-4.
2. Ломазова И.А. Сети Петри и анализ поведенческих свойств распределенных систем. – Ярославль: ЯрГУ, 2002. 164 с.
3. Petri Nets: Properties, Analysis and Applications, by Tadao Murata, in: Proceedings of the IEEE, vol. 77, no. 4, April 1989. (pp. 541-580)
4. Carl Adam Petri and Wolfgang Reisig. Petri net. *Scholarpedia*, 3(4):6477 (2008). http://www.scholarpedia.org/article/Petri_net

- *Additional references/books/reading:*

1. В.Е.Котов. Сети Петри. М.: Наука, 1984.
2. C. Girault, R. Valk. Petri Nets for Systems Engineering: A Guide to Modeling, Verification, and Applications. Springer-Verlag, 2002.
3. Jensen K. and Kristensen L. M. Coloured Petri Nets Modelling and Validation of Concurrent Systems, Springer-Verlag, 2009.

4. Вирбицкайте И.Б. Сети Петри: модификации и расширения. Новосибирск: Изд-во НГУ, 2005, 123 с.
5. Ломазова И.А. Вложенные сети Петри: моделирование и анализ распределенных систем с объектной структурой. – М.: Научный мир, 2004. 208 с.
6. Питерсон Дж. Теория сетей Петри и моделирование систем. М.: Мир, 1984.
7. The Petri Nets World http://www.informatik.uni-hamburg.de/TGI/PetriNets/
8. Wolfgang Reisig. Petrinetze. Modellierungstechnik, Analysemethoden, Fallstudien. Vieweg+Teubner, 2010.

Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

Topic 5. Petri nets analysis. Checking structural and behavioral properties.

- *Topic outline:*
  - Interleaving and concurrent semantics for Petri nets. Sequential and concurrent runs.
  - Coverability tree.
  - Propositional state properties of P/T nets: incidence matrix, state equation, place invariants.
  - Positive place invariants and boundedness; transition invariants and deadlocks; siphons and traps.
  - Analysis of behavioral problems for Petri Nets: Safeness; Boundedness; Conservation; Liveness; Reachability and coverability.
  - Analysis techniques for State Machines, Marked Graphs, Extended Free Choice Nets.
- *Main references/books/reading:*

1. Wolfgang Reisig, Understanding Petri Nets. Modeling Techniques, Analysis Methods, Case Studies, 2013, 230 p. ISBN 978-3-642-33278-4.
2. C. Girault, R. Valk. Petri Nets for Systems Engineering: A Guide to Modeling, Verification, and Applications. Springer-Verlag, 2002.
3. Ломазова И.А. Сети Петри и анализ поведенческих свойств распределенных систем. – Ярославль: ЯрГУ, 2002. 164 с.
4. Jörg Desel, Wolfgang Reisig, Grzegorz Rozenberg (Eds.) Lectures on Concurrency and Petri Nets, Advances in Petri Nets, Lecture Notes in Computer Science, vol. 3098, Springer-Verlag, 2004.

- *Additional references/books/reading:*

5. Jensen K. and Kristensen L. M. Coloured Petri Nets Modelling and Validation of Concurrent Systems, Springer-Verlag, 2009.
1. Ломазова И.А. Вложенные сети Петри: моделирование и анализ распределенных систем с объектной структурой. – М.: Научный мир, 2004. 208 с.
2. Вирбицкайте И.Б. Сети Петри: модификации и расширения. Новосибирск: Изд-во НГУ, 2005, 123 с.
6. В.Е.Котов. Сети Петри. М.: Наука, 1984.
3. Питерсон Дж. Теория сетей Петри и моделирование систем. М.: Мир, 1984.
4. The Petri Nets World http://www.informatik.uni-hamburg.de/TGI/PetriNets/

5. Wolfgang Reisig. Petrinetze. Modellierungstechnik, Analysemethoden, Fallstudien. Vieweg+Teubner, 2010.

Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

Topic 6. High-level Petri nets. Colored Petri nets and CPNTools.

- *Topic outline:*
  - Expressibility of Petri nets. Extending Petri nets with reset and inhibitor arcs.
  - Introducing colored tokens and types.
  - Hierarchical modeling.
  - Modeling multi-agent systems with nested Petri nets.
  - Modeling case studies: producer/consumer system, sequential and parallel buffers, crosstalk algorithm, mutual exclusion, dining philosophers.
- *Main references/books/reading:*
  1. C. Girault, R. Valk. Petri Nets for Systems Engineering: A Guide to Modeling, Verification, and Applications. Springer-Verlag, 2002.
  2. Jensen K. and Kristensen L. M. Coloured Petri Nets Modelling and Validation of Concurrent Systems, Springer-Verlag, 2009.
  3. Reisig, Wolfgang. Elements of distributed algorithms :modeling and analysis with Petri Nets. Berlin : Springer, 1998.
  4. Ломазова И.А. Сети Петри и анализ поведенческих свойств распределенных систем. – Ярославль: ЯрГУ, 2002. 164 с.
- *Additional references/books/reading:*
  1. Вирбицкайте И.Б. Сети Петри: модификации и расширения. Новосибирск: Изд-во НГУ, 2005, 123 с.
  2. В.Е.Котов. Сети Петри. М.: Наука, 1984.
  3. Ломазова И.А. Вложенные сети Петри: моделирование и анализ распределенных систем с объектной структурой. – М.: Научный мир, 2004. 208 с.
  4. Питерсон Дж. Теория сетей Петри и моделирование систем. М.: Мир, 1984.
  5. The Petri Nets World http://www.informatik.uni-hamburg.de/TGI/PetriNets/
  6. Wolfgang Reisig. Petrinetze. Modellierungstechnik, Analysemethoden, Fallstudien. Vieweg+Teubner, 2010.

Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

Topic 7. Modeling distributed and concurrent system with process algebras. Algebra CCS: syntax, semantics, modeling technique.

- *Topic outline:*
  - Reactive systems: main notions and examples.
  - Flow diagrams of distributed systems. Ports and interactions.
  - Interleaving semantics of concurrent systems. Labeled transition systems. Concurrency and nondeterminism.

- The Calculus of Communicating Systems (CCS) of R.Milner informally.
- Formal definition of CCS; semantics of CCS; transition diagrams; examples.
- CCS case studies.

♦ *Main references/books/reading:*

1. R.A. Milner. Calculus of communicating systems. Lecture Notes in Computer Science, v.92, Springer, 1980. (pp. 65-84)
2. Fokkink Wan. Introduction to Process Algebra. – Springer-Verlag, 2007. – 169 p.
3. Roscoe, A. W. The Theory and Practice of Concurrency. Prentice Hall, 1997. – 605 p. http://web.comlab.ox.ac.uk/oucl/work/bill.roscoe/publications/68b.pdf

♦ *Additional references/books/reading:*

1. Fokkink W. Modelling distributed systems (Texts in Theoretical Computer Science. An EATCS Series), Springer-Verlag New York, Inc., Secaucus, NJ, 2007. 156 pp.
2. Хоар А.Ч. Взаимодействующие последовательные процессы. М.: Мир, 1989.
3. Glenn Brunes. Distributed system analysis with CCS. Prentice Hall Europe, 1997. – 168 p.
4. Glynn Winskel, Mogens Nielsen. Models for Concurrency. http://www.daimi.au.dk/PB/463/PB-463.pdf

Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

Topic 8. The notion and properties of bisimilarity relation.

♦ *Topic outline:*

- Trace equivalence; strong bisimilarity; bisimulation games; properties of strong bisimilarity.
- Weak bisimilarity; weak bisimulation games; properties of weak bisimilarity; example (a tiny communication protocol).
- Analysis of CCS behavior; examples.
- Value passing CCS.
- The language of Communicating Sequential Processes (CSP): brief overwiew.

♦ *Main references/books/reading:*

1. R.A. Milner. Calculus of communicating systems. Lecture Notes in Computer Science, v.92, Springer, 1980. (pp. 98-111)
2. Glenn Brunes. Distributed system analysis with CCS. Prentice HallEurope, 1997. – 168 p.

♦ *Additional references/books/reading:*

1. Fokkink Wan. Introduction to Process Algebra. – Springer-Verlag, 2007. – 169 p.
2. Fokkink W. Modelling distributed systems (Texts in Theoretical Computer Science. An EATCS Series), Springer-Verlag New York, Inc., Secaucus, NJ, 2007. 156 pp.
3. Хоар А.Ч. Взаимодействующие последовательные процессы. М.: Мир, 1989.
4. Roscoe, A. W. The Theory and Practice of Concurrency. Prentice Hall, 1997. – 605 p. http://web.comlab.ox.ac.uk/oucl/work/bill.roscoe/publications/68b.pdf

Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

Topic 9. Verifying reactive concurrent systems with CCS. Hennesy-Milner logic and temporal properties. The notion of fixed point and its and Tarski's fixed point theorem.

- *Topic outline:*
  - Syntax of Hennessy-Milner logic; semantics of Hennessy-Miler logic; examples.
  - Correspondence between strong bisimilarity and Hennessy-Milner logic.
  - Strong bisimulation as a greatest fixed point
  - Game semantics and temporal properties of reactive systems
- *Main references/books/reading:*
  1. Glenn Brunes. Distributed system analysis with CCS. Prentice HallEurope, 1997. – 168 p.
- *Additional references/books/reading:*
  5. Roscoe, A. W. The Theory and Practice of Concurrency. Prentice Hall, 1997. – 605 p. http://web.comlab.ox.ac.uk/oucl/work/bill.roscoe/publications/68b.pdf

Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

Topic 10. Transition systems and program graphs. Nondeterminism, parallelism and communication. Peterson algorithm.

- *Topic outline:*
  - Transition systems. Meanings of nondeterminism in transition systems.
  - Transition systems and program graphs for sequential and parallel programs. Transition system semantics of a program graph.
  - Guarded Command Language.
  - Parallelism and communication. Interleaving for a transition system, and for a program graph.
  - Mutual exclusion with semaphore.
  - Peterson algorithm.
- *Main references/books/reading:*
  1. Карпов Ю.Г. MODEL CHECKING. Верификация параллельных и распределенных программ и систем. – СПб.: БХВ-Петербург, 2010. – 560 с.
  2. J.-P. Katoen, C. Baier : Principles of model checking (Chap.2, 19-87). ISBN:026202649X 9780262026499, The MIT Press, 2008.
- *Additional references/books/reading:*
  1. Schneider K. Verification of Reactive Systems. – Springer-Verlag, 2004. – 216 p.
  2. Кларк Э.М., Грамберг О., Пелед Д. Верификация моделей программ: Model Checking. – М.: МЦНМО, 2002. – 416 с.

Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

Topic 11. Specifying distributed systems with Promela. Spin model checker.

- *Topic outline:*

- Sequential Programming in PROMELA specification language: data types, operators and expressions, control statements.
- Verification of sequential programs, assertions, guided simulation.
- Interactive simulation of concurrent programs.
- Synchronization and nondeterminism in concurrent programs.
- Deadlock verification.
- Verification with temporal logic LTL.
- Expressing and verifying safety properties.
- Expressing and verifying liveness properties.
- Case studies.

♦ *Main references/books/reading:*

1. Ben-Ari M. Principles of the Spin Model Checker. – Springer-Verlag, 2008. – 216 p.

♦ *Additional references/books/reading:*

1. Карпов Ю.Г. MODEL CHECKING. Верификация параллельных и распределенных программ и систем. – СПб.: БХВ-Петербург, 2010. – 560 с.
2. Schneider K. Verification of Reactive Systems. – Springer-Verlag, 2004. – 216 p.
3. Кларк Э.М., Грамберг О., Пелед Д. Верификация моделей программ: Model Checking. – М.: МЦНМО, 2002. – 416 с.
4. Кузьмин Е.В. Верификация моделей программ. – Ярославль: ЯрГУ, 2008. – 76 с.

Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

Topic 12. Temporal logics LTL and CTL.

♦ *Topic outline:*

- Model and temporal logics: main consepts.
- Linear Temporal Logic LTL: syntax, semantics, main properties and case studies.
- Linear time properties: safety, liveness, decomposition.
- Fairness: unconditional, strong and weak fairness.
- Computational Tree Logic CTL: syntax, semantics, equational laws.
- Comparing LTL and CTL.

♦ *Main references/books/reading:*

3. Карпов Ю.Г. MODEL CHECKING. Верификация параллельных и распределенных программ и систем. – СПб.: БХВ-Петербург, 2010. – 560 с.
4. Manna Z., Pnueli A. The temporal logic of reactive and concurrent systems. – Springer-Verlag, 1991. 427 p.

♦ *Additional references/books/reading:*

3. Schneider K. Verification of Reactive Systems. – Springer-Verlag, 2004. – 216 p.

4. Кларк Э.М., Грамберг О., Пелед Д. Верификация моделей программ: Model Checking. – М.: МЦНМО, 2002. – 416 с.
5. Кузьмин Е.В. Верификация моделей программ. – Ярославль: ЯрГУ, 2008. – 76 с.

Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

Topic 13. Automata-based approach for verification of LTL formulae.

- *Topic outline:*
  - Automata on finite words.
  - Verifying regular safety properties. Product construction, counterexamples.
  - Automata on infinite words. Generalized Büchi automata, ω-regular languages.
  - Verifying ω-regular properties: nested depth first search.
- *Main references/books/reading:*
  1. Карпов Ю.Г. MODEL CHECKING. Верификация параллельных и распределенных программ и систем. – СПб.: БХВ-Петербург, 2010. – 560 с.
  2. Schneider K. Verification of Reactive Systems. – Springer-Verlag, 2004. – 216 p.
- *Additional references/books/reading:*
  1. Кларк Э.М., Грамберг О., Пелед Д. Верификация моделей программ: Model Checking. – М.: МЦНМО, 2002. – 416 с.
  2. Кузьмин Е.В. Верификация моделей программ. – Ярославль: ЯрГУ, 2008. – 76 с.

Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

Topic 14. Model checking algorithm for verification of CTL formulae.

- *Topic outline:*
  - Kripke structures.
  - Semantics of CTL on computational trees.
  - CTL model checking: recursive descent, backward reachability, complexity.
  - Fairness, counterexamples/witnesses.
  - CTL^{+} and CTL* .
  - Fair CTL semantics, model checking.
- *Main references/books/reading:*
  1. Карпов Ю.Г. MODEL CHECKING. Верификация параллельных и распределенных программ и систем. – СПб.: БХВ-Петербург, 2010. – 560 с.
  2. Schneider K. Verification of Reactive Systems. – Springer-Verlag, 2004. – 216 p.
- *Additional references/books/reading:*
  1. Кларк Э.М., Грамберг О., Пелед Д. Верификация моделей программ: Model Checking. – М.: МЦНМО, 2002. – 416 с.
  2. Кузьмин Е.В. Верификация моделей программ. – Ярославль: ЯрГУ, 2008. – 76 с.

Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

Practical study: solving problems, using software tools for modeling and analysis of parallel and distributed systems.

8 Educational technologies

Used educational technologies:

- case study;
- problem solving;
- software for learning support (computer simulation);
- delivery of classes by world-class experts in the field from Dutch university-partner (Eindhoven University of Technology) is planned.

8.1 Methodological recommendations to teachers

Used software:

- CWB: The Edinburgh Concurrency Workbench (http://homepages.inf.ed.ac.uk/perdita/cwb/)
- CPNTools (http://cpntools.org/)
- SPIN (http://spinroot.com)

9 Tools for mid-term, intermediate and final assessment

9.1 Assignment topics for various education control forms.

The final exam is based on the course topics:

- Operational, denotational and axiomatic semantics of sequential program
- The least fixpoint semantics of loop statement
- Verification of sequential programs with partial and total correctness assertions.
- Interleaving semantics of concurrent programs.
- Labeled transition systems.
- Formal models of concurrent and distributed systems.
- Theory of process algebras.
- Branching time semantics of concurrent processes.
- Trace and bisimulation equivalence of concurrent programs. Strong and weak bisimulation.
- Hennessy-Milner logic for process algebra CCS.
- Process algebra CSP.
- Petri net theory.
- Interleaving and concurrent semantics for Petri nets.
- Structural properties of Petri nets.
- Classification of Petri nets.
- Expressibility of Petri nets.
- Proving Petri nets properties with reachability and coverability trees.
- Temporal logics for specification of concurrent systems behavior.
- Syntax, semantics and equational laws of Linear Temporal Logic LTL.
- Syntax, semantics and equational laws of Computational Tree Logic CTL.

- Comparing LTL and CTL expressibility.
- Automata on infinite words and ω-regular languages.
- Model checking of LTL and CTL formulae.

10 Courseware.

10.1 Study guides.

There is no study guide textbook for the course.

10.2 Main reading:

1. Wolfgang Reisig, Understanding Petri Nets. Modeling Techniques, Analysis Methods, Case Studies. 2013. ISBN 978-3-642-33278-4. (Available through HSE library).
2. Jensen K. and Kristensen L. M. Coloured Petri Nets Modelling and Validation of Concurrent Systems. Springer-Verlag, 2009. (Available through HSE library)
3. Ben-Ari M. Principles of the Spin Model Checker. Springer-Verlag, 2008. (Available through HSE library).
4. J. C. M. Baeten, T. Basten and M. A. Reniers: Process Algebra: Equational Theories of Communicating Processes. Cambridge Tracts in Theoretical Computer Science, Vol. 30. Cambridge University Press, 2010
5. Michael Fisher. An Introduction to Practical Formal Methods Using Temporal Logic. Wiley publisher, 2011. SBN-10: 0470027886 | ISBN-13: 978-0470027882
6. R.A. Milner. Calculus of communicating systems. Lecture Notes in Computer Science, v.92. Springer, 1980.
7. Карпов Ю.Г. MODEL CHECKING. Верификация параллельных и распределенных программ и систем. СПб.: БХВ-Петербург, 2010.
8. Rajeev Alur, Tom Henzinger. Invariant verification. Chapter II in manuscript “Computer-aided verification”. http://mtc.epfl.ch/courses/CAV2006/Notes/2.pdf (электронная версия)

10.3 Additional reading:

1. Ломазова И.А. Сети Петри и анализ поведенческих свойств распределенных систем. Ярославль: ЯрГУ, 2002.
2. Хопкрофт Дж., Мотвани Р., Ульман Дж. Введение в теорию автоматов, языков и вычислений: Пер. с англ. М.: Издательский дом "Вильямс", 2008.
3. Nielson H. R. and Nielson F. Semantics with Applications: An Appetizer. Springer-Verlag, 2007.
4. Schneider K. Verification of Reactive Systems. Springer-Verlag, 2004.
5. Girault C., R. Valk. Petri Nets for Systems Engineering: A Guide to Modeling, Verification, and Applications. Springer-Verlag, 2002.
6. Peled D. Software Reliability Methods. Springer-Verlag, 2001.
7. Грис Д. Наука программирования. М.: Мир, 1984.
8. Huth Michael R. A., Ryan Mark D.. *Logic in Computer Science – modelling and reasoning about systems*. Cambridge University Press, 2004.
9. Singh A. Elements of Computation Theory. Springer-Verlag, 2009.
10. Glynn Winskel. The Formal Semantics of Programming Languages: An Introduction. MIT Pres, 1993.
11. Fokkink W. Modelling distributed systems (Texts in Theoretical Computer Science. An EATCS Series). Springer-Verlag New York, Inc., Secaucus, NJ, 2007.
12. Roscoe, A. W. The Theory and Practice of Concurrency. Prentice Hall, 1997. http://web.comlab.ox.ac.uk/oucl/work/bill.roscoe/publications/68b.pdf
13. Glenn Brunes. Dystributed system analysis with CCS. Prentice HallEurope, 1997.

14. C. Girault, R. Valk. Petri Nets for Systems Engineering: A Guide to Modeling, Verification, and Applications. Springer-Verlag, 2002.
15. ван дер Аалст В., ван Хей К. Управление потоками работ: модели, методы и системы. М.: Физматлит, 2007.

Internet References:

1. Marcelo Fiore. Course materials *Denotational Semantics* (University of Cambridge). http://www.cl.cam.ac.uk/teaching/0910/DenotSem/
2. Wolfgang Schreiner. Course materials *Formal Semantics of Programming Languages* (RICS) http://moodle.risc.uni-linz.ac.at/course/view.php?id=30
3. Matthew Parkinson. Course materials *Software Verification* (University of Cambridge). http://www.cl.cam.ac.uk/teaching/0910/L19/
4. Carl Adam Petri and Wolfgang Reisig. Petri net. *Scholarpedia*, 3(4):6477 (2008). http://www.scholarpedia.org/article/Petri_net

10.4 References, dictionaries and encyclopedias

Recommended sources:

- Wikipedia (http://en.wikipedia.org; http://ru.wikipedia.org)
- Formal Methods Wiki (http://formalmethods.wikia.com/wiki/Formal_methods)
- Formal Methods Europe (http://www.fmeurope.org/)
- Formal Methods Education Resources (http://www.cs.indiana.edu/formal-methods-education/)
- The Petri Nets World http://www.informatik.uni-hamburg.de/TGI/PetriNets/
- Internet resource: Workflow management coalition http://www.wfmc.org/
- Internet resource: Workflow And Reengineering International Association http://www.waria.com/

10.5 Software

The next software is used in the educational process:

- CWB - The Edinburgh Concurrency Workbench (http://homepages.inf.ed.ac.uk/perdita/cwb/)
- CPNTools (http://cpntools.org/)
- SPIN (http://spinroot.com)

10.6 Distant support of the discipline

Students are allowed and encouraged to direct their questions about assignments and theoretical issues to instructors in class or by e-mail.

11 Course materiel and maintenance

Hardware needed for the course:
Lectures:

- Projector

Practical studies:

- Personal computer for a tutor
- Personal computers for students with installed Java runtime environment