

Московский физико-технический институт (ГУ)  
Факультет инноваций и высоких технологий  
Вероятностно проверяемые доказательства, технический курс по выбору  
Программа курса

### Описание курса

В курсе будет изучена теория вероятностно проверяемых доказательств и её приложения к приближённому решению различных вычислительных задач. Основным результатом курса — знаменитая **PCP**-теорема о полиномиальных вероятностно проверяемых доказательствах для любого языка из **NP**.

### Список тем

1. Вероятностно проверяемые доказательства. Определение класса **PCP** и его вариации. Теорема:  $\text{PCP}(\log n, 1) \subset \text{NP}$ .
2. Приближённое решение **NP**-полных задач. Примеры: **MAX-3SAT**, **INDEPENDENT-SET**. Задача о выполнении условий (**CSP**). Эквивалентность двух формулировок **PCP**-теоремы: равенство классов **NP** и  $\text{PCP}(\log n, 1)$  и **NP**-трудность приближённого решения задачи **MAX-3SAT**.
3. Коды Уолша–Адамара. Доказательство экспоненциальной **PCP**-теоремы:  $\text{NP} \subset \text{PCP}(\text{poly}(n), 1)$ .
4. Интерактивные доказательства с несколькими проверяющими. Теорема:  $\text{MIP} = \text{PCP}(\text{poly}(n), \text{poly}(n)) = \text{NEXP}$ .
5. Экспандерные графы: определение и конструкции.
6. Доказательство главной **PCP**-теоремы:  $\text{NP} = \text{PCP}(\log n, 1)$ .
7. **PCP**-теорема Хостада о трёх битах.
8. Неприближаемость различных конкретных задач. Unique games conjecture.

### Требования к слушателям:

1. Знакомство с теорией сложности вычислений. Классы **P** и **NP**, полиномиальная сводимость, **NP**-полнота. Вероятностные алгоритмы, класс **BPP**.
2. Свободное владение методами комбинаторики и дискретной математики.

### Литература:

1. S. Arora, B. Barak, “Computational Complexity: A Modern Approach”, Cambridge University Press, 2009 (Черновики доступны по адресу <http://www.cs.princeton.edu/theory/index.php/Compbook/Draft>)

2. V. Vazirani, "Approximation Algorithms", Springer, 2004
3. S. Khot, "On the Unique Games Conjecture", Proc. 25th IEEE Conference on Computational Complexity, pp. 99–121  
<http://cs.nyu.edu/~khot/papers/UGCSurvey.pdf>

#### **Дополнительная литература:**

4. J. Katz, "Notes on Complexity Theory", 2011  
<http://www.cs.umd.edu/~jkatz/complexity/f11/all.pdf>
5. O. Goldreich, "Computational Complexity: a Conceptual Perspective", Cambridge University Press, 2008
6. R. O'Donnell, "A history of the PCP Theorem",  
<http://people.csail.mit.edu/dmoshkov/courses/pcp/pcp-history.pdf>

#### **Конспекты, видеолекции и полезные сетевые ресурсы:**

1. Андрей Станкевич, "Теория сложности", Викиконспекты НИУ ИТМО,  
[http://neerc.ifmo.ru/wiki/index.php?title=Теория\\_Сложности](http://neerc.ifmo.ru/wiki/index.php?title=Теория_Сложности)
2. Д. М. Ицкxон, "Вероятностно проверяемые доказательства", видеолекции,  
<http://www.compsciclub.ru/courses/probcheckproofs>
3. Dana Moshkovitz, "Probabilistically Checkable Proofs and Hardness of Approximation", course notes,  
<http://people.csail.mit.edu/dmoshkov/courses/pcp-mit/index.html>
4. Scott Aaronson, Charles Fu, Greg Kuperberg, Christopher Granade, "Complexity Zoo".  
[https://complexityzoo.uwaterloo.ca/Complexity\\_Zoo](https://complexityzoo.uwaterloo.ca/Complexity_Zoo)
5. Dick Lipton, "Gödel's Lost Letter and P=NP",  
<http://rjlipton.wordpress.com/>
6. Scott Aaronson, "Shtetl-Optimized",  
<http://www.scottaaronson.com/blog/>
7. Computational Complexity Blog,  
<http://blog.computationalcomplexity.org/>
8. Вопросы и ответы по теоретической информатике  
<http://cstheory.stackexchange.com/>