PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Complexity Theory, Semester I 2018 - IIC3242
Homework 7
Deadline: Friday, July 6, 2018 at 23:59 Chilean time

In this course we saw many fundamental results about the theory of computation, but there are many more results on the topic that we did not have the time to cover. The goal of this homework is that the student selects some result connected to the topics we covered, or any related topic, which they think is fundamental, important or interesting (and not necessarily all three), and hands in a **written report** which justifies why the result is important, and provides a brief proof, or an explanation of why the result is correct.

More specifically, the homework is to prepare a short report about a certain result in Complexity Theory (or computation in general) which was not covered in the lessons. This report should include:

- An explanation of why the result is important.
- A precise formulation of the result.
- A proof of the result, or, in the case when the proof is extremely long, a detailed sketch of the proof.

The expected length is anywhere between 3 and 7 pages. If you need more space (or less), please explain why is this so. The assignments will be graded based on the clarity of the presentation, the justification of why the problem is important, and on the quality of your English language skills (although this part will only be work up to 10% of the mark).

Finding a topic for the assignment

The first source are the books we used in the course, more specifically, the book by Papadimitriou, and the one by Arora-Barak. Both of these contain a big number of very interesting results that we did not cover in class.

The second source are lecture notes of Complexity Theory courses given at different universities around the world. Some of these cover substantially more material than we did, or cover more advanced topics, so using these is also allowed. The notes I particularly like are by Johnatan Katz from the University of Maryland, but there are many others as well.

A great starting point is also the blog by Lance Fortnow (`http://blog.computationalcomplexity.org`) which discusses some of the most important modern advancements in Complexity Theory. Another good blog is run by Richard Lipton at `http://rjlipton.wordpress.com`.

Next, we have the webpage of the Complexity Zoo, which defines most of the complexity classes which are currently known (`https://complexityzoo.uwaterloo.ca/Complexity_Zoo`). The page also lists some of the most important results about these classes.

Of course, if you want to get to know about the most recent results in the area, you will have to go through the relevant journals and conferences in the area. A partial list of these is:

- Journal of the ACM: `http://www.informatik.uni-trier.de/~ley/db/journals/jacm/index.html`
- SIAM Journal on Computing: `http://www.informatik.uni-trier.de/~ley/db/journals/siamcomp/index.html`

- ACM Symposium on Theory of Computing (STOC): `http://www.informatik.uni-trier.de/~ley/db/conf/stoc/index.html`
- IEEE Symposium on Foundations of Computer Science (FOCS): `http://www.informatik.uni-trier.de/~ley/db/conf/focs/index.html`

In case you want something more, a good general repository of information about journals and conferences in Computer Science is The DBLP Computer Science Bibliography available at `http://www.informatik.uni-trier.de/~ley/db/`.

Some preselected topics

If you are having trouble finding a topic for your assignment, this section contains several preselected topics which you can cover, together with a source that will get you started.

1. Counting complexity: give a motivation on why to study this, define the class $\#P$ and sketch the proof of Valiant's theorem. [Arora-Barak, chapter 17]
2. Toda's theorem: explain the setting and sketch the proof. [Arora-Barak, chapter 17]
3. Communication complexity: define the setting, and explain at least three different techniques for proving communication complexity. [Arora-Barak, chapter 13]
4. Interactive proof and PSPACE: explain the setting and sketch the proof that IP=PSPACE. [Arora-Barak, chapter 8]
5. Interactive proofs for #SAT and the Permanent: explain the setting and the algorithms. [Arora-Barak, chapter 8]
6. PCP Theorem and hardness of approximation: explain the problem and show that different statements are equivalent. [Arora-Barak, chapter 11; Lecture notes by Jonathan Katz]
7. The gap theorem and the speedup theorem: prove them. [Papadimitriou - theorem 7.3, Kozen - chapter 33]
8. Ladner's theorem: give a proof based on the padding technique as presented in the Arora-Barak book.
9. Alternating Turing machines: define them, relate them to PSPACE, and show the tradeoff theorem for SAT. [Arora-Barak, section 5.3, 5.4; Sipser]
10. Quantum computation: define basic concepts (such as quantum entanglement) needed to define quantum computation. Define quantum computation and the class BQP. Show some easy algorithms on quantum computers. [Arora-Barak, section 10.1, 10.2, 10.3]
11. Basic premises of Cryptography: one way functions and pseudo random generators. Prove Goldreich-Levin theorem. [Arora-Barak, chapters 9.1, 9.2, 9.3]
12. Probabilistic algorithms and complexity classes: in class we only started examining probabilistic complexity. To deepen this study, you are first asked to do explain three famous probabilistic algorithms: finding the median, polynomial identity testing, and primality testing. You should then explore probabilistic complexity classes that capture the notion of one sided error (RP and coRP), and define the notion of randomized reductions. [Arora-Barak, 7.2, 7.3 and 7.6]

Remark. Once you select the topic please send me an email confirming which topic it is, so that we do not end up with duplicates.

P.S. Results will be on Tuesday, July 10, together with final notes.