Skoltech
Skolkovo Institute of Science and Technology

Jury Member Report – Doctor of Philosophy thesis.

Name of Candidate: Elena Egorova

PhD Program: Computational and Data Science and Engineering

Title of Thesis: Signature Codes for Multiple Access Channels, Digital Fingerprinting Codes and Symmetric Group Testing

Supervisor: Prof. Grigory Kabatyansky

Name of the Reviewer: Miklós Ruszinkó

I confirm the absence of any conflict of interest	**Signature:** **Date: 29-03-2020**

The purpose of this report is to obtain an independent review from the members of PhD defense Jury before the thesis defense. The members of PhD defense Jury are asked to submit signed copy of the report at least 30 days prior the thesis defense. The Reviewers are asked to bring a copy of the completed report to the thesis defense and to discuss the contents of each report with each other before the thesis defense.

If the reviewers have any queries about the thesis which they wish to raise in advance, please contact the Chair of the Jury.

Reviewer's Report

Reviewers report should contain the following items:

- Brief evaluation of the thesis quality and overall structure of the dissertation.
- The relevance of the topic of dissertation work to its actual content
- The relevance of the methods used in the dissertation
- The scientific significance of the results obtained and their compliance with the international level and current state of the art
- The relevance of the obtained results to applications (if applicable)
- The quality of publications

The summary of issues to be addressed before/during the thesis defense

Elena Egorova's thesis concentrates on bounds and constructions of codes for multiple access channels. Multiple access information theory was booming in the late seventies and eighties of the last century, but it seems to me that researchers of this area got tired from investigating notoriously hard unsolved problems. Alon, Körner[1] and Monti regarded them as follows ``...all of these problems had one thing in common. Not even the exponential growth rate of the maximum number of n-strings with the required property was known. The breakthrough occurred with cancelative set families when Shearer disproved the corresponding conjecture of Erdős and Katona and this led way to Tolhuizein's beautiful discovery that the Frankl-Füredi bound is tight.'' On the other hand - maybe due to technical needs - this subject is in the main stream of mathematical investigations again. So, Egorova chose an important and hard topic to investigate.

By the reasons mentioned above, the size of codes are usually measured on a rough scale, the *rate* which estimates their exponential growth. Egorova gives new bounds and construction in this perspective. In Chapter 2 she investigates codes for A-channels, I will skip the definition here. Maybe the most important result in this chapter is a construction of signature codes with efficient decoding algorithm.

Theorem 1. *There exist t-signature codes for A-channel with rate of order* $O(t^{-3})$ *and decoding complexity polynomial in the code length.*

In order to prove this, a random inner code and a Reed-Solomon code with large distance as an outer code is concatenated. The result is important because it makes efficient decoding possible. I liked this result, although it contains a random part - so it is not exactly a `construction'. Clearly, big distance codes with suitable parameters are cover-free. I am wondering, if replacing the inner random part with a constructive, positive rate code obtained, say, from algebraic geometry (e.g., Tsfasman-Vladut-Zink) would give a much weaker rate? This is my first question to the candidate.

In Chapter 3 codes for B-channels are investigated, let me skip the definition again. The main result of this section can be formulated in the following - two in one - theorem where I will skip the small terms. (In the dissertation the two bounds are separate theorems.)

Theorem 2.

$$\frac{q-1}{4t}\log t - O(t^{-1}) \le R_q^B(t) \le \frac{q-1}{2t}\log t + O(t^{-1})$$

The proof of the lower bound is a non trivial probabilistic argument. Entropy is used to show the upper bound. It seems to me that it is easy to obtain a $\frac{q-1}{t}\log t + O(t^{-1})$ upper bound. Here the 1/2 factor improvement is important, since it is in the exponent. I have to confess that I did not make the computation, but it seems to me that second moment would give a similar upper bound to the one obtained with entropy. My second (maybe not fully mathematical) question to Egorova is the following. Is somehow the second (or higher) moment `encoded' in the entropy approach? Is there any kind of observation, where is it better to use entropy than moments or vice versa?

[1] Claude Shannon award, 2014

Chapter 4 deals with applications: multimedia digital fingerprinting (MDF) codes, constant weight IPP codes and symmetric group testing. The found applications seem to be useful and important.

The obtained results are important, the dissertation is well written. Although there are several misprints, especially in the spellings of the names foreign authors (e.g., Csros, in reference 68). I think that reference 72 has been written by two authors... The references are not in a unified format. I suggest to correct these inaccuracies.

In general, the inaccuracies mentioned above are not essential. As already mentioned, the obtained results are important. They were presented on international conferences and were published in regarded international journals. Therefore, *I recommend that the doctoral degree to Elena Egorova be awarded*.

Miklós Ruszinkó
Alfréd Rényi Institute of Mathematics
Reáltanoda utca 13-15, Budapest, Hungary 1053
ruszinko.miklos@renyi.hu

Provisional Recommendation

☒ *I recommend that the candidate should defend the thesis by means of a formal thesis defense*

☐ I recommend that the candidate should defend the thesis by means of a formal thesis defense only after appropriate changes would be introduced in candidate's thesis according to the recommendations of the present report

☐ The thesis is not acceptable and I recommend that the candidate be exempt from the formal thesis defense