

Jury Member Report – Doctor of Philosophy thesis.

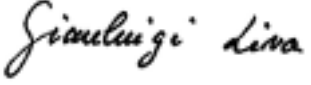
Name of Candidate: Elena Egorova

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:

I confirm the absence of any conflict of interest	Signature:  Date: 23-03-2020
---	---

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

The dissertation addresses the derivation of upper and lower bounds on the rate achievable by signature codes for several classes of MAC channel problems, with application to digital fingerprinting and to (symmetric) group testing. The work is presented in a clear, concise and highly insightful manner, providing all the required background (including a well-conducted literature survey) for correctly place the contributions of the thesis. The contributions are mainly contained in chapters 2 and 3, and partly in chapter 4 (which builds, in particular, on the results of chapter 2). The technical depth of the work is outstanding, and the mathematical tools used to derive the bounds (and to prove the existing of low-complexity code constructions) are sophisticated. Nevertheless, the candidate made a remarkable effort to provide the reader with a clear guidance, providing a number of impressive insights on the adopted techniques. The results achieved in the work are remarkable, since they either provide new bounds on the rate (A/B and wBAC channel) or improve over existing rates (for the care of digital fingerprinting, leveraging on the results achieved over the A channel). The constructive approaches to obtain classes of good signature codes out of know existing constructions are also particularly enlightening. Further comments follow, for each chapter.

Chapter 1. The chapter introduces the main notions required in the rest of the dissertation, in particular: The various MAC channels, the class of coding problems that will be treated, and the proper rate definitions. Additional tools are provided, which include the concept of partial MAC channel ordering, which will turn to be useful to obtain quickly results for some channels. The main definitions for the classical binary adder channel (BAC) are discussed, with the related rate bounds. Signature codes for several MAC channels are introduced. Finally, two applications are presented, namely symmetric combinatorial group testing and digital fingerprinting. The chapter provides an excellent survey on the topic of the thesis, and lies down a clear ground for the upcoming chapters.

Chapter 2. The chapter attacks the first challenge of the work, i.e., the derivation of bounds for signature codes over the A channel as well as the construction of efficiently decodable codes. After recalling the main definitions for the A channel, an approach for the derivation of the lower bound on the rates is illustrated, which relies on using the OR channel as a proxy and of the partial ordering approach (Proposition 1.1.1). Codes that can be efficiently decoded are discussed, showing how a class of asymptotically good codes exist, which enables decoding with

polynomial complexity in n (at the cost of a rate loss w.r.t. the best rate, as a function of t). The construction is based on concatenated codes, with an outer RS codes and inner random codes. Codes that can deal with noisy outputs are also discussed, in Section 2.4. Here, an adversarial channel model is assumed. Lower bounds on the rates are derived, again, results known for the OR channel. Upper and lower bounds, in general, are derived for the A channel. The chapter contains the first major contributions, and it develops bounds and code constructions in an elegant and clever way. The adopted arguments are quite sophisticated, nevertheless the candidate made an excellent work in guiding the reader through the result, providing a number of insights for the various approaches. The technical contribution provided here is of excellent quality.

Chapter 3. Signature codes for the B channel are introduced, which make use of the “intensity” information. In particular, lower bounds (to the limit inferior) and upper bounds (to the limit superior) are analyzed, providing two tight inequalities to “sandwich” the actual rate. The lower bound is obtained by asymptotic enumeration applied to a random coding bound argument. The upper bound is proved by developing bounds on the R.V. associated to the set of t -elements subsets of the code. Generalizations of the B channel, and of the binary adder channel, are discussed, showing how the results for the B channel can be used to obtain alternative bounds for the binary adder channel. The adopted arguments are, again, very elegant and insightful. Attention is shifted, then, to a variant of the binary adder channel, which allows positive real weights to build superpositions of codewords. The chapter is on par with the previous one, both in terms of technical contribution (which is outstanding) and of exposition quality (which is excellent and makes the reading extremely pleasant).

Chapter 4. The last chapter deals with the applications identified already in the introduction, i.e., multimedia fingerprint codes, and symmetric group testing. For the first case, novel and remarkable results are obtained w.r.t. the problem of coalition attacks. More specifically, the candidate addresses the general scenario where the coalition members are allowed to choose an arbitrary linear combination (with the only limitation of allowing positive coefficients, summing up to 1). By exploiting the results of Chapter 2 for the A channel, bounds on the achievable rates are derived, which improve on the existing bounds (that were derived by even assuming a simplified setting of pure averaging). The result is outstanding, and shows the

impact of the results attained in Chapter 2. Also for the symmetric group testing case, the results for the A channel (with adversarial error model) are employed.

Final remarks. The overall contribution of the dissertation is outstanding. The candidate showed an excellent capability to enter deeply in a complex topic, and a phenomenal capability do obtain elegant, new results based on clever intuitions. The presentation of the work is also excellent, and it allows to shed light on the (many) important contributions of this work.

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