REVIEW

on the PhD thesis for acquiring
the educational and scientific degree of „doctor“

Topic: „ Discrete Transforms and their Application in Coding Theory and Combinatorics“

Author: Paskal Nikolaev Piperkov,
Section Mathematical Foundations of Informatics (MFI), Institute of mathematics and informatics (IMI), Bulgarian academy of sciences (BAS)

Scientific advisor: Prof. Iliya Georgiev Bouyukliev, DSc

Area of higher education: 4. Natural sciences, mathematics and informatics

Professional Field: 4.5. Mathematics

Scientific field: Algebra and number theory

Reviewer: Prof. Nikolay Ivanov Yankov, DSc, Shumen University "Bishop Konstantin of Preslav”

I was appointed by order № 159/27.06.2022 of IMI’s director to be a member of this scientific jury and on the first session I was voted to write this review. I confirm that I have received all materials for this procedure according to LDASRB (the Law for the development of the academic staff in the Republic of Bulgaria). I do not have information for violations of the procedure, nor I’m aware of plagiarism in the presented PhD thesis.

1. **PhD student “curriculum vitae”**

Paskal Piperkov has a degree of mathematics from Sofia University issued 1997 г. Since January 2018 he has been a Mathematics doctoral student in the scientific field „Algebra and number theory“ studying at section MFI of IMI.

In the attached resume, as well as in the other materials for the present procedure, unfortunately, I did not find any data on the participation of the doctoral student in scientific projects, which I consider important because the legislator has provided that the doctorate degree is "educational and scientific."

2. **About the candidates’ doctoral education**

Paskal Piperkov was enrolled in full-time doctoral degree studies from 01.01.2018 for a period of 3 years, and later, by Order No. 226 of 02.12.2018, the doctoral studies were transformed into part-time studies with a study period of 01.01.2018–01.01.2022.

By decision of the Scientific Council of IMI (Protocol No. 5/07.01.2022) the doctoral education was complete with the right of thesis defense. The preliminary discussion of the dissertation took place on 10.06.2022 at an extended meeting of MOI, which I attended. By

order of the director of IMI, a scientific jury and the date of the defense were determined. I believe that the procedure is regular and there are no violations.

3. About the thesis and its abstract

The submitted thesis consists of: introduction (5 pages), main text (76 pages) in 4 chapters, divided into sections. Included in the dissertation is a list of contributions, a bibliography of 71 titles, lists of publications and presentations at scientific forums.

The thesis meets the requirements of LDASRB and RALDASRB (Rules on the application of the Law for the development of the academic staff in the Republic of Bulgaria), as well as of Regulations on the terms and conditions for acquiring scientific degrees and for holding academic positions in BAS. The abstract (in 31 pages) adequately reflects the main ideas and significant final results that are described in the dissertation.

4. Importance of the research

It is well known from the 1978 work of Berlekamp, McEliece, and van Tilborg, that the problem of finding the weight distribution of a linear code is a NP-complete problem. About the code covering radius: In 1984 Aileen McLoughlin proved that the covering radius of a linear code is a NP-hard problem. Therefore, the work on simplifying the algorithms, and even more so on their acceleration, is relevant. Moreover, the relevance and scientific contributions of the PhD thesis to the development of the subject are indisputable. The importance of the thesis' achievements is also confirmed by the three citations of the authors' paper published in Cryptography and Communications.

5. Degree of knowledge of the problem state

The PhD student understands the current state of the problem well enough. The list of 71 literary sources chronologically begins with works by Sylvester from 1867 and Hadamard from 1893. A total of 20 of the publications are contemporary – dating from 2000 to the present. The educational part in the "doctoral degree" requires the doctoral student to show that he has entered the relevant scientific field. In this regard, I believe that Paskal Piperkov has successfully entered the field of algebraic coding theory – a modern mathematics subject, and the dissertation gives a clear idea of the history and current state of the problems under consideration and of the methods applied in this research.

6. Scientific contributions

Chapter 2 of the dissertation shows a new algorithm for calculating the weight distribution of a code over a prime finite field. This is achieved using characteristic vector and distribution, as well as shortened characteristic distribution, which is a generalization of Walsh spectrum. In addition to the new theoretical results, the thesis calculates the complexity of the proposed new algorithm and presents experimental results. Using data from the thesis, one can make the

conclusion that in large codelengths $n > 300$ the acceleration achieved in the new algorithm is between 5 and 500 times with comparison to the best known algorithms. If we compere the proposed new algorithm with the corresponding algorithm implemented in the computer algebra system „MAGMA“ the acceleration achieved is between 2 and 20 times. This, in my opinion, is an excellent result since MAGMA has always known for implementing the fastest and latest algorithms.

In Chapter 3 a new method for computing the weight distribution of a linear code over a composite finite field $\mathbb{F}_q$ is presented. With the trace transformation and self-dual basis, a Walsh-Hadamard type transformation is used in the case of characteristics 2. Whereas a Vilenkin-Krestenson type transformation is employed when $p > 2$. This leads to a reduction in the complexity of the proposed butterfly algorithm, and the complexity can be reduced by a factor of q. Again, there is an improvement here, mainly in cases where the code length is large or we have a larger field, i.e., in the more difficult cases.

Chapter 4 shows new methods for finding the covering radius of a code over finite field, where both cases are considered here: when we have a prime and a composite field, respectively. In the case of a prime field the connection between the Vilenkin-Krestenson transformation and the covering radius is used, whereas a code's parity-check matrix is needed. The proposed method can be applied for finding the weight distribution of the coset leaders of a linear code over odd prime field $\mathbb{F}_p, p > 2$. In the case of composite field this method is reformulated by using the trace transformation, which allows the shortened characteristic distribution to be used to find the covering radius and the algorithms from the previous two chapters also can be used. The methods in this chapter are proven generalizations of Karpowski's method, which has been used only for binary codes, and in the thesis a generalization to the more complex cases is shown.

The PhD thesis under review has an adequate completeness, with the main claims and facts used being properly proven theoretically. The resulting algorithms are described with pseudocode, illustrated with diagrams, theoretically proven, and also implemented in practice. These new algorithms are showing improvements over previously known algorithms.

I acknowledge the scientific and applied-scientific contributions indicated in the thesis.

7. Publications and participation in scientific forums

There are 4 scientific papers in the list of publications. All of these papers have at least one co-author and all works are peer-reviewed. One of the journals: Cryptography and Communications Discrete Structures, Boolean Functions and Sequences has an impact-factor (JCR-2021, IF=1.376) and it's in the second quartile of the "Applied mathematics" section. Two of the other papers are in thematic collections: "Recent Topics in Differential Geometry

and its Related Fields" and "New Horizons in Differential Geometry and its Related Fields" published by World Scientific Publishing Company, Singapore. The fourth paper is published in the proceeding of the international scientific conference „Optimal Codes and related topics" (OCRT 2017).

I believe that the participation of the doctoral student in all publications is equal to the other co-authors. The number of articles meets the requirements of LDASRB, RALDASRB, as well as the rules of BAS and IMI.

In the text of the dissertation, a list of 13 scientific talks (of which 6 are independent) is attached, in which the doctoral student himself announced the results of this dissertation at various national and international forums. In my opinion, this approval of the results of the dissertation work exceeds the minimum requirements and shows the readiness of Paskal Piperkov for independent scientific research.

8. Conclusion

This PhD thesis fully meets the requirements established by the LDASRB, as well as the regulations of BAS and IMI, so I confidently suggest to the esteemed scientific jury to vote for the educational and scientific degree "Doctor" to BE ACQUIRED by Paskal Nikolaev Piperkov in professional field 4.5. „Mathematics", scientific field „Algebra and number theory".

Reviewer ……

/ Prof. Nikolay Yankov, PhD /

25.07.2022 г.

Shumen, Bulgaria