ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

REVIEWER'S OPINION OF FINAL THESIS

I. IDENTIFICATION DATA

Thesis name:	**Analysis and comparison of methods of Grobner bases for solving nonlinear polynomial systems in finite fields of characteristic 2**
Author's name:	**Ildar Nizamov**
Type of thesis :	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Department of Computer Science
Thesis reviewer:	Ishmukhametov Shamil Talgatovich
Reviewer's department:	Kazan Federal University, Institute of Computer Mathematics and Information Technologies, Department of System Analysis and Information Technologies

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment **challenging**

Evaluation of thesis difficulty of assignment.

The Master Thesis submitted by Ildar Nizamov considers an important problem of solving nonlinear polynomial equations in finite fields of characteristic 2. This problem arises in Cryptography in and in Coding Theory. As a possible solution to the problem, the author proposes a method that uses Grobner bases introduced by Bruno Buchberger, an analogue of the Gauss method for systems of nonlinear equations. The diploma thesis main goal was to provide a comparative analysis of algorithms for constructing these bases, develop the own software implementation of these algorithms, which is capable to operate with elements of finite fields of characteristic 2 unlike other known implementations, and verify the obtained results in practice.

Satisfaction of assignment **fulfilled with minor objections**

Assess that handed thesis meets assignment. Present points of assignment that fell short or were extended. Try to assess importance, impact or cause of each shortcoming.

The Thesis begins with a full study of the problem in the search for a solution. In the first part, the author gives a brief overview of the existing methods for solving systems of equations of this type. Next part is the full-scale review of the theory of ideals in polynomial rings of many variables. In the process, he introduces the definition of the concept of the Grobner basis for an ideal, and an algorithm for its construction. Later in this part, Ildar describes an improvement for this algorithm and gives an estimate for its complexity. The third part of the work is devoted to a special type of algorithms for construction of Grobner bases based on polynomials signatures. These algorithms allow the researcher to find desired bases with the highest efficiency. A detailed analysis of several algorithms of this type is provided: F5 and its modifications F5R and F5C. Last part of the Thesis describes the library of classes, which was implemented by the author. The author provides the structure of library and the obtained experimental results.
The work is performed at the high level, the content is fully consistent with the assignment. The diploma Thesis also contains a lot of examples for the representation of used theory and algorithms. However, there is some moments in the document, which could be described more in detail. For example, I would like to get more information about the testing process.

Method of conception **correct**

Assess that student has chosen correct approach or solution methods.

The author analyzed many existing solutions of the problem. It was shown that all of them are suitable for the problem solving only in some certain cases. The author chose the Grobner bases methods, because they are appropriate for all known cases.

Technical level **A - excellent.**

Assess level of thesis specialty, use of knowledge gained by study and by expert literature, use of sources and data gained by experience.

The theory that mentioned in the Thesis requires the high level of knowledge in mathematics and number theory. The author didn't use many sources, but all of them are handy and fully appropriate.

Formal and language level, scope of thesis	**B - very good.**
Assess correctness of usage of formal notation. Assess typographical and language arrangement of thesis.	
There is a few typographical errors in the document. The author uses many formulas to provide the explanation of the theory. The division of the text into chapters and its presentation corresponds to the internal logic. Also, the author tries not to use very sophisticated sentences in order to provide understandability.	

Selection of sources, citation correctness	**B - very good.**
Present your opinion to student's activity when obtaining and using study materials for thesis creation. Characterize selection of sources. Assess that student used all relevant sources. Verify that all used elements are correctly distinguished from own results and thoughts. Assess that citation ethics has not been breached and that all bibliographic citations are complete and in accordance with citation convention and standards.	
The author didn't use many sources, but all of them are handy and fully appropriate. The sources contain all information, which is related to the problem. The use of citations is appropriate. The author tried to use citation conventions and standards, but not all citations are correct in the Thesis.	

Additional commentary and evaluation
Present your opinion to achieved primary goals of thesis, e.g. level of theoretical results, level and functionality of technical or software conception, publication performance, experimental dexterity etc.
In conclusion, the theme of the work is fully disclosed, all goals have been achieved, and all tasks have been accomplished. However, the text itself has a few drawbacks. Perhaps this is due to lack of time. Considering these facts, the value of this work is very good.

III. OVERALL EVALUATION, QUESTIONS FOR DEFENSE, CLASSIFICATION SUGGESTION

Summarize thesis aspects that swayed your final evaluation. Please present apt questions which student should answer during defense.

I evaluate handed thesis with classification grade **B - very good.**

1. *The testing process is not described in detail. How the testing of the implemented library was conducted?*
2. *The author says about the possible production use of the Grobner bases. Can the author give an example?*

Date: **4.6.2018** Signature: