Advisor's evaluation for Master's thesis of Sára Vyhnalová

Vítězslav Kala

September 3, 2021

The thesis of Sára Vyhnalová studies ideal lattices and their applications in modern cryptography. This is a new and active area of research that applies number theory and the study of lattices. The thesis expands on the work of Ding and Lindner (2007), which provided an algorithm for identifying an ideal lattice. *Most of the work supervising the thesis was done by Pavlo Yatsyna (listed as 'consultant'), who also wrote most of this evaluation.*

The first two chapters include the necessary preliminaries (from linear algebra and elementary number theory) and introduce lattices, in particular ideal lattices. The second chapter also incorporates the expanded versions of the results of Ding and Lindner for identifying ideal lattices. Chapter 3 includes the algorithm from Ding and Lindner's paper, with added examples, consideration of cyclic lattices and generalizations of certain results from the paper (their Theorem 3). Chapter 4 on NTRU lattices is a great extension of Section 2.7 from Ding and Lindner's paper and includes many more examples and interesting interpretations. This is by far the strongest and most original chapter of the thesis. Chapter 5 gives applications to modern cryptography, which is a literature review of the applications of lattices in this field of research. The thesis ends with a conclusion.

The main **strength** of the thesis is that it manages to formalize much of the material included in Ding and Lindner's paper and tries to consider various interpretations/generalizations. This is a difficult task as the above-mentioned paper is interdisciplinary and not the easiest piece of work to study rigorously. The examples provided are interesting and may be misleading as to the difficulty of the task. There is also an overarching narrative to the thesis, joining the chapters together, making it easy to read. The proofs are detailed and quite well explained.

On the other hand, all the tools used are elementary and only Chapters 3 and 4 provide new material and examples. The thesis contains rather small amount of material that is sufficiently advanced for a Master's thesis. The overall length (52 pp.) of the thesis does not suggest this; however, the thesis is rather sparse: quite a lot of space is taken (e.g.) by large matrices, and sometimes the text is unnecessarily detailed. Specifically, Proposition 28 states a rather easy fact, whose proof nevertheless takes more than 2 pages in the thesis. There is of course nothing wrong with giving lots of details (which is why we advised the student to keep the proof) – but overall the contents of the thesis are barely advanced enough. This is the main **weakness** of the thesis.

However, the thesis fulfills the topic assigned in SIS, and so I recommend it to be accepted as a diploma thesis and suggest the grade *very good* (2).

Vítězslav Kala