Aalto University

Dissertation press release 19.10.2020

Wireless communications, Lattices, and Number Theory.

Title of the dissertation	Well-Rounded Lattices and Applications to Physical Layer Security.
Contents of the dissertation	Physical layer communication is a family of methods and techniques that are dedicated to ensuring reliability and security by exploiting noisy communication channels' characteristics. In plain terms, the present thesis is devoted to using our understanding of the noise to propose reliable and secure codes. Indeed, one can define a reliable communication system as a system where the probability of error is as small as possible. Similarly, a secure communication scheme can be seen as a system where the chances of an eavesdropper recovering the message are minimal. In the wireless setting, these optimisation problems can be again translated to finding configurations of points in Euclidean space satisfying some given properties. In fact, one can represent signals of finite bandwidth by points in Euclidean space, and this representation allowed mathematicians to see codewords or messages as geometric objects. More precisely, we can consider cookbooks as discreet sets in Euclidean spaces. Lattices are simply discrete subgroups of Euclidean spaces. Consequently, many reliability and security problems can be reformulated as optimisation problems on the space of all lattices. The space of all lattices has many technical difficulties, thus, a natural direction to take is to restrict our problems to "smaller" subspaces, in our case, we considered a particular subset of lattices called well-rounded lattices, and our investigation laid on studying the restriction of some communication problems to these lattices. The significance of this restriction can be supported by the fact that well-rounded lattices are rare among all lattices. Hence, constructing them is also an interesting problem in its own right. Our study is further supported by explicit constructions where we used number theoretic methods or more precisely the arithmetics of number fields to capture the well-roundedness property.
Field of the dissertation	Mathematics.
Doctoral candidate	Mohamed Taoufiq Damir, M. Sc.
Time of the defence	06.11.2010 time 15h00.
Place of the defence	Aalto University School of Science, lecture hall M1, Otakaari 1, Espoo + Zoom
Opponent	Professor Kazim Büyükboduk, University College Dublin, Ireland.
Custos	Professor Camilla Hollanti., Aalto University School of Science, Department of Mathematics and Systems Analysis.
Doctoral candidate's contact information	Mohamed Taoufiq Damir, Department of Mathematics and Systems Analysis 0505215321, mohamed.damir@aalto.fi, mohamed.taoufiq.damir@gmail.com