Title: Kerdock codes and around
Author: Kateřina Teplá
Department: Department of algebra
Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc., Department of algebra

Abstract: Kerdock codes form a family of nonlinear codes, that contains more codewords than any known linear code with the same parameters. The main goal of this thesis is a connection of Kerdock codes with other areas of mathematics, mainly orthogonal geometry, combinatorics and cryptography. It describes theory of symplectic and quadratic forms on vector spaces of characteristic 2 and its relationship to Kerdock codes. Then it is proven, that codewords of Kerdock code of constant weight form combinatorial 3-design. Finally usage of Kerdock codes in construction of Boolean bent functions and t-resilient functions, that are basis of many cryptographic primitives, is analysed.

Keywords: Kerdock code, Kerdock set, t-design, resilient function