Název práce: Kerdockovy kódy a okolí
Autor: Kateřina Teplá
Katedra: Katedra algebry
Vedoucí diplomové práce: prof. RNDr. Aleš Drápal, CSc., DSc., Katedra algebry

Abstrakt: Kerdockovy kódy tvoří rodinu nelineárních kódů, které obsahují více kódových slov než libovolný známý lineární kód se stejnými parametry. Hlavním cílem této práce je propojení Kerdockových kódů s jinými oblastmi matematiky, zejména ortogonální geometrií, kombinatorikou a kryptografií. Je zde popsána teorie symplektických a kvadratických forem na vektorových prostorech charakteristiky 2 a jejich vztah ke Kerdockovým kódům. Dále je dokázáno, že kódová slova Kerdockova kódu libovolné váhy tvoří kombinatorický 3-design. Závěrem je rozebrána použitelnost Kerdockových kódů při konstrukci Booleovských bent funkcí a t-resilientních funkcí, které jsou základem mnoha kryptografických primitiv.

Klíčová slova: Kerdockův kód, Kerdockova množina, t-design, resilientní funkce