

Nedávné studie přinesly několik různých přístupů ke klasifikaci vektorových booleovských funkcí na základě různě definovaných relací ekvivalence, a k nalezení nových kvadratických “téměř dokonale nelineárních” (APN) funkcí. V této práci se zabýváme těmito klasifikacemi a to především takovými, které zmenšují počet všech hledaných funkcí na základě rozdělení do tříd EA-ekvivalence nebo lineární ekvivalence. Zároveň se také věnujeme různým přístupům pro hledání kvadratických APN funkcí. Tyto metody mají základ v odlišných odvětvích algebraické teorie. Podrobněji se zabýváme matematickou částí této teorie a poskytujeme popis jejího praktického uplatnění. Rovněž přinášíme implementace těchto metod a vysvětlujeme je v kontextu popsání teorie.