

Algebrai kódoláselmélet

Heti óraszám: 2+0

Célkitűzés: A hibakorlátozó kódolás matematikai elméletének bevezető tárgyalása (feltételezve, hogy a legalapvetőbb fogalmak a korábbi tanulmányokból ismeretesek) néhány jelentős kódosztály és kódkonstrukció ismertetésével. A félév során gyakorlatilag csak a véletlen hibát javító blokk-kódokkal foglalkozunk, a hibacsomók javítását éppen csak érintjük. A célkitűzés elsősorban az, hogy a kommunikációval vagy számítógép-hálózattal foglalkozó szakemberek, továbbá a számítástechnikát oktatók ismerjék a hibakorlátozás lehetőségeit és korlátait, elképzelésük legyen a hibakorlátozás elveiről, lehetőségeiről és korlátairól.

Tematika: A kódoláselmélet valószínűségi alapjai: hibakorlátozó kódok; csatornák; döntési séma, döntési hiba, ideális megfigyelő, maximum likelihood döntés; ismétléses kód, kódsebesség; entrópia, kölcsönös információ, csatornakapacitás; zajos csatorna kódolási tétele és megfordításai (távirati stílusban)

- b. Minimális távolságú dekódolás emlékezet nélküli diszkrét szimmetrikus csatornával
- c. Ekvivalens kódok, szisztematikus kód
- d. Lineáris kódok, skalárekvivalencia, generátormátrix standard formája; duális kód, önortogonális és önduális kód
- e. Ciklikus kódok; maximális és minimális ciklikus kód; ciklikus kódok szisztematikus generálása; ciklikus kód gyökei, a gyökök és kódszavak kapcsolata; szisztematikus ciklikus kód szindrómája, az eltolt szindrómája
- f. Szindróma-dekódolás, hibacsapda-dekódolás
- g. Kódkonstrukciók I. (kiterjesztés, átszúrás, kódszavak elhagyása, növelés, rövidítés, hosszabbítás, direkt összeg, $u, u+v$ konstrukció, maradékkód)
- h. Optimális kód, kódolási korlátok (elemi korlátok, Varshamov-Gilbert, Hamming, Singleton, Plotkin, BCH, Griesmer korlát; aszimptotikus korlátok); perfekt kód
- i. Hamming-kód, rövidített és kiterjesztett Hamming-kód; Hamming-kód duálisa, szimplex kód
- j. MDS-kódok
- k. Reed-Solomon kód, RS-kód generálása inverz diszkrét Fourier-transzformációval; binárisba fejtett RS-kód és általánosítása, hibacsomó, hibacsomó-javítás
- l. Kódkonstrukciók II. (átfűzéses kód, direkt szorzat kód, kódok konkatenálása)
- m. RS-kódok dekódolása a diszkrét Fourier-transzformáció és rekurzív sorozatok felhasználásával
- n. Alternáns és Goppa-kódok; bináris Goppa-kód
- o. Alternáns kódok dekódolása euklideszi algoritmussal

Előismeretek: a Bevezetés a matematikába vagy Matematika I. című tárgy első három féléve, vagy az Algebra című tárgy, továbbá a Véges testek

Irodalom: a. McWilliams, Sloane: The theory of error-correcting codes, North-Holland, 1977

van Lint: Introduction to coding theory, Springer Verlag, 1982

Roman: Coding and information theory, Springer Verlag, 1992

Lucky-Salz-Weldon: Adatátvitel, Budapest