Előszó

Az információelmélet a hírközlés matematikai elmélete. Születését lényegében Claude Shannon [39] művének 1948-as megjelenéséhez köthetjük. Ez a munka volt az első, amely matematikai alapossággal tárgyalta az adattömörítés, a biztonságos adatátvitel és a titkosítás problémáit. Shannon adott először kezelhető és hasznos matematikai modelleket az információs folyamatok leírására, mégpedig úgy, hogy az egyes problémák esetén tisztázta az elvi határokat, és többségében meg is konstruálta azokat a módszereket, amelyek ezeket az elvi határokat aszimptotikusan elérik. Ugyanakkor napjainkban tömegesen terjedtek el az egyes adattömörítő és hibakorlátozó eljárások, tehát indokolt, hogy ezek alapvető elveit is áttekintsük. Az 1. fejezetben ismertetjük a veszteségmentes adattömörítést, míg a 2. fejezetben a veszteséget (torzítást) megengedő adattömörítő (forráskódoló) eljárásokat tárgyaljuk. A 3. fejezet témája a csatornakódolás.

A forráskódolás elméletével ellentétben a csatornakódolás eredményei nem konstruktívak, tehát ma még nem ismertek olyan kódolási–dekódolási eljárások, amelyek tetszőleges csatorna esetén a csatornakapacitást megközelítenék. Ugyanakkor ismertek olyan algebrai hibavédő kódok, amelyek számos gyakorlati probléma megoldását segítik. A '80-as évektől alkalmazzák polgári célokra is a hibavédő kódokat, napjainkban a CD-ben használt Reed–Solomon-kód szinte minden háztartásban megtalálható. A 4. fejezet összefoglalja a hibajavító kódok alapjait.

Az 5. fejezet témája a nyilvános kulcsú titkosítás, tehát az a probléma, hogy nyilvános hálózaton hogyan biztosítható az adat- illetve hozzáférésvédelem.

Ez a tankönyv a Linder – Lugosi [22] és a Györfi – Vajda [20] jegyzet „uniójának" a kiegészítése azon tapasztalatok felhasználásával, amelyeket a BME műszaki informatikusoknak tartott Információelmélet és Kódelmélet tárgyak oktatása során szereztünk az elmúlt 10 évben.

A mű elkészítésében nyújtott segítségükért szeretnénk köszönetet mondani György Andrásnak, Laczay Bálintnak, Linder Tamásnak, Lois Lászlónak, Lugosi Gábornak, Patricza Andrásnak és Pintér Mártának.

Budapest, 2000. augusztus 22.

Györfi László
Győri Sándor
Vajda István