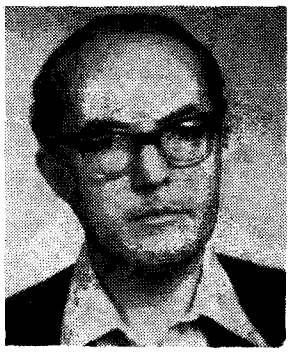
Hírközlő hálózatok információelméleti problémái*

DR. CSISZÁR IMRE
MTA — Matematikai Kutató Intézete



ÖSSZEFOGLALÁS

A szerző SHANNON-nak az egy csatornán történő, egyirányú információátvitelre kialakított modelljéből indulva, a több felhasználós rendszerek terén folyó kutatásokba segíti betekintésünket. Elemzésének egyik központi kérdése a csatornák kapacitása, kapacitástartománya. Elemzései során vizsgálja a point—muiti point rendszereket is. (□)

A hírközlési hálózatok és szolgáltatások új típusainak megjelenésével párhuzamosan a matematikai információelméletben az érdeklődés homlokterébe kerültek a több felhasználós rendszerek optimális kihasználására vonatkozó vizsgálatok. Ez a témakör mind elméleti, mind gyakorlati szempontból nagyon szerteágazó, de az alapvető kérdések és eredmények jellegéről talán néhány kiragadott példa vázlatos ismertetése is nyújthat némi információt (1. ábra).

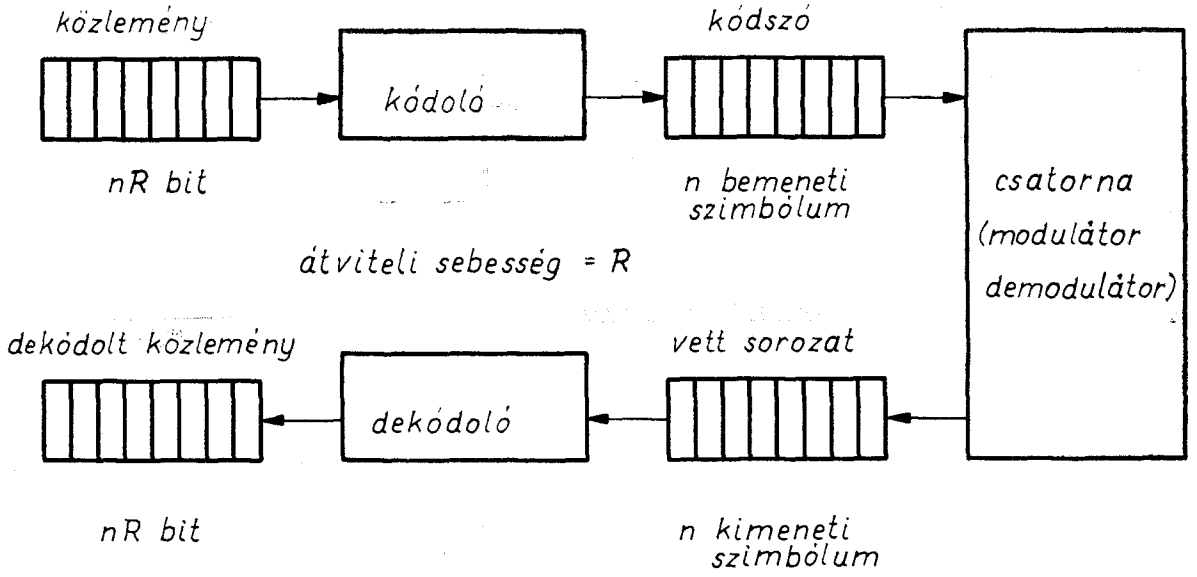
A Shannon-féle információelmélet klasszikus része az egy csatornán történő egyirányú információátvitelre vonatkozik. Alapvető eredménye, hogy megfelelő kódolással az átvitel megbízhatóságára vonatkozó tetszőlegesen szigorú kritérium is teljesíthető, ha az átvitel sebessége kisebb, mint egy — a csatornát jellemző — információelméleti mértékszám, az ún. kapacitás (1. táblázat).

DR. CSISZÁR IMRE

1961-ben szerzett matematikusi diplomát az Eötvös Loránd Tudományegyetemen. 1967-ben lett kandidátus és 1977-ben a matematikai tudományok doktora. Az MTA Matematikai Kutató Intézete információelméleti osztályának vezetője és az ELTE valószínűségszámítási tanszékén egyetemi tanár. Kutatási területe: az információelmélet és alkalmazásai. Az „Information Theory: Coding Theorems for Discrete Memoryless Systems" (Akadémiai Kiadó — Academic Press, 1981) monográfia társszerzője.

1982-ben lényeges előrehaladás történt abban az irányban, hogy ilyen elméletileg optimális kódolást hogyan lehet ténylegesen megvalósítani (2. ábra).

A több felhasználós rendszerek egyik legegyszerűbb matematikai modellje az ún. több bemenetű csatorna (multiple access channel). Itt két (vagy több) térbelileg elkülönült adó továbbít információt egy közös vevőnek. Az átviteli sebesség szerepét most az (R_1, R_2) sebességpár játssza, a kapacitását pedig az ún. kapacitástartomány. A klasszikus esettől eltérőleg az utóbbi függ attól, hogy a hibavaló-



Egyirányú információátvitel blokk-kódolással

1. ábra

* Elhangzott az MTA 1983. V. 2-i tudományos ülésszakán.

H896-1

Shannon tétele: tetszóleges kis hibavalószínűségű átvitel lehetséges, ha $R < C$, *de nem lehetséges, ha* $R > C$.

$$C = \max I(X \wedge Y) = \max_{P} \sum_{x} \sum_{y} P(x) W(y|x) \log \frac{W(y|x)}{\sum_{x'} P(x') W(y|x')}$$

Shannon elmélet ~ Algebrai kódelmélet

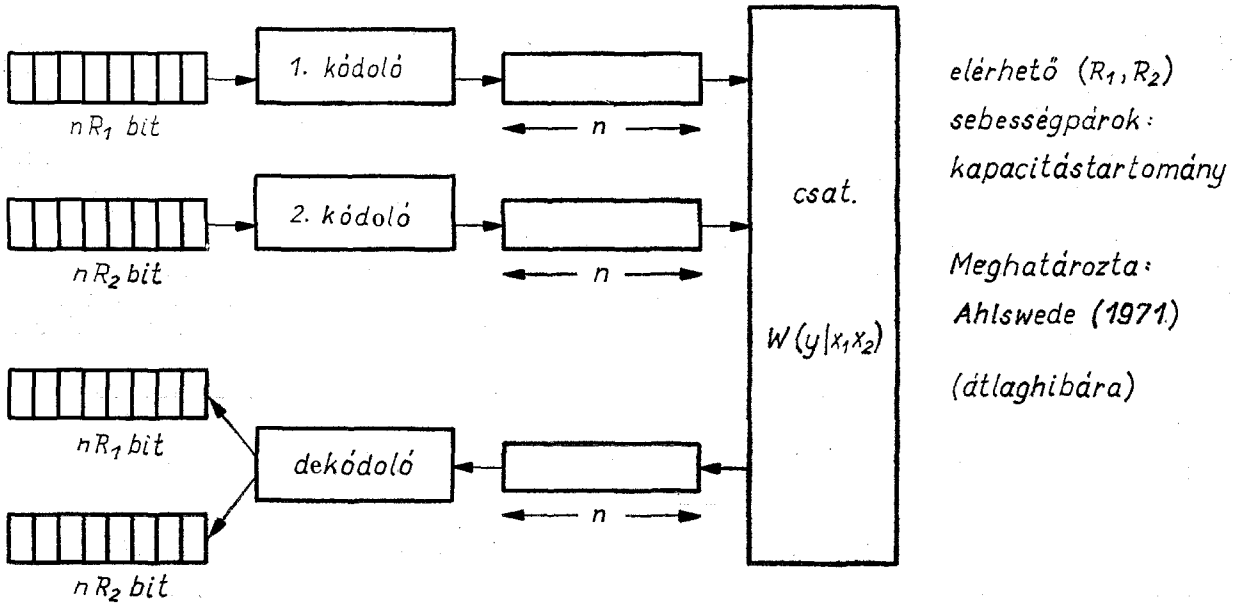
Aszimptotikusan optimális effektiv kódolás-dekódolás:

Delsarte - Piret (1982)

Kódolás egyetlen csatornára

H 896-1T

1. táblázat



Több bemenetű csatorna

H 896-2

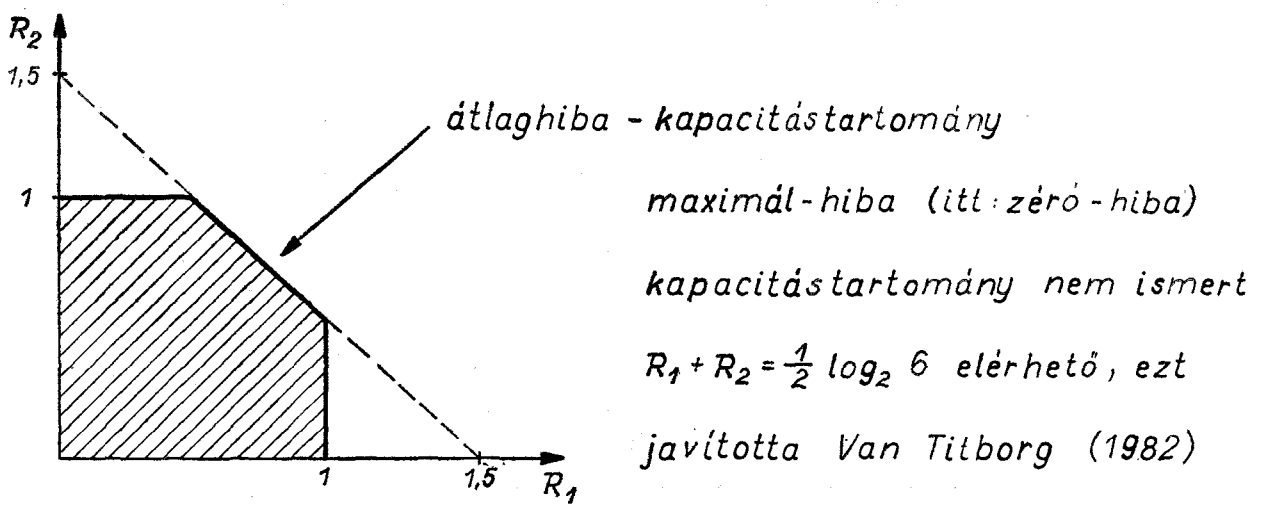
2. ábra

színűségnek az átlagát vagy pedig a maximumát kell-e előírt korlát alá szorítani. A kétféle kapacitástartomány közül jelenleg csak az elsőnek ismeretes kiszámítási módja (3. ábra).

A kétbemenetű csatornák egyszerű példája a zaj nélküli bináris összeadó csatorna. Ennek átlaghiba-kapacitástartományát az ábra mutatja; a maximálhiba-kapacitástartomány (amely most a zéróhiba-kapacitástartománnyal azonos) még ebben a nagyon speciális esetben sem ismert (4. ábra).

Másik érdekes modell, amikor egy adó közvetít különböző üzeneteket két (vagy több) térbelileg elkülönült vevőnek. A matematikai vizsgálat azt mutatta, hogy a természetes „időosztásos" üzemmód általában nem optimális, de a pontos kapacitástartomány jelenleg csak bizonyos speciális esetekre ismert (2. táblázat).

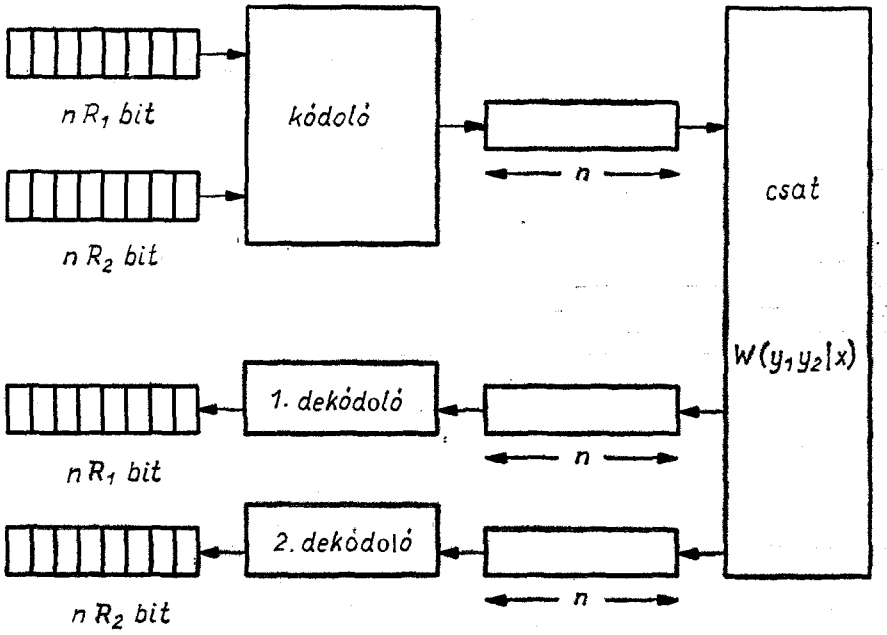
Bár az említett és hasonló jellegű modellek információelméleti vizsgálata fontos kiindulópontot nyújt a konkrét hírközlési hálózatok lehetőségeinek analíziséhez, a gyakorlatban további szempontokra is figyelemmel kell lenni. Így *a)* mind az adók, mind a vevők száma nagy lehet és időben változhat, *b)* az adók közt nincs meg a modellekben feltételezett szinkronizmus,



Példa: bináris összeadó csatorna

H 896-3

3. ábra



A kapacitástartomány csak speciális esetekben ismert. Körner-Marton (1977)

Több kimenetű csatorna (broadcast channel)

H 896-4

4. ábra

c) effektív kódolási—dekódolási algoritmusokra van szükség, *d)* gyakran követeimény a titkosság biztosítása. Jellegzetes példaként említem az ún. kiterjesztett spektrumú rendszereket (5. ábra).

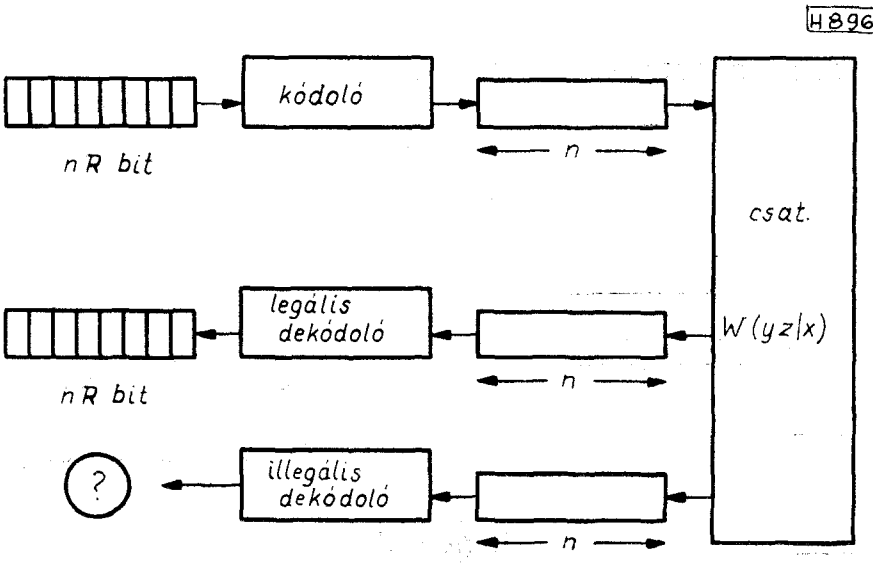
A titkosság szempontjából az elvi lehetőségek vizsgálatára szolgál az ábrán szemléltetett modell. Itt pontosan megadható az a maximális sebesség, mellyel az adó a legális vevőnek tetszőlegesen előírt megbízhatósággal továbbíthat információt úgy, hogy az illegális dekódoló semmi információt se kapjon (3. táblázat).

A titkosság az irodalomban csak az utóbbi években merült fel, mint a polgári célú hírközlésben is alapvetően fontos kérdés. Nagyon érdekes ebből a szempontból a „nyilvános kulcsú kriptorendszerek" (public key cryptosystems) gondolata, amely azon alapszik, hogy léteznek olyan „kis számítási bonyolultságú" operációk, melyek egymás inverzei, de egyik a másikból csak irreálisan nagy bonyolultságú számítással határozható meg. Bár ez matematikailag nincs bizonyítva, az ábrán illusztrált RSA rendszer általános vélemény szerint messzemenően eleget tesz mind a titkosság, mind a hamisíthatatlanság követelményének.

Reális rendszerek:	sok adó és vevő számuk változhat, cserélődnek nincs szinkronizmus effektív kódolás - dekódolás titkosság
Kiterjesztett spektrumú rendszer:	hibavalószínűség konkrét kódolási - dekódolási eljárásra, melyben az adó és vevő szinkronizált véletlenszám - generátort használ, többi adó-vevő nem ismeri: Győrfi - Vajda (1983)

2. táblázat

Áttekintés



Lehallgatott csatorna (wiretap channel)

H896-5

5. ábra

F és $G = F^{-1}$ "kis bonyolultságú operációk,

F-ből G nem határozható meg reális időn belül.

Rirest - Shamir - Adleman (1978):

p, q nagy prímszámok (100 - 100 bit), $n = pq$

$a\,b = c(p-1)(q-1) + 1$; nyílt kulcs: (n, a)

$m < n$, $F(m) = m^a \pmod n$ $G(k) = k^b \pmod n$

3. táblázat

Nyílt kulcsu kriptorendszer (public key cryptosystem)

H896-3T