Hírközléselmélet II.

Dr. Pap László

2011. november 25.

Tartalomjegyzék

1. fejezet

A diszkrét valószínűségelmélet rövid áttekintése

A fejezet célja azoknak a korábban megismert valószínűségszámítási fogalmaknak a felidézése és áttekintése, amelyek a hírközléselméletben fontos szerepet játszanak. Feltehető a kérdés, hogy a hírközlésben és az információátvitelben egyáltalán miért vetődnek fel valószínűségelméleti problémák. Ennek igen egyszerű a magyarázata:

- Az információátviteli rendszerekben az információ forrását mindig sztochasztikus forrásként célszerű modellezni, ugyanis csak akkor van értelme információátvitelről beszélni forrás és nyelő (adó és vevő) között, ha a nyelő nem rendelkezik előismerettel a küldött üzenettel kapcsolatban. Ha ugyanis előre ismerné a küldött üzenet aktuális tartalmát, akkor az üzenet átvitelére nem volna szükség. Egyszerűen fogalmazva az információ az üzenetnek éppen azzal a tulajdonságával kapcsolatos, hogy annak konkrét tartalma (a véletlen folyamat egyik realizációja) milyen mértékben képes a vevő (nyelő) "kétségeinek" az eloszlatására.
- Az információ átvitele során maga az átviteli csatorna is sztochasztikus modellekkel írható le abban az esetben, ha a csatornában a forrástól és nyelőtől függetlenül hibák jöhetnek létre az ott fellépő zavaró hatások (zaj, interferencia, stb.) következtében, és ezekről a hatásokról sincsenek előismeretek sem az adóban, sem a vevőben.

Vegyük ezután sorra a legfontosabb valószínűségelméleti fogalmakat.

- **Eseménytér**
  A valószínűségelmélet alapok felidézésének első lépéseként vezessük be az **eseménytér** (S) fogalmát, ami egy véletlen esemény kimeneteli lehetőségeinek a halmaza: $S = \{s_1, s_2, ..., s_n\}$, ahol S a biztos esemény, $\oslash$ a lehetetlen esemény. Ha a véletlen esemény kimeneteli lehetőségeinek a száma, n véges vagy megszámlálhatóan végtelen, akkor **diszkrét** eseménytérről beszélünk.
- **Esemény**
  Az **esemény** nem más, mint az S eseménytér egy részhalmaza.
- **Valószínűségi mérték**
  A **valószínűségi mérték** $(\Pr)$ az események egy valós függvénye, amelynek az értékkészlete a $[0,1]$ tartományba esik, és amely teljesíti az alábbi feltételeket:

$$\Pr(S) = 1 \tag{1.1}$$

$$\Pr(A \cup B) = \Pr(A) + \Pr(B), \quad \texttt{ha } A \cap B = \oslash \tag{1.2}$$

  Jegyezzük meg, hogy a fentiekből következik:

$$\Pr(\oslash) = 0. \tag{1.3}$$

- **Elemi esemény**
  Az eseménytér definíciójában szereplő s_i **az elemi esemény**, amelyre igaz, hogy:

$$p_i = \Pr(s_i), \quad i = 1,2,....,n \tag{1.4}$$

és

$$\sum_{i=1}^{n} p_i = 1. \tag{1.5}$$

- **Valószínűségi változó**
  A **diszkrét valószínűségi változó** az eseménytér leképzése egy véges vagy megszámlálhatóan végtelen halmazra, azaz nem más, mint az eseménytér egy függvénye. Az alábbiakban megadunk néhány példát a diszkrét valószínűségi változóra:
  $X(s)$ valós értékkészletű valószínűségi változó:

$$\begin{aligned} s_1 &\rightarrow -5, \\ s_2 &\rightarrow 0, \\ s_3 &\rightarrow +5. \end{aligned} \tag{1.6}$$

  $Y(s)$ Bool típusú valószínűségi változó:

$$\begin{aligned} s_1 &\rightarrow yes, \\ s_2 &\rightarrow yes, \\ s_3 &\rightarrow no. \end{aligned} \tag{1.7}$$

  $Z(s)$ vektor értékkészletű valószínűségi változó:

$$\begin{aligned} s_1 &\rightarrow [1,0], \\ s_2 &\rightarrow [0,1], \\ s_3 &\rightarrow [1,1]. \end{aligned} \tag{1.8}$$

  A valószínűségi változó értékkészlete az a tartomány, ahonnan a valószínűségi változó az értékeit felveheti. Példáink esetén ez az alábbi:

$$\begin{aligned} X(s) &\in \{-5,0,+5\}, \\ Y(s) &\in \{yes, no\}, \\ Z(s) &\in \{[1,0],[0,1][1,1]\}. \end{aligned} \tag{1.9}$$

- **Eloszlásfüggvény**
  Egy X diszkrét valószínűségi változó $P_X(x)$ **valószínűségi eloszlásfüggvényét** az alábbi formában adhatjuk meg:

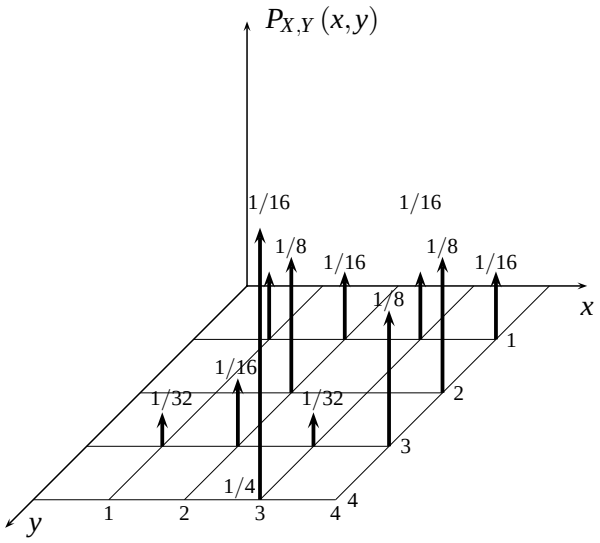
$$P_X(x) = \Pr(X = x) = \Pr(\{s; X(s) = x\}). \tag{1.10}$$

  A valószínűségi eloszlásfüggvényre teljesülnek az alábbi összefüggések:

$$P_X(x) \geq 0 \quad \forall\, x \in X(s) \tag{1.11}$$

és

$$\sum_{x} P_X(x) = 1. \tag{1.12}$$



1.1. ábra. A kétdimenziós együttes eloszlás illusztrációja

- **Vektor valószínűségi változó**
  Vektor valószínűségi változó esetén az eseménytér elemeihez több valószínűségi változót rendelünk, azaz megadunk több függvényt $X_1(s), X_2(s), ..., X_N(s)$, amelyeknek az értelmezési tartománya az eseménytér. Mindez nem jelent mást, mint azt, hogy egy adott elemi eseményhez egy valószínűségi változó vektor tartozik.
- **Együttes eloszlásfüggvény**
  Egy vektor valószínűségi változó **együttes eloszlásfüggvénye** az $(X_1(s), X_2(s), ..., X_N(s))$ vektor leképzése a $[0,1]$ tartományra az alábbi feltételek mellett:

$$P_{X_1,X_2,....,X_N}(x_1,x_2,....,x_N) = Pr(\{X_1 = x_1\} \cap \{X_2 = x_2\} \cap .... \cap \{X_N = x_N\}), \tag{1.13}$$

  és

$$P_{X_1,X_2,....,X_N}(x_1,x_2,....,x_N) \geq 0, \tag{1.14}$$

  valamint

$$\sum_{x_1}\sum_{x_2}....\sum_{x_N} P_{X_1,X_2,....,X_N}(x_1,x_2,....,x_N) = 1. \tag{1.15}$$

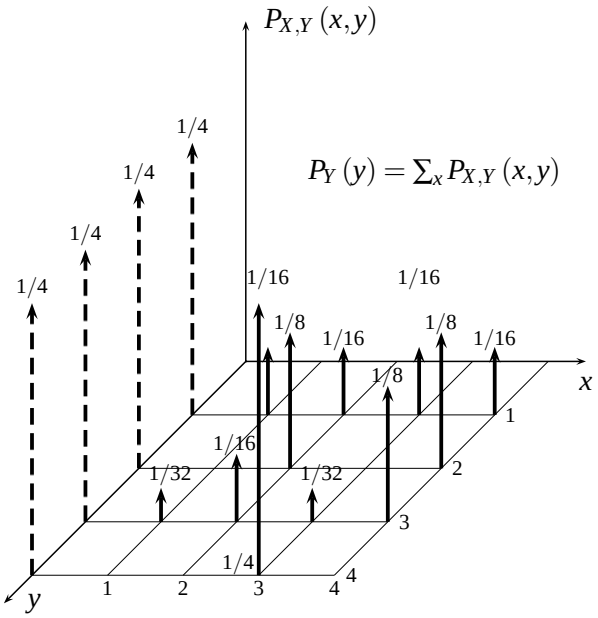
  Ez utóbbi kifejezés annyit jelent, hogy az együttes valószínűségi eloszlásfüggvény összege ("integrálja") a teljes értelmezési tartomány felett mindig egységnyi.
  Egy kétdimenziós vektor valószínűségi változó együttes eloszlását az 1.1. ábrán illusztráljuk.
- **Peremeloszlás**
  Egy kétdimenziós vektor valószínűségi változó eloszlásfüggvényéből egyszerű szummázással (integrálással) előállítható az egyik változó **peremeloszlása**:

$$\sum_{x_2} P_{X_1,X_2}(x_1,x_2) = P_{X_1}(x_1), \tag{1.16}$$

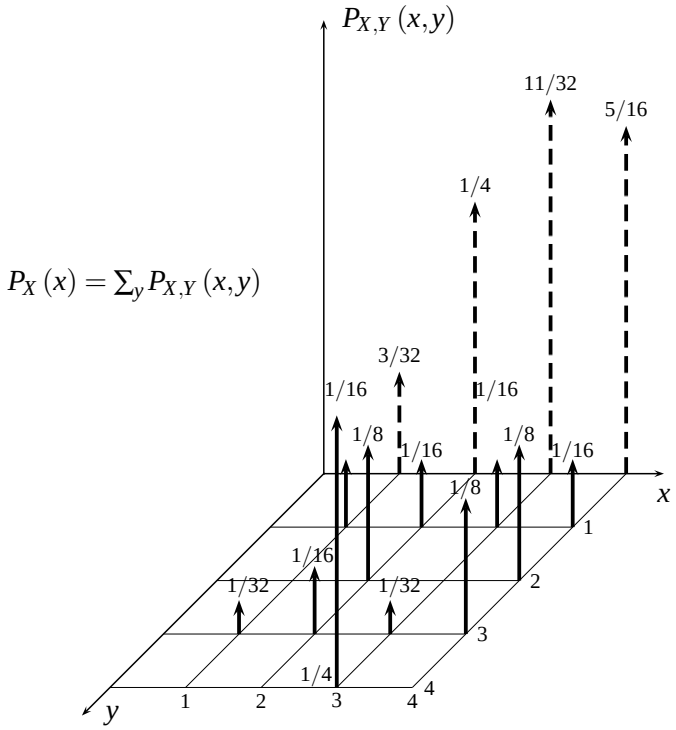
  amiből általánosan igaz, hogy

$$\sum_{x_2}....\sum_{x_N} P_{X_1,X_2,....,X_N}(x_1,x_2,....,x_N) = P_{X_1}(x_1). \tag{1.17}$$

  A kétdimenziós vektor valószínűségi változó peremeloszlásait a 1.2. és 1.3. ábrán szemléltetjük.



1.2. ábra. Az Y valószínűségi változó peremeloszlásának a számítása



1.3. ábra. Az X valószínűségi változó peremeloszlásának a számítása

- **Függetlenség**
  A valószínűségi változók **statisztikailag függetlenek** akkor, ha az együttes eloszlásfüggvényük az alábbi formában

$$P_{X_1,X_2,\ldots,X_N}(x_1,x_2,\ldots,x_N)=\prod_{i=1}^{N}P_{X_i}(x_i) \tag{1.18}$$

  a peremeloszlások szorzataként állítható elő.

- **Várható érték**
  Az X valószínűségi változó $F(X)$ valós értékkészletű függvényének a **várható értéke** az alábbi módon definiálható:

$$\mathbf{E}[F(X)]=\sum_{x}P_X(x)F(x), \tag{1.19}$$

  ami a függvénynek a valószínűségi eloszlással súlyozott összege.

- **Feltételes eloszlás**
  Az Y valószínűségi változó X-re vonatkozó **feltételes eloszlásának** definíciója az alábbi formában adható meg:

$$P_{Y|X}(y\mid x)=\frac{P_{Y,X}(y,x)}{P_X(x)}, \tag{1.20}$$

  ha

$$P_X(x)>0. \tag{1.21}$$

  A feltételes valószínűségi eloszlás az alábbi lényeges tulajdonságokkal rendelkezik:

$$P_{Y|X}(y\mid x)\geq 0 \quad \forall\, y\in Y(s), \tag{1.22}$$

  és igaz, hogy

$$\sum_{y}P_{Y|X}(y\mid x)=1. \tag{1.23}$$

  A valószínűségi változók feltételes eloszlását a 1.4. ábra szemlélteti.

- **Feltételes várható érték**
  A valószínűségi változók valós értékkészletű függvényének a **feltételes várható értéke** az alábbi módon definiálható:

$$\mathbf{E}[F(X)\mid A]=\sum_{x}\Pr(X=x\mid A)F(x), \tag{1.24}$$

  ahol A az eseménytér egy tetszőleges eseménye.
  Tételezzük fel, hogy az A esemény nem más, mint az, hogy az Y valószínűségi változó éppen az y_0 értéket veszi fel, azaz

$$A=\{Y=y_0\}. \tag{1.25}$$

  Ekkor az X valószínűségi változó $F(X)$ függvényének a feltételes várható értékét az

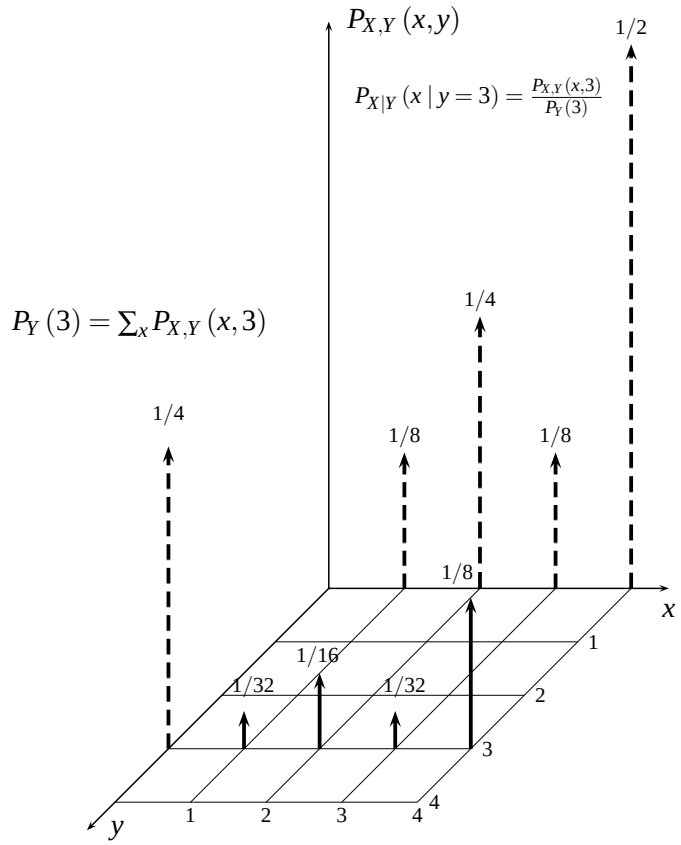
$$\mathbf{E}[F(X)\mid Y=y_0]=\sum_{x}F(x)P_{X|Y}(x\mid y_0) \tag{1.26}$$

  kifejezés adja meg.
  A kifejezés általánosabb értelmezéséhez vezessük be az X és Y valószínűségi változók egy valós értékkészletű

$$F(X,Y) \tag{1.27}$$

  függvényét. Ekkor e függvény feltételes várható értéke egy tetszőleges A esemény bekövetkeztének a feltételével könnyen megadható:

$$\mathbf{E}[F(X,Y)\mid A]=\sum_{x}\sum_{y}F(x,y)\Pr(\{X=x\}\cap\{Y=y\}\mid A). \tag{1.28}$$



1.4. ábra. Az X valószínűségi változó feltételes eloszlásának illusztrálása, ha $Y = 3$

Ha az A eseményt úgy választjuk meg, hogy $A = \{Y = y_0\}$, akkor a fenti kifejezés az alábbi formába írható:

$$\mathbf{E}\left[F(X,Y) \mid Y = y_0\right] = \sum_x \sum_{y=y_0} F(x,y_0) \Pr\left(\{X = x\} \cap \{Y = y_0\} \mid Y = y_0\right) =$$

$$= \sum_x F(x,y_0) P_{X|Y}(x \mid y_0). \tag{1.29}$$

Az $F(X,Y)$ függvény feltételes várható értéke ilyen esetben tehát úgy számítható, hogy a függvény értékét a $P_{X|Y_0}(x \mid y_0)$ feltételes eloszlással súlyozzuk. Ezen kívül a teljes várható érték tétel alapján tudjuk, hogy a feltételes várható érték várható értéke a (feltétel nélküli) várható érték, azaz:

$$\mathbf{E}\left[F(X,Y)\right] = \sum_y \mathbf{E}\left[F(X,Y) \mid Y = y\right] P_Y(y). \tag{1.30}$$

- **Konvergencia valószínűségben**
  Ha létezik egy valószínűségi változó sorozatunk, $Y_1, Y_2, ..., Y_i, ...$, és ez a sorozat **valószínűségben konvergál** az Y valószínűségi változóhoz, tehát

$$Y = p \lim_{N\to\infty} Y_N, \tag{1.31}$$

akkor teljesül az alábbi összefüggés:

$$\lim_{N\to\infty} \Pr\left(\{|Y - Y_N| < \varepsilon\}\right) = 1. \tag{1.32}$$

Egyszerűen fogalmazva ez annyit jelent, hogy az $Y_1, Y_2, ..., Y_i, ...$ valószínűségi változó sorozat akkor konvergál valószínűségben az Y valószínűségi változóhoz, ha minden nagy N esetén lényegében

biztos az, hogy az Y_N valószínűségi változó az Y valószínűségi változóhoz igen közel veszi fel az értékeit.

A valószínűségben konvergáló sorozatokra talán az egyik legismertebb példa **a nagy számok gyenge törvénye**, ahol az $X_1, X_2, ..., X_N$ független azonos eloszlású valós értékkészletű valószínűségi változók számtani átlaga

$$Y_N = \frac{X_1 + X_2 + ... + X_N}{N} \tag{1.33}$$

egy valószínűséggel tart az $\{X_i\}$ valószínűségi változók m közös várható értékéhez, azaz:

$$p \lim_{N \to \infty} Y_N = m. \tag{1.34}$$

2. fejezet

A digitális információ Shannon féle mértéke

A digitális információ mértékének a fogalmát **Claude E. Shannon** vezette be híres "The Mathematical Theory of Communication" című cikkében, amely 1948-ban jelent meg a Bell System Technical Journal-ban (Vol. 27, July and October, 1948, pp. 379-423 és pp. 623-656). Bár Shannon elsőségét senki sem kérdőjelezheti meg, érdekes, hogy már húsz évvel korábban **R. V. L. Hartley** is megjelentetett egy hasonló témájú cikket, "Transmission of Information"' címmel ugyancsak ebben a folyóiratban (BSTJ, Vol. 3, July, 1928, pp. 535-564), és már ő is foglalkozott az információ mértékének meghatározásával. Az információ mérésével kapcsolatos fogalomrendszer pontosabb megértéséhez érdemes először megismerni a Hartley által bevezetett információmértéket.

2.1. A Hartley féle információmérték

Hartley szerint az X diszkrét valószínűségi változóhoz (szimbólumhoz) az

$$I(X) = \log_b(L) \tag{2.1}$$

információmennyiség rendelhető, ahol L az X valószínűségi változó értékkészletének nagysága, az a szám, amely megmondja, hogy a valószínűségi változó (szimbólum) éppen hány lehetséges értéket vehet fel, b pedig a logaritmus alapja. Az ötlet lényege igen világos és egyszerű. Hartley úgy gondolkodott, hogy a valószínűségi változó (szimbólum) és a vele összefüggő véletlen esemény n-szeri megismétlése esetén az információ mennyiségének éppen n-szer nagyobbnak kell lenni az egy szimbólum által hordozott információ mennyiségénél. Ugyanakkor nyilvánvaló, hogy ha egy szimbólum éppen L értéket vehet fel, akkor egy n szimbólumból álló vektor értékkészletének a mérete éppen L^n , vagyis az $\mathbf{X} = (X_1, X_2, ..., X_n)$ vektor által hordozott összes információ Hartley definíciója szerint

$$I(\mathbf{X}) = n\log_b(L), \tag{2.2}$$

ami jól mutatja, hogy a Hartley az általa bevezetett információmértéknél célszerűen használta a logaritmus függvényt, mivel így az egyes független szimbólumok információtartalma összeadódik. Mindezek mellett érdemes megjegyezni, hogy Hartley azt javasolta, hogy amennyiben a logaritmus alapja 2, akkor az információ egysége a **bit** legyen.

A Hartley által bevezetett információmérték értelmezéséhez nézzünk meg egy illusztratív példát (lásd 2.1. ábra). Legyen a véletlen esemény az, hogy egy dobozból, amelyben négy golyó van egyet véletlenszerűen kihúzunk, és a valószínűségi változó legyen a golyóra írott 1 vagy 0. Tekintsünk két esetet: a.) amikor a négy golyó közül kettőn 0 és kettőn 1, illetve b.) amikor a négy golyó közül három golyón 0 és egyen 1 szerepel.

a.) *b.*)

2.1. ábra. A Hartley mérték illusztrálása

Gondolatban hajtsuk végre a kijelölt feladatot, és $b = 2$ értéket feltételezve határozzuk meg a valószínűségi változók által hordozott információ mértékét a Hartley féle definíció felhasználásával. A feladat rendkívül egyszerű, hiszen a valószínűségi változó értékkészlete mind az a., mind a b. esetben $L = 2$, ami miatt az információ mértéke pontosan egyenlő 1-gyel, függetlenül attól, hogy az adott valószínűségi változónak milyen a statisztikája. A Hartley-mérték tehát nem veszi figyelembe a valószínűségeket, ami jól érezhető hiba, hiszen nyilvánvaló, hogy a két eset között jelentős különbség van.

2.2. A Shannon féle információmérték

Térjünk vissza az előbbi példára, és próbáljuk feloldani a korábban említett ellentmondást, azaz vegyük figyelembe az események valószínűségét is. Foglalkozzunk a b.) esettel, ahol a golyókon egy 1-es, és három 0-ás szerepel. Ha azt az eseményt vizsgáljuk, hogy a kihúzott golyón a címke 1-es, akkor tudjuk, hogy a véletlen esemény (egy golyó véletlen kiválasztása négy közül) négy lehetséges kimenetele közül csak egy van ilyen. Az is nyilvánvaló, hogy a valószínűségi változó éppen ekkora eséllyel venné fel az 1 értéket akkor is, ha a négy különböző golyóra négy különböző szám volna írva, és ezek közül csak az egyiken lenne 1-es. A Hartley által bevezetett információmérték ez utóbbi esetben éppen

$$\log_2(4) = 2 \texttt{ bit} \tag{2.3}$$

lenne, mivel a valószínűségi változó értékkészletének a mérete (számossága) 4.

A 0 címkéjű golyók kihúzását vizsgálva megállapíthatjuk, hogy most az a.) esettel szemben a véletlen esemény négy lehetséges kimenetele közül három olyan van, amikor a valószínűségi változó értéke (a golyó cimkéje) 0. A fenti meggondoláshoz hasonlóan ezt úgy is felfoghatjuk, mintha most $4/3$ "lehetőség" közül egyet választanánk, vagyis ilyenkor a Hartley által bevezetett információmérték éppen

$$\log_2(4/3) = 0.415 \texttt{ bit} \tag{2.4}$$

lenne.

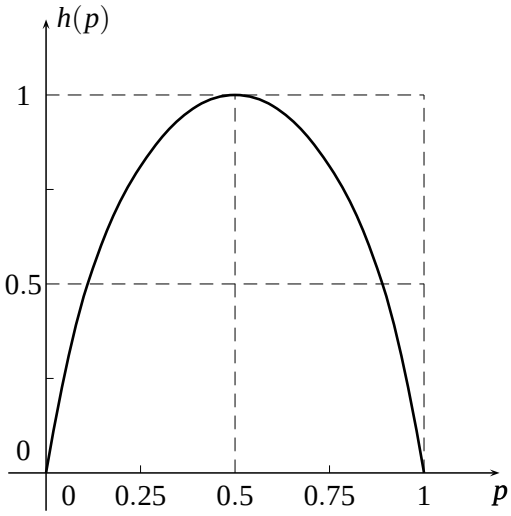
Ezekre a megfontolásokra támaszkodva Shannon a valószínűségi változó által hordozott átlagos információ értékét a fent kiszámított értékek átlagában határozta meg, vagyis szerinte az információ mértéke

$$\frac{1}{4}\log_2(4) + \frac{3}{4}\log_2(4/3) = 0.811 \texttt{ bit}. \tag{2.5}$$

Mindezt általánosítva a Shannon féle információmértéket az alábbi alakban adhatjuk meg:

$$-\sum_{i=1}^{L} p_i \log_2(p_i) \qquad p_i \neq 0. \tag{2.6}$$

2.1. Definició



2.2. ábra. A bináris entrópia függvény

Egy X valószínűségi változó **"bizonytalanságának" a mértéke, entrópiája** az alábbi értékkel adható meg:

$$H(X) = -\sum_{x:\, P_X(x)\neq 0} P_X(x)\log_b\left(P_X(x)\right) = \mathbf{E}\left[-\log_b\left(P_X(x)\right)\right], \tag{2.7}$$

azaz az entrópia a valószínűség b alapú logaritmusa minusz egyszeresének a várható értéke, de a várható érték számításakor a 0 valószínűségű eseményekkel nem kell számolni.

Természetesen a fenti definíció bármilyen valószínűségi változó esetére általánosítható, tehát például egy kétdimenziós $[X,Y]$ vektor valószínűségi változó esetén

$$H(XY) = \mathbf{E}\left[-\log_b\left(P_{X,Y}(x,y)\right)\right] = -\sum_{x,y:\, P_{X,Y}(x,y)\neq 0} P_{X,Y}(x,y)\log_b\left(P_{X,Y}(x,y)\right). \tag{2.8}$$

Példa: A bináris entrópia függvény.

Legyen az X valószínűségi változó bináris, azaz két különböző értéket vegyen fel, x_1-et és x_2-t, emellett legyen

$$\Pr(X = x_1) = P_X(x_1) = p \quad \text{és} \quad \Pr(X = x_2) = P_X(x_2) = 1-p. \tag{2.9}$$

Ekkor a valószínűségi változó entrópiája (ha $b = 2$)

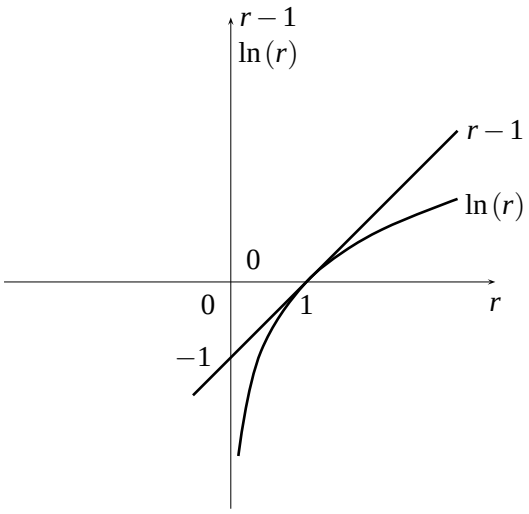
$$H(X) = -p\log_2(p) - (1-p)\log_2(1-p) = h(p). \tag{2.10}$$

A bináris entópia függvényt a 2.2. ábrán adtuk meg. Az ábra jól mutatja, hogy a biztos esemény (ha $p = 0$ vagy $p = 1$) entrópiája nulla, és az egyenletes eloszláshoz ($p = 0.5$) tartozik a legnagyobb bizonytalanság (entrópia).

2.3. A Shannon féle információmértékkel kapcsolatos néhány összefüggés és egyenlőtlenség

A fejezetben szereplő állítások megalapozásához először vezessük be az úgynevezett **információelméleti egyenlőtlenséget**, amely több további összefüggés bizonyításánál jelent igen hasznos segítséget.

2.1. Segédtétel



2.3. ábra. Az információelméleti egyenlőtlenség illusztrációja

Az információelméleti egyenlőtlenség szerint igaz az alábbi összefüggés:

$$\log(r) \leq (r-1)\log(e), \tag{2.11}$$

és az egyenlőség akkor és csak akkor áll fent, ha $r = 1$.

Bizonyítás

Tudjuk, hogy

$$\ln(r) \leq r-1, \tag{2.12}$$

és

$$\frac{d}{dr}(\ln(r)) = \frac{1}{r} = \begin{cases} > 1, & \texttt{ha} \quad r < 1 \\ < 1, & \texttt{ha} \quad r > 1 \end{cases}, \tag{2.13}$$

így

$$\log_b(r) \leq (r-1)\log_b(e), \tag{2.14}$$

és az egyenlőség csak az $r = 1$ pontban áll fent, amivel a segédtételt bebizonyítottuk.

A 2.3. ábrán a fenti állítást illusztrációját is megadtuk.

2.1. Tétel

Ha adott egy X diszkrét valószínűségi változó, amely L különböző értéket vehet fel, akkor a valószínűségi változó bizonytalansági (entrópia) függvényére igaz az alábbi egyenlőtlenség:

$$0 \leq H(X) \leq \log_b(L), \tag{2.15}$$

és a jobboldali egyenlőség akkor és csak akkor áll fent, ha $P_X(x) = 1/L$.

Bizonyítás

A következőkben az egyszerűbb jelölések kedvéért az alábbi egyszerűsítést fogjuk alkalmazni:

$$-P_X(x)\log(P_X(x)) = \begin{cases} = 0, & \texttt{ha} \quad P_X(x) = \ 0 \ \texttt{vagy} \ 1 \\ > 0, & \texttt{ha} \quad 0 < P_X(x) < 1 \end{cases}, \tag{2.16}$$

és a logaritmus b alapjának ismételt feltüntetésétől is eltekintünk.

Ezeket felhasználva a tétel az alábbi módon bizonyítható:

$$H(X) - \log(L) = -\sum_x (P_X(x)\log(P_X(x))) - \log(L) = \sum_x P_X(x)\left[-\log(P_X(x)) - \log(L)\right] =$$

$$= \sum_x P_X(x) \left[\log\left(\frac{1}{LP_X(x)} \right) \right] \leq \sum_x P_X(x) \left[\frac{1}{LP_X(x)} - 1 \right] \log(e) =$$

$$= \left[\sum_x \frac{1}{L} - \sum_x P_X(x) \right] \log(e) = (1-1)\log(e) = 0, \tag{2.17}$$

és az egyenlőség az információelméleti egyenlőtlenség alapján akkor és csak akkor áll fent, ha

$$\frac{1}{LP_X(x)} - 1 = 0\,; \quad \texttt{azaz} \quad P_X(x) = \frac{1}{L}\,. \tag{2.18}$$

A továbbiakban a jelölések egyszerűsítése érdekében $P_X(x)$ helyett egyszerűen $P(x)$-et fogunk írni.

2.2. Definíció

Az X diszkrét valószínűségi változó **feltételes bizonytalansága (feltételes entrópiája)** abban az esetben, ha egy másik Y valószínűségi változó éppen a $Y = y$ értéket veszi fel, az alábbi módon határozható meg:

$$H(X \mid Y = y) = - \sum_{x;\ P(x|y)\neq 0} P(x \mid y) \log(P(x \mid y))\,. \tag{2.19}$$

Megjegyzendő, hogy ez a kifejezés felírható úgy is, mint a valószínűségi változó egy függvényének a várható értéke, azaz:

$$H(X \mid Y = y) = \mathbf{E}[-\log(P(X \mid Y = y))]\,. \tag{2.20}$$

A **feltételes entrópia** értelmezéséhez idézzük fel az X és Y valószínűségi változók egy $F(X,Y)$ függvénye feltételes várható értékének a definícióját abban az esetben, ha az egyik valószínűségi változó éppen az $Y = y$ értéket veszi fel. Ilyenkor

$$\mathbf{E}[F(X,Y \mid Y = y)] = \sum_{x;\ P(x|y)\neq 0} P(x \mid y) F(x,y)\,, \tag{2.21}$$

és az $F(X,Y)$ függvény feltétel nélküli várható értékét az

$$\mathbf{E}[F(X,Y)] = \sum_{y;\ P(y)\neq 0} \mathbf{E}[F(X,Y \mid Y = y)] P_Y(y) \tag{2.22}$$

határozza meg.

A 2.1. Tétel következménye

Ha X egy L kimeneti lehetőséggel rendelkező diszkrét valószínűségi változó, akkor:

$$0 \leq H(X \mid Y = y) \leq \log(L)\,, \tag{2.23}$$

és a baloldali egyenlőség akkor és csak akkor áll fent, ha valamilyen x értékre $P(x \mid y) = 1$, és a jobboldali egyenlőség akkor és csak akkor igaz, ha $P(x \mid y) = 1/L$.

2.3. Definíció

Egy X diszkrét valószínűségi változó **feltételes bizonytalansági (entrópia) függvénye**, ha egy másik Y diszkrét valószínűségi változó ismert, az alábbi kifejezéssel határozható meg:

$$H(X \mid Y) = \sum_{y;\ P(y)\neq 0} P(y) H(X \mid Y = y)\,, \tag{2.24}$$

ami más formában írva nem más, mint

$$H(X \mid Y) = \mathbf{E}[-\log(P(X \mid Y))] = - \sum_{x,y;\ P(x,y)\neq 0} P(x,y) \log(P(x \mid y))\,. \tag{2.25}$$

A kifejezés alapján az X diszkrét valószínűségi változó feltételes bizonytalansága (entrópiája), ha az Y valószínűségi változó ismert a feltételes eloszlás logaritmusa minusz egyszeresének a várható értéke. A feltételes entrópiára érvényes az alábbi tétel.

2.2. Tétel

Két diszkrét valószínűségi változó esetén igaz, hogy

$$0 < H(X \mid Y) \leq H(X), \tag{2.26}$$

és a jobboldali egyenlőség akkor és csakis akkor áll fent, ha X és Y statisztikailag függetlenek egymástól.

Bizonyítás

$$H(X \mid Y) - H(X) = \mathbf{E}\left[-\log\left(P(X \mid Y)\right)\right] - \mathbf{E}\left[-\log\left(P(X)\right)\right] =$$

$$= \mathbf{E}\left[-\log\left(P(X \mid Y)\right) + \log\left(P(X)\right)\right] = \mathbf{E}\left[\log\left(\frac{P(X)}{P(X \mid Y)}\right)\right] = \mathbf{E}\left[\log\left(\frac{P(X)P(Y)}{P(X,Y)}\right)\right] =$$

$$= \sum_{x,y;\ P(x,y)\neq 0} P(x,y)\log\left(\frac{P(x)P(y)}{P(x,y)}\right) \leq \sum_{x,y;\ P(x,y)\neq 0} P(x,y)\left(\frac{P(x)P(y)}{P(x,y)} - 1\right)\log(e) =$$

$$= \sum_{x,y;\ P(x,y)\neq 0} \left(P(x)P(y) - P(x,y)\right)\log(e) = (1-1)\log(e) = 0, \tag{2.27}$$

és az információelméleti egyenlőtlenség alapján az egyenlőség akkor és csak akkor áll fent, ha

$$P(x,y) = P(x)P(y), \tag{2.28}$$

vagyis X és Y függelenek egymástól. Ezzel a tételt bebizonyítottuk.

A feltételes entrópia fogalmát a 2.4. ábrán illusztráljuk.

Megjegyzések a 2.2. Tételhez

A korábbi eredmények alapján nyilvánvaló, hogy:

$$H(X \mid Y) \leq \log(L), \tag{2.29}$$

és az egyenlőség akkor és csak akkor áll fent, ha X egyenletes eloszlású $(P(x) = 1/L)$, és a két valószínűségi változó független egymástól.

A feltételes entrópiára érvényes a

$$H(X \mid Y) \geq 0, \tag{2.30}$$

és az egyenlőség akkor és csak akkor áll fent, ha minden y; $P(y) \neq 0$ esetén van egy olyan x érték, melynél $P(x) = 1$. Ekkor Y egyértelműen meghatározza az X mindenkori értékét, azaz X Y determinisztikus függvénye, mert minden $Y = y$ értékhez egy és csakis egy $X = x$ érték tartozik.

A feltételes entrópia fogalmát és számítási módját két valószínűségi változó esetén a 2.4. ábrán illusztráljuk.

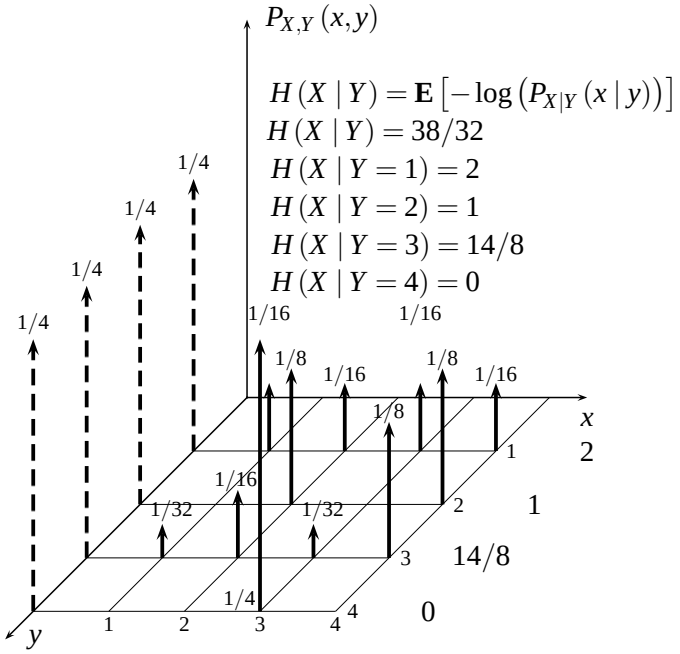
A feltételes entrópia természetesen általánosítható kettőnél több valószínűségi változó esetére is, például három valószínűségi változó esetében értelemszerűen érvényes az alábbi összefüggés:

$$H(X \mid YZ) = \mathbf{E}\left[-\log\left(P_{X|YZ}(X \mid YZ)\right)\right] = -\sum_{x,y,z;\ P(x,y,z)\neq 0} P(x,y,z)\log\left(P(x \mid y,z)\right). \tag{2.31}$$

2.4. Definíció

Az X diszkrét valószínűségi változó feltételes bizonytalansága (feltételes entrópiája) abban az esetben, ha az Y valószínűségi változó ismert és a Z valószínűségi változó éppen a $Z = z$ értéket veszi fel, az alábbi kifejezéssel határozható meg:

$$H(X \mid Y, Z = z) = \mathbf{E}\left[-\log\left(P_{X|YZ}(X \mid Y, Z = z)\right)\right] \tag{2.32}$$



2.4. ábra. Az X valószínűségi változó feltételes entrópiájának az illusztrálása

vagy

$$H(X \mid Y, Z=z) = -\sum_{x,y;\ P(x,y|z)\neq 0} P(x,y \mid z)\log\left(P(x \mid y,z)\right). \tag{2.33}$$

A 2.2. Tétel 1. következménye

A 2.2. tételből egyenesen következik, hogy fennáll az alábbi egyenlőtlenség:

$$H(X \mid Y, Z=z) \leq H(X \mid Z=z), \tag{2.34}$$

s az egyenlőség akkor és csak akkor áll fent, ha az X és Y valószínűségi változók feltételesen függetlenek, azaz

$$P(x,y \mid z) = P(x \mid z)P(y \mid z), \tag{2.35}$$

minden x és y értékre.

Megjegyezzük, hogy a korábbi definíciók alapján az X diszkrét valószínűségi változó feltételes entrópiája, ha az Y és Z valószínűségi változók ismertek a következőképpen határozható meg:

$$H(X \mid YZ) = \mathbf{E}\left[-\log\left(P_{X|YZ}(X \mid YZ)\right)\right] = \sum_{z;\ P(z)\neq 0} P(z)H(X \mid Y, Z=z) =$$

$$= -\sum_{x,y,z;\ P(x,y,z)\neq 0} P(x,y,z)\log\left(P(x \mid y,z)\right). \tag{2.36}$$

A 2.2. Tétel 2. következménye

A 2.2. Tétel alapján egyszerűen belátható az is, hogy

$$H(X \mid YZ) \leq H(X \mid Y), \tag{2.37}$$

és az egyenlőség akkor és csak is akkor áll fent, ha az X és Y valószínűségi változók függetlenek Z-től, azaz

$$P(x,y,z) = P(x,y)P(z). \tag{2.38}$$

Mindez annyit jelent, hogy egy diszkrét valószínűségi változó feltételes bizonytalansága (feltételes entrópiája) egy újabb feltétel megjelenése esetén nem növekedhet.

A fenti eredményeket érdemes kiegészíteni egy érdekes összefüggéssel, amely egy vektor valószínűségi változó entrópiájának kiszámítását feltételes entrópiák addíciójára vezeti vissza. Tekintsük az $(X_1, X_2, ..., X_N)$ vektor valószínűségi változót, és határozzuk meg annak entrópiáját, azaz számítsuk ki a

$$H(X_1, X_2, ..., X_N) = \mathbf{E}\left[-\log\left(P_{X_1,X_2,...,X_N}(X_1, X_2, ..., X_N)\right)\right] \tag{2.39}$$

értéket. Felhasználva a feltételes valószínűség korábban ismertetett definícióját a fenti kifejezés a

$$\mathbf{E}\left[-\log\left(P_{X_1,X_2,...,X_N} P(X_1, X_2, ..., X_N)\right)\right] =$$

$$= \mathbf{E}\left[-\log\left\{P_{X_1}(X_1) P_{X_2|X_1}(X_2 \mid X_1) P_{X_3|X_2,X_1}(X_3 \mid X_2, X_1) ... P_{X_N|X_{N-1},...,X_1}(X_N \mid X_{N-1}, ..., X_1)\right\}\right], \tag{2.40}$$

amiből egyenesen következik, hogy

$$\mathbf{E}\left[-\log\left(P_{X_1,X_2,...,X_N} P(X_1, X_2, ..., X_N)\right)\right] =$$

$$= \mathbf{E}\left[-\log\left(P_{X_1}(X_1)\right)\right] + \mathbf{E}\left[-\log\left(P_{X_2|X_1}(X_2 \mid X_1)\right)\right] + ... + \mathbf{E}\left[-\log\left(P_{X_N|X_{N-1},...,X_1}(X_N \mid X_{N-1}, ..., X_1)\right)\right], \tag{2.41}$$

így az $(X_1, X_2, ..., X_N)$ vektor valószínűségi változó entrópiája valóban előállítható additív alakban, miszerint:

$$H(X_1, X_2, ..., X_N) = H(X_1) + H(X_2 \mid X_1) + H(X_3 \mid X_2, X_1) + ... + H(X_N \mid X_{N-1}, ..., X_1). \tag{2.42}$$

Példa

A fent ismertetett fogalmak jobb megértése érdekében vizsgáljunk meg egy egyszerű példát. Tekintsünk egy (X, Y, Z) vektor valószínűségi változót, amely egyenletes eloszlással vesz fel az alábbi értékeket: $[0,0,0]$ $[0,1,0]$ $[1,0,0]$ $[1,0,1]$, és számítsunk ki néhány érdekes paramétert. Az adatokból nyilvánvaló, hogy

$$P_X(0) = P_X(1) = \frac{1}{2}, \tag{2.43}$$

hiszen az X valószínűségi változó egyenletes eloszlással vesz fel az 1 és 0 értéket.

A bináris entrópiafüggvény alkalmazásával:

$$H(X) = h(1/2) = 1. \tag{2.44}$$

Az Y valószínűségi változó feltételes entrópiáája, ha az X valószínűségi változó ismert, az alábbi módon határozható meg:

$$P_{Y|X}(0 \mid 1) = 1, \quad \texttt{ezért } H(Y \mid X = 1) = 0 \,\texttt{bit} \tag{2.45}$$

és

$$P_{Y|X}(0 \mid 0) = 1/2, \quad \texttt{ezért } H(Y \mid X = 0) = 1 \,\texttt{bit}, \tag{2.46}$$

amiből

$$H(Y \mid X) = \frac{1}{2} H(Y \mid X = 1) + \frac{1}{2} H(Y \mid X = 0) = \frac{1}{2} \,\texttt{bit}. \tag{2.47}$$

Vizsgáljuk meg ezután a Z valószínűségi változó feltételes entrópiáját, ha az X és Y valószínűségi változó páros ismert. Ehhez szükségünk van a $P_{Z|X,Y}(z \mid x, y)$ feltételes eloszlás értékeire. A korábbi adatok alapján:

$$P(z \mid x, y) = 1 \quad \texttt{ha } (x, y, z) = (0, 0, 0), \tag{2.48}$$

$$P(z \mid x, y) = 1 \quad \texttt{ha } (x, y, z) = (0, 1, 0), \tag{2.49}$$

és

$$P(z \mid x, y) = \frac{1}{2} \quad \texttt{ha } (x, y, z) = (1, 0, 0) \quad \texttt{vagy } (x, y, z) = (1, 0, 1). \tag{2.50}$$

Ezeknek az adatoknak a felhasználásával:

$$H(Z \mid X=0,Y=0)=0, \tag{2.51}$$

$$H(Z \mid X=0,Y=1)=0, \tag{2.52}$$

$$H(Z \mid X=1,Y=0)=1 \texttt{ bit}, \tag{2.53}$$

vagyis a keresett feltételes entrópia:

$$H(Z \mid X,Y)=\frac{1}{4}H(Z \mid X=0,Y=0)+\frac{1}{4}H(Z \mid X=0,Y=1)+\frac{1}{2}H(Z \mid X=1,Y=0)=\frac{1}{2} \texttt{ bit}. \tag{2.54}$$

A három valószínűségi változó együttes entrópiáját a láncszabály alkalmazásával az alábbi módon számíthatjuk ki:

$$H(X,Y,Z)=H(X)+H(Y \mid X)+H(Z \mid X,Y)=1+\frac{1}{2}+\frac{1}{2}=2 \texttt{ bit}. \tag{2.55}$$

Érdekes megjegyezni, hogy

$$H(Y)=h(1/4)=0.811 \texttt{ bit}, \tag{2.56}$$

és természetesen igaz, hogy

$$H(Y \mid X)=\frac{1}{2}<H(Y)=0.811 \texttt{ bit}. \tag{2.57}$$

Ugyanakkor fontos megállapítani, hogy

$$H(Y \mid X=0)=1>H(Y)=0.811 \texttt{ bit}, \tag{2.58}$$

vagyis a feltételes entrópia értéke egy adott feltétel esetén nagyobb lehet, mint a feltétel nélküli entrópia, tehát a korábban ismertetett egyenlőtlenség csak az átlagos feltételes entrópiára érvényes, ahogyan azt a 2.2. Tételben kimondtuk.

2.4. A kölcsönös információ

A Shannon féle információmérték felhasználásával bevezethetjük két valószínűségi változó **kölcsönös információjának** a fogalmát.

2.5. Definíció

Két diszkrét valószínűségi változó, X és Y kölcsönös információja definíció szerint az alábbi érték:

$$I(X;Y)=H(X)-H(X \mid Y). \tag{2.59}$$

A kölcsönös információ értéke független a változók sorrendjétől, mivel:

$$H(X,Y)=H(X)+H(Y \mid X)=H(Y)+H(X \mid Y), \tag{2.60}$$

így

$$H(X)-H(X \mid Y)=H(Y)-H(Y \mid X), \tag{2.61}$$

azaz

$$I(X;Y)=I(Y;X). \tag{2.62}$$

Példa

Visszatérve a korábban vizsgált példára, ahol egy háromdimenziós diszkrét vektor valószínűségi változó paramétereit határoztuk meg, az X és Y valószínűségi változók kölcsönös információja egyszerűen számítható, mivel:

$$H(Y)=0.811 \texttt{ bit}, \tag{2.63}$$

és

$$I(X;Y) = H(Y) - H(Y \mid X) = 0.811 - 0.5 = 0.311 \quad \texttt{bit}. \tag{2.64}$$

2.6. Definíció

Vezessük be ezután az X és Y diszkrét valószínűségi változók közötti feltételes kölcsönös információt, akkor, ha egy harmadik Z diszkrét valószínűségi változó éppen a $Z = z$ értéket veszi fel:

$$I(X;Y \mid Z = z) = H(X \mid Z = z) - H(X \mid Y, Z = z). \tag{2.65}$$

A korábbi ismeretek alapján könnyen eljuthatunk a feltételes kölcsönös információ fogalmához az alábbi definíció bevezetésével:

2.7. Definíció

Az X és Y diszkrét valószínűségi változók közötti feltételes kölcsönös információt, akkor, ha egy harmadik Z diszkrét valószínűségi változó ismert az alábbi összefüggéssel definiáljuk:

$$I(X;Y \mid Z) = H(X \mid Z) - H(X \mid Y, Z), \tag{2.66}$$

ami nem más, mint

$$I(X;Y \mid Z) = \mathbf{E}[I(X;Y \mid Z = z)] = \sum_{z;P(z)\neq 0} P(z)\, I(X;Y \mid Z = z). \tag{2.67}$$

Természetesen a feltételes kölcsönös információ értéke sem függ a változók sorrendjétől, azaz

$$I(X;Y \mid Z) = I(Y;X \mid Z). \tag{2.68}$$

A kölcsönös információ lehetséges értéktartományát a 2.3. Tétel határozza meg.

2.3. Tétel

Két diszkrét valószínűségi változó, X és Y kölcsönös információjára érvényes az alábbi egyenlőtlenség:

$$0 \leq I(X;Y) \leq \min[H(X), H(Y)], \tag{2.69}$$

és a baloldali egyenlőség akkor és csak akkor áll fent, ha X és Y statisztikailag függetlenek egymástól, a jobboldali egyenlőség pedig akkor és csak akkor áll fent, ha Y egyértelműen meghatározza X-et, és/vagy X egyértelműen meghatározza Y-t.

Bizonyítás

A bizonyítás lényegében a kölcsönös információ definíciójából következik, mivel a baloldali egyenlőség esetén fenn kell állni annak, hogy

$$H(X \mid Y) = H(X), \tag{2.70}$$

ami akkor és csak akkor igaz, ha X és Y statisztikailag függetlenek egymástól. A jobboldali egyenlőség esetén pedig

$$H(X \mid Y) = 0, \tag{2.71}$$

ami akkor és csak akkor igaz, ha Y egyértelműen meghatározza X-et. Ilyenkor azonban az is igaz, hogy

$$I(X;Y) = I(Y;X) = H(X) = H(Y) - H(Y \mid X), \tag{2.72}$$

amiből nyilvánvaló, hogy

$$H(X) \leq H(Y). \tag{2.73}$$

Természetesen a fenti bizonyításnál a változók sorrendje felcserélhető. Megjegyzendő, hogy abban az esetben, ha X és Y kölcsönösen egyértelműen meghatározzák egymást, akkor

$$H(X) = H(Y). \tag{2.74}$$

Ezzel a tételt bebizonyítottuk.

A 2.3. Tétel értelemszerűen igaz a feltételes kölcsönös információra is, miszerint:

$$0 \leq I(X;Y \mid Z=z) \leq \min\left[H(X \mid Z=z), H(Y \mid Z=z)\right], \tag{2.75}$$

és

$$0 \leq I(X;Y \mid Z) \leq \min\left[H(X \mid Z), H(Y \mid Z)\right]. \tag{2.76}$$

3. fejezet

A digitális információk forráskódolása

A fejezet célja az optimális forráskódolási eljárások áttekintése, és annak igazolása, hogy a Shannon féle információmérték valóban jól alkalmazható gyakorlati feladatok megoldására is.

3.1. Prefix-free kódok és a Kraft-egyenlőtlenség

Vizsgáljuk meg a 3.1. ábrán látható egyszerű forráskódolási modellt. Legyen

- U a forrás által generált valószínűségi változó, amelynek az értékkészlete $\{u_1, u_2, ..., u_K\}$,
- X_i a kód egy szimbóluma (betűje), amely egy D-szintű ABC-ből veszi fel az értékeit, azaz az értékkészlete $\{0, 1, ..., D-1\}$,
- $\mathbf{Z}$ a kódoló által előállított változó hosszúságú kódszó,
- és W a kód hosszát mérő valószínűségi változó.

A forráskódoló működésének a minőségét a $\mathbf{E}[W]$-vel, a kódszó átlagos hosszúságával mérjük. Annál jobban működik a forráskódoló, minél rövidebb az általa kibocsátott kódszavak átlagos hosszúsága, a

$$\mathbf{E}[W] = \sum_{i=1}^{K} w_i P_U(u_i), \tag{3.1}$$

ahol $P_U(u_i)$a forrás valószínűségi eloszlása, w_i pedig az u_i üzenethez tartozó

$$\mathbf{z}_i = \left\{ x_{i_1}, x_{i_2}, ..., x_{i_{w_i}} \right\} \tag{3.2}$$

kódszó hossza.

Követelmények

- A forráskódolónak olyan kódszavakat kell előállítani, amelyek egyértelműen kötődnek egy-egy üzenethez. Ez azt jelenti, hogy ugyanaz a kódszó nem tartozhat egynél több üzenethez.
- Nem lehet egyetlen olyan kódszó sem, amelyik előzménye, prefix-e valamilyen másik kódszónak. Ha ez a feltétel nem teljesül, akkor az egymást követő kódszavak egyértelmű felismerhetősége nem megoldható.

A prefix-free kódok értelmezéséhez tekintsünk egy illusztratív példát (lásd a 3.2. ábrát).

Példa

A 3.2. ábrán két egyszerű forráskódolót mutatunk be, amelyek egy három kimenetű forrás üzeneteit kódolják. Az **A** kódoló által előállított kódszavak egyike sem előzménye (folytatása) egy másik kódszónak, míg a **B** kódoló esetében az u_1 üzenethez tartozó $\mathbf{z}_1 = (1)$ kódszó előzménye az u_3 üzenethez tartozó $\mathbf{z}_3 = (1,\ 1)$ kódszónak. Nyilvánvaló, hogy a kódszavak egymás után írásakor, például a $\{..., 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 1, ...\}$ sorozat esetében nem lehet eldönteni, hogy az $\{..., u_2,\ u_1,\ u_2,\ u_1,\ u_1, ...\}$

3.1. ábra. A forráskódoló modellje

A kódoló

U	**Z**
u_1	0
u_2	1 0
u_3	1 1

prefix-free kód

B kódoló

U	**Z**
u_1	1
u_2	0 0
u_3	1 1

nem prefix-free kód

3.2. ábra. A prefix-free kódolás illusztrálása

vagy az $\{...,u_2,\ u_1,\ u_2,\ u_3,...\}$ volt az eredeti üzenet, mivel a két egymást követő 1-es egyaránt jelenthet két egymást követő u_1-es vagy egy u_3-as üzenetet.

3.1 Definíció

Egy N mélységű D szintű teljes fa olyan gráf, amely egy közös gyökérből ered, minden belső csomópontjából éppen D számú elágazás indul és D^N levele, olyan terminális csomópontja van, amelynek a távolsága a gyökértől N.

A 3.3. ábrán egy ilyen teljes fát ábrázolunk, $D = 3$ és $N = 2$ esetben.

Minden D szintű prefix-free kód kölcsönösen egyértelműen hozzárendelhető egy D szintű fa terminális csomópontjaihoz, ha az elágazásokhoz a kódszavak egyes betűit rendeljük. A 3.4. ábrán ezt illusztráljuk $D = 3$ és $N = 2$ esetben, ha a kódszavak száma 5. Az ábrán két egyelemű és három kételemű kódszó látható. A kódszó ABC-jének a mérete $D = 3$.

Kraft-egyenlőtlenség

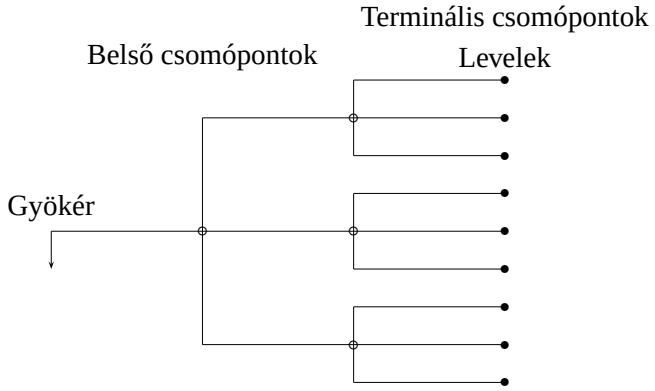
A Kraft-egyenlőtlenség tétele kimondja, hogy akkor és csak akkor létezik egy D szintű $\{w_1,\ w_2,...,w_K\}$ kódszóhosszakkal rendelkező prefix-free kód, ha teljesül a

$$\sum_{i=1}^{K} D^{-w_i} \leq 1 \tag{3.3}$$

Kraft-egyenlőtlenség.

Bizonyítás

Tudjuk, hogy egy N mélységű D szintű teljes fa terminális csomópontjainak a száma D^N. Ha erre a fára egy w hosszúságú kódszót illesztünk oly módon, hogy a kódszót egy olyan belső csomóponthoz rendeljük, amely a gyökértől w távolságra van, azaz a teljes fa belső csomópontjából terminális csomópontot hozunk létre, akkor a fa minden olyan ágát "le kell vágnunk", amelyik a teljes fán ebből a belső csomópontból származott. Nyilvánvaló, hogy ebben az esetben a eredeti teljes fáról D^{N-w} számú terminális csomópontot "vágtunk" le $(w < N)$.



3.3. ábra. Egy $N = 2$ mélységű $D = 3$ szintű teljes fa

Tételezzük fel, hogy van egy D szintű $\{w_1, w_2, ..., w_K\}$ kódszóhosszakkal rendelkező prefix-free kód, és ennek minden kódszavát illesztjük az N mélységű D szintű teljes fához a fent említett módon, egyúttal feltételezzük, hogy $N = \max_i \{w_i\}$. Mivel egy w_i hosszúságú kódszó illesztése esetén éppen D^{N-w_i} számú terminális csomópontot "vágunk" le a fáról, biztosan fenn kell állni az alábbi egyenlőtlenségnek

$$D^{N-w_1} + D^{N-w_2} + ... + D^{N-w_K} \leq D^N, \tag{3.4}$$

ugyanis a "levágott" terminális csomópontok száma nem lehet nagyobb az N mélységű teljes fa terminális csomópontjainak a számánál. Ezzel az állítás első részét, tehát azt, hogy minden D szintű $\{w_1, w_2, ..., w_K\}$ kódszóhosszakkal rendelkező prefix-free kód teljesíti a Kraft-egyenlőtlenséget bebizonyítottuk. A következőkben az állítás második részét kívánjuk igazolni, tehát azt, hogy minden kód, amely teljesíti a Kraft-egyenlőtlenséget egyúttal D szintű $\{w_1, w_2, ..., w_K\}$ kódszóhosszakkal rendelkező prefix-free kód.

Legyen az a feladat, hogy generáljunk egy D szintű $\{w_1, w_2, ..., w_K\}$ kódszóhosszakkal rendelkező prefix-free kódot. Rendezzük nagyságrendi sorrendbe a kódhosszakat $\{w_1 \leq w_2 \leq ... \leq w_K\}$, és legyen $N = w_K$.

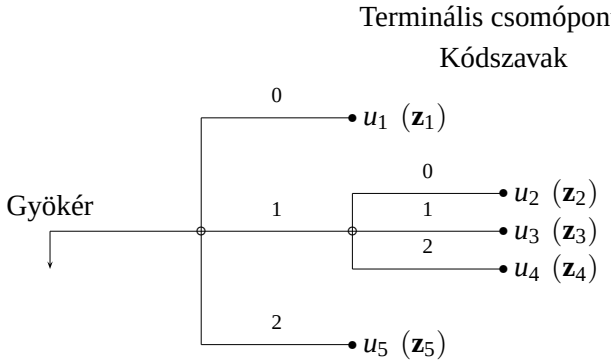
Hajtsuk végre ezután az alábbi algoritmust:

- Legyen a kezdeti lépésben $i = 1$.
- * Válasszunk ki az N mélységű D szintű fán egy Z_i még megmaradó (túlélő) csomópontot úgy, hogy a csomópont távolsága a gyökértől legyen w_i ($w_i \leq N$), és "vágjuk le" a fa minden olyan ágát, amelyik a Z_i csomópontból ered. Állitsuk meg az algoritmust, ha nincsen olyan túlélő csomópont, amelyik ebben a lépésben az algoritmushoz szükséges.
- Ha $i = K$, akkor fejezzük be az algoritmust, ellentétes esetben növeljük meg az i értékét $i + 1$-re, és térjünk vissza a *-gal jelölt lépéshez.

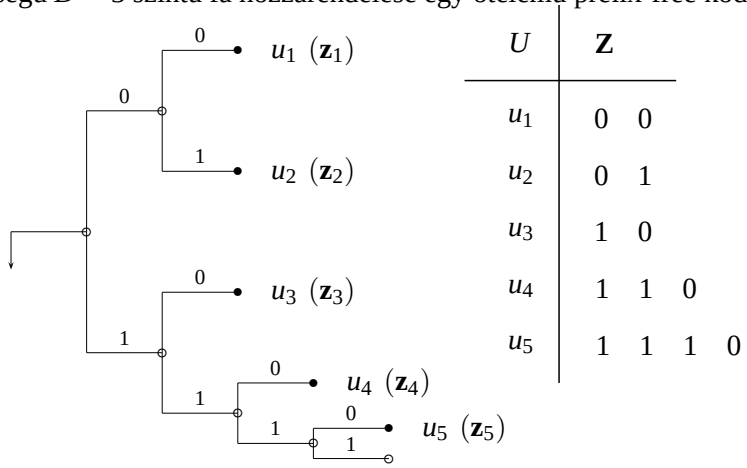
  Ebben a fázisban biztosan teljesül az alábbi egyenlőtlenség:

$$D^N - \left(D^{N-w_1} + D^{N-w_2} + ... + D^{N-w_i}\right) = D^N \left(1 - \sum_{j=1}^{i} D^{-w_j}\right) > 0, \tag{3.5}$$

ami azt jelenti, hogy amennyiben eljutunk az $i = K$-ig, akkor teljesül a Kraft-egyenlőtlenség, ha nem, akkor viszont nem lehet ilyen paraméterekkel rendelkező D szintű $\{w_1, w_2, ..., w_K\}$ kódszóhosszakkal rendelkező prefix-free kódot létrehozni. Érdemes megjegyezni, hogy amennyiben $i < K$ esetén van még N mélységű túlélő csomópont, akkor ebben a fázisban mindenképpen kell lenni olyan csomópontnak is, amelynek a mélysége $< N$.



3.4. ábra. Egy $N = 2$ mélységű $D = 3$ szintű fa hozzárendelése egy ötelemű prefix-free kódhoz



U	$\mathbf{Z}$
u_1	0 0
u_2	0 1
u_3	1 0
u_4	1 1 0
u_5	1 1 1 0

3.5. ábra. Prefix-free kód konstrukciója bináris fán

Ezzel az állítás második felét is igazoltuk, azaz a tételt bebizonyítottuk.

Példa

Konstruáljunk egy bináris ($D = 2$) prefix-free kódot a $\{w_1 = 2,\ w_2 = 2,\ w_3 = 2,\ w_4 = 3,\ w_5 = 4\}$ paraméterekkel. Mindenek előtt vizsgáljuk meg azt, hogy teljesül-e a Kraft-egyenlőtlenség. A számítás alapján igaz, hogy

$$\sum_{i=1}^{K} 2^{-w_i} = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} = \frac{15}{16} < 1, \tag{3.6}$$

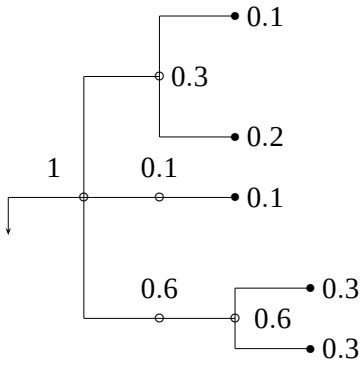
azaz a Kraft-egyenlőtlenség teljesül, így biztosan igaz, hogy ilyen paraméterekkel lehet prefix-free kódot generálni. A kód létrehozását, illetve a fent bevezetett algoritmus alkalmazását a 3.5. ábrán mutatjuk be.

3.2. Gyökeres fa valószínűségekkel

A gyökeres fa valószínűségekkel olyan véges fa típusú gráf, amelynek minden csomópontjához nem negatív számokat rendelünk az alábbi szabályok szerint:

- A gyökér valószínűsége 1.
- Minden csomópont valószínűsége azonos a csomóponthoz tartozó részfa (a csomópontból induló fa) valószínűségeinek az összegével.

A 3.6. ábrán a gyökeres fa valószínűségekkel fogalmára adunk meg egy példát.



3.6. ábra. Példa a gyökeres fára valószínűségekkel

Az úthossz segédtétel

Egy valószínűségekkel felcímkézett gyökeres fán **a terminális csomópontok $\mathbf{E}[W]$ átlagos távolsága** a gyökértől (ahol W az út hosszát jelző valószínűségi változó), azonos a nem terminális csomópontokhoz rendelt valószínűségek összegével, nem terminális csomópontnak tekintve a gyökeret is.

Bizonyítás

Minden belső csomópont valószínűsége azonos a csomóponthoz tartozó részfa (a csomópontból induló fa) valószínűségeinek az összegével. Egy a gyökértől d távolságra lévő terminális csomópontból a gyökérig vezető út éppen d belső csomópontot érint (ennyi csomóponton halad keresztül), éppen ezért a terminális csomópont valószínűsége éppen d-szer szerepel a kölönböző belső csomópontok valószínűségeinek az összegében. Mivel a gyökértől mért átlagos távolság nem más, mint a terminális csomópontok távolsága és valószínűsége szorzatának az összege, ez az összeg azonos a belső csomópontokhoz rendelt valószínűségek összegével beleértve a gyökeret is. Ezzel az állítást bebizonyítottuk.

Példa

A 3.6. ábrán bemutatott példa esetén ez a következőképpen számítható: $\mathbf{E}[W] = 1+0.1+0.3+0.6+0.6 = 0.1\times 2+0.2\times 2+0.1\times 2+0.3\times 3+0.3\times 3 = 2.6$, ahol W az út hosszát jelző valószínűségi változó.

Entrópia (bizonytalansági) függvények a gyökeres fán

Ha van egy valószínűségekkel felcímkézett gyökeres fa, amelynek T számú terminális csomópontja van éppen $p_1, p_2, ..., p_T$ valószínűségekkel, akkor a **terminális entrópia** a

$$H_\tau = -\sum_{i;\ p_i\neq 0}^{T} p_i \log(p_i) \tag{3.7}$$

összefüggéssel határozható meg.

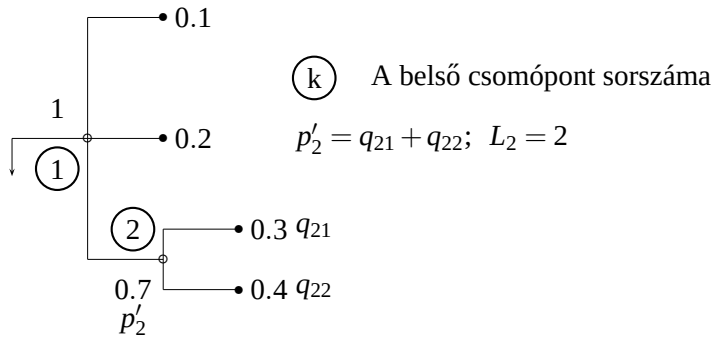
Tételezzük fel, hogy ez a gyökeres fa N számú belső (nem terminális) csomóponttal rendelkezik, és ezek valószínűségei rendre a $p'_1, p'_2, ..., p'_N$ értékek, valamint tudjuk, hogy $\sum_k p'_k = \mathbf{E}[W]$, a terminális csomópontok átlagos távolsága a gyökértől, akkor a k-dik belső csomóponthoz rendelt **elágazási entrópia** a

$$H_k = -\sum_{j;\ q_{kj}\neq 0}^{L_k} \frac{q_{kj}}{p'_k} \log\left(\frac{q_{kj}}{p'_k}\right) \tag{3.8}$$

kifejezéssel számítható, ahol p'_k a belső csomópont valószínűsége, q_{kj} az adott belső csomópontból kiinduló j-dik ág végén található valószínűség értéke, L_k pedig az ilyen ágak száma.

Példa

Számítsuk ki a fent bevezetett értékeket a 3.7. ábrán bemutatott példa esetén.



3.7. ábra. Példa a valószínűségekkel felcímkézett gyökeres fa entrópiáinak a számítására

Az ábrán látható esetben az egyes entrópiákat az alábbi módon határozhatjuk meg:

$$H_\tau = -\sum_{i;\ p_i \neq 0}^{T} p_i \log(p_i) = 1.846\ \texttt{bit}, \tag{3.9}$$

$$H_1 = -\sum_{j;\ q_{1j} \neq 0}^{L_1} \frac{q_{1j}}{p'_1} \log\left(\frac{q_{1j}}{p'_1}\right) = -0.1\log(0.1) - 0.2\log(0.2) - 0.7\log(0.7) = 1.157\ \texttt{bit}, \tag{3.10}$$

$$H_2 = -\sum_{j;\ q_{2j} \neq 0}^{L_2} \frac{q_{2j}}{p'_2} \log\left(\frac{q_{2j}}{p'_2}\right) = -\frac{0.3}{0.7}\log\left(\frac{0.3}{0.7}\right) - \frac{0.4}{0.7}\log\left(\frac{0.4}{0.7}\right) = 0.985\ \texttt{bit}. \tag{3.11}$$

Megjegyzés

A fenti eredmények alapján fontos megjegyezni, hogy a valószínűségekkel felcímkézett gyökeres fa entrópia függvényei között fennáll az alábbi összefüggés:

$$p'_k H_k = -\sum_{j;\ q_{kj} \neq 0}^{L_k} q_{kj} \log\left(q_{kj}\right) + p'_k \log\left(p'_k\right), \tag{3.12}$$

ami a 3.8. egyenletből triviálisan következik.

3.1. Tétel

Egy valószínűségekkel felcímkézett gyökeres fa terminális entrópiája (terminális bizonytalansági mértéke) azonos a nem terminális csomópontokhoz tartozó elágazási entrópiáknak (bizonytalanságoknak) az adott csomóponthoz tartozó valószínűséggel súlyozott összegével, azaz:

$$H_\tau = \sum_{k=1}^{N} p'_k H_k. \tag{3.13}$$

Bizonyítás

A l-dik belső csomópont esetében $p'_l \log\left(p'_l\right)$ természetesen része a fenti összegnek. Ugyanakkor p'_l egyúttal egy q_{kj} eleme egy előző elágazásnak, így a fenti megjegyzés alapján megjelenik az eredő összegben ennek az értéknek az ellentétes előjelű párja, így ezek összege 0. Az összes belső csomópontra történő összegezés után csak a terminális csomópontokhoz tartozó $p_i \log(p_i)$ szorzatoknak és a gyökér $p' \log(p')$ szorzatának nem lesz ellentétes előjelű párja, azaz a maradék valóban

$$H_\tau = \sum_{k=1}^{N} p'_k H_k. \tag{3.14}$$

Ezzel a tételt bebizonyítottuk.

3.3. A prefix-free kódok átlagos hosszának alsó korlátja

Jelöljük egy K értékkészletű U valószínűségi változó D-szintű prefix-free kódjának átlagos szóhosszát $\mathbf{E}[W]$-vel. A korábbi eredményekből következik, hogy ha $P_U(u)$ az U valószínűségi eloszlása, akkor fennállnak az alábbi összefüggések:

$$H_\tau = H(U), \tag{3.15}$$

$$H_k \leq \log(D), \tag{3.16}$$

és az egyenlőség akkor és csakis akkor áll fenn, ha az k-dik csomópont belső elágazása egyenletes eloszlású, valamint ebből következően

$$H(U) = H_\tau = \sum_{k=1}^{N} p'_k H_k \leq \log(D) \sum_{k=1}^{N} p'_k = \log(D)\,\mathbf{E}[W]. \tag{3.17}$$

3.2. Tétel
Egy K értékkészletű U valószínűségi változó D-szintű prefix-free kódjának átlagos szóhosszára, $(\mathbf{E}[W])$-re fennáll, hogy

$$\mathbf{E}[W] \geq \frac{H(U)}{\log(D)}, \tag{3.18}$$

ahol az egyenlőség akkor és csakis akkor áll fent, ha minden kódszó bármely részeleme után a következő kódbetű a D lehetséges érték közül egyenletes eloszlással sorsolódik ki, azaz minden elágazási entrópia maximális. A tétel a fent megadott összefüggések alapján egyszerűen belátható.

3.4. A Shannon-Fano prefix-free kód

Ebben a fejezetben megmutatunk egy eljárást arra, hogy miként lehet egy "elegendően jó", de nem feltétlenül optimális prefix-free kódot konstruálni egy K értékkészletű, $P_U(u)$ valószínűségi eloszlással rendelkező U valószínűségi változót generáló forráshoz. Ha a forrás éppen $P_U(u_i)$ eséllyel az $U = u_i$ értéket állítja elő, akkor ez úgy is értelmezhető, minha egy $L = 1/P_U(u_i)$ értékkészletű, egyenletes eloszlású valószínűségi változó vette volna fel az $U = u_i$ értéket. Nyilvánvaló viszont, hogy egy L értékkészletű, egyenletes eloszlású forráshoz rendelt kód, amelynek minden szimbóluma egy D méretű ABC-ből veszi fel az értékeit legalább

$$w_i = \lceil \log_D L \rceil \tag{3.19}$$

hosszúságú kódszavakat igényel, ahol $\lceil x \rceil$ az x valós számnál nagyobb vagy azzal egyenlő egész érték. Felhasználva a fenti összefüggéseket, átalakítások után az alábbi eredményre jutunk:

$$w_i = \left\lceil \log_D \left(\frac{1}{P_U(u_i)} \right) \right\rceil = \lceil -\log_D(P_U(u_i)) \rceil = \left\lceil -\frac{\log(P_U(u_i))}{\log(D)} \right\rceil. \tag{3.20}$$

Mivel $x \leq \lceil x \rceil < x+1$, ezért

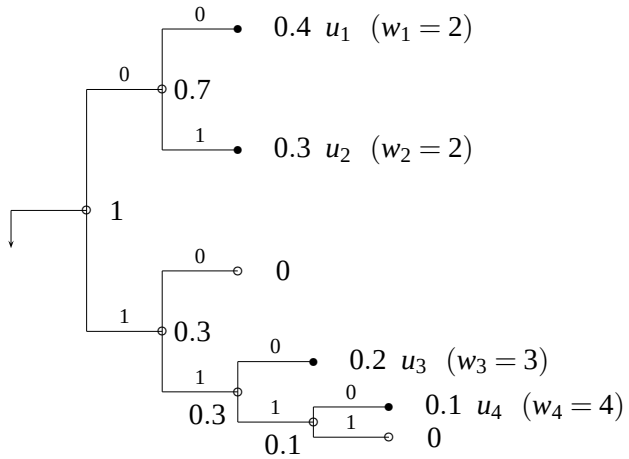
$$w_i \geq -\log_D(P_U(u_i)), \tag{3.21}$$

és K kódszó esetén

$$\sum_{i=1}^{K} D^{-w_i} \leq \sum_{i=1}^{K} D^{\log_D(P_U(u_i))} = \sum_{i=1}^{K} P_U(u_i) = 1, \tag{3.22}$$

amiből a Kraft-egyenlőtlenség alapján biztosan következik, hogy ilyen prefix-free kód létezik. A szóhosszra vonatkozó korábbi egyenlet alapján igaz az is, hogy

$$w_i < \frac{-\log(P_U(u_i))}{\log(D)} + 1, \tag{3.23}$$



3.8. ábra. A Shannon-Fano kód generálásának illusztrációja

amiből $P_U(u_i)$-vel történő szorzás, és i szerinti összegzés után az alábbi eredményhez jutunk:

$$\mathbf{E}[W] = \sum_{i=1}^{K} w_i P_U(u_i) < \sum_{i=1}^{K} \left(\frac{-\log(P_U(u_i))}{\log(D)} + 1 \right) P_U(u_i) = \frac{H(U)}{\log(D)} + 1. \tag{3.24}$$

Az így konstruált kódot Shannon-Fano kódnak nevezzük.

A K értékkészletű valószínűségi változó kódolási tétele

A Shannon-Fano kódkostrukció alapján megállapíthatjuk, hogy egy K értékkészletű U valószínűségi változóhoz rendelt optimális D méretű ABC-vel rendelkező prefix-free kód teljesíti az alábbi egyenlőtlenséget:

$$\frac{H(U)}{\log(D)} \leq \mathbf{E}[W] < \frac{H(U)}{\log(D)} + 1. \tag{3.25}$$

A tétel bizonyítása a Shannon-Fano kód konstrukciójából egyenesen következik.

Példa

Elemezzünk ezután egy illusztratív példát. Legyen $K = 4$, $D = 2$ és $\{P_U(u_1) = 0.4,\ P_U(u_2) = 0.3,\ P_U(u_3) = 0.2,\ P_U(u_4) = 0.1\}$. A Shannon-Fano kódolási szabály alapján, miszerint

$$w_i = \left\lceil -\frac{\log(P_U(u_i))}{\log(D)} \right\rceil, \tag{3.26}$$

az egyes kódszavak hosszára a $\{w_1 = 2,\ w_2 = 2,\ w_3 = 3,\ w_4 = 4\}$ érték adódik. Magát a kódot a 3.8. ábrán egy bináris fán adtuk meg, a prefix-free kódok előállítására vonatkozó korábbi szabály alkalmazásával.

Az ábra alapján kiszámíthatjuk a kódhossz várható értékét, valamint a forrás entrópiáját:

$$\mathbf{E}[W] = 1 + 0.7 + 0.3 + 0.3 + 0.1 = 2.4, \tag{3.27}$$

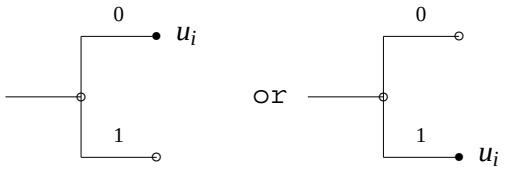
$$H(U) = -[0.4\log_2(0.4) + 0.3\log_2(0.3) + 0.2\log_2(0.2) + 0.1\log_2(0.1)] = 1.846 \ \texttt{bit}, \tag{3.28}$$

amiből valóban igaz, hogy

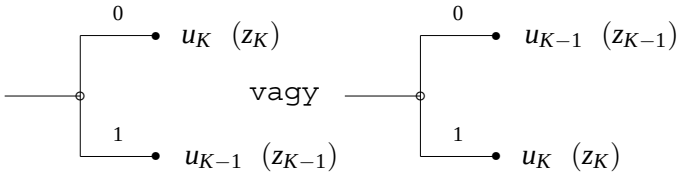
$$\frac{H(U)}{\log(D)} = 1.846 \leq \mathbf{E}[W] = 2.4 < \frac{H(U)}{\log(D)} + 1 = 2.846. \tag{3.29}$$

3.5. Huffman-kódok, változó hosszúságú optimális prefix-free kódok

Célunk olyan algoritmus kidolgozása, amely segítségével adott forráshoz optimális változó hosszúságú prefix-free kódot tudunk rendelni. A forrás K értékkészletű U valószínűségi változót állít elő $P_U(u_i)$, $i =$



3.9. ábra. A 3.1. Segédtétel illusztrációja



3.10. ábra. A 3.2. Segédtétel illusztrációja

$1,2,...,K$ valószínűségi eloszlással, és ehhez D szintű ABC-vel rendelkező optimális változó hosszúságú kódot kívánunk létrehozni. A feladatot először bináris kód-ABC esetében oldjuk meg, azaz $D = 2$.

Bináris Huffman-kód

A feladat megoldása előtt mondjunk ki két segédtételt.

3.1. Segédtétel

Az U valószínűségi változóhoz rendelt optimális bináris prefix-free kódot tartalmazó bináris fán nincsen nem használt terminális csomópont.

A segédtétel a 3.9. ábra alapján igen egyszerűen belátható, ugyanis, ha a bináris fa egyik terminális csomópontjához nem rendelünk kódszót (az ábrán az üres körrel jelzett terminális csomóponthoz nem tartozik kódszó (forrásszimbólum), míg a tele körrel jelzett csomóponthoz az u_i forrásszimbólum tartozik), akkor az u_i-hez tartozó kódszó utolsó kódbetűje elhagyható, tehát az adott kódszó egy betűvel rövidebb lehet. Ebből az következik, hogy optimális prefix-free kód esetén nem lehet nem használt terminális csomópont a kódhoz rendelt gyökeres fán.

3.2. Segédtétel

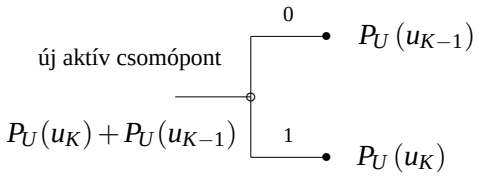
Az U valószínűségi változóhoz rendelt optimális bináris prefix-free kód esetén a két leghosszabb kódszó azonos hosszúságú és csak az utolsó betűben különbözik egymástól.

A 3.2. segédtétel a 3.10. ábra alapján szintén igen egyszerűen belátható. Tételezzük fel, hogy a forrás által előállított szimbólumokat valószínűségeik szerint sorbaállítottuk, azaz

$$P_U(u_K) \leq P_U(u_{K-1}) \leq, ..., \leq P_U(u_1), \tag{3.30}$$

és legyen z_i, $(i = (K-1)$ vagy $i = K)$ a kódoló által előállított optimális prefix-free kód egyik leghosszabb kódszava. Ekkor csak az ábrán feltüntetett kétféle eset fordulhat elő, vagyis a két legkisebb valószínűségű forrásszimbólumhoz rendelt kódszónak kell a leghosszabbnak lenni, különben az átlagos kódszóhossz nem lehet minimális. Ugyanakkor a 3.1. segédtétel következményeképpen, mivel a bináris fa minden terminális csomópontjához kódszót rendelünk, a két legkisebb valószínűségű forrásszimbólumhoz rendelt kódszó azonos hosszúságú és olyan terminális csomópontokhoz tartozik, amelyek csak az utolsó lépésben ágaznak el, azaz a kódszavak csak az utolsó kódbetűben különböznek egymástól.

A bináris Huffman-kód algoritmusa



3.11. ábra. A bináris Huffmam-algoritmus második lépésének az illusztrációja

Ezek alapján módunk van arra, hogy létrehozzuk azt az algoritmust, amely a bináris Huffman-kód előállítását lehetővé teszi. A feladat nem jelent mást, mint egy olyan optimális bináris prefix-free kód generálását, amelynek az átlagos szóhossza $\mathbf{E}[W]$ adott $P_U(u_i)$ és K esetében minimális. Az úthossz altétel alapján tehát olyan valószínűségekkel felcímkézett bináris gyökeres fát kell konstruálnunk, amely éppen K terminális csomóponttal rendelkezik, és amelyre igaz, hogy a belső csomópontok valószínűségeinek az összege (beleértve a gyökeret is) minimális.

A bináris Huffman-algoritmus az alábbi lépésekből áll:

- Jelöljünk ki K terminális csomópontot és rendeljük hozzájuk az $u_1,\ u_2, \ldots\ u_K$ forrásszimbólumokat úgy, hogy a forrásszimbólumok az előállítási valószínűségeik alapján csökkenő sorrendben legyenek rendezettek ($P_U(u_1) \geq P_U(u_2) \geq \ldots \geq P_U(u_{K-1}) \geq P_U(u_K)$). Nevezzük ezeket a csomópontokat aktív csomópontnak.
- * Képezzünk egy új csomópontot oly módon, hogy összekötjük a két legkisebb valószínűségű aktív csomópontot, és címkézzük fel ezt az új csomópontot a két aktív csomópont valószínűségeinek az összegével (lásd a mellékelt ábrát). Töröljük a két csomópontot az aktív csomópontok listájáról, és vegyük fel a listára az új csomópontot.
- Ha nincs már aktív csomópont, akkor az utolsónak generált új csomóponthoz rendeljük hozzá a gyökeret, és fejezzük be az algoritmust. Ha van még aktív csomópont, akkor és térjünk vissza a *-gal jelölt lépéshez.

Példa a bináris Huffman-kód generálására

Legyenek a $K=6$ értékkészletű forrás adatai a következők: $P_U(u_6)=0.05,\ P_U(u_5)=0.1,\ P_U(u_4)=0.15,\ P_U(u_3)=0.2,\ P_U(u_2)=0.23,\ P_U(u_1)=0.27$, és az a feladatunk, hogy a Huffman-algoritmus felhasználásával hozzunk létre optimális bináris prefix-free kódot.

A kód generálását a 3.12. ábrával illusztráljuk:

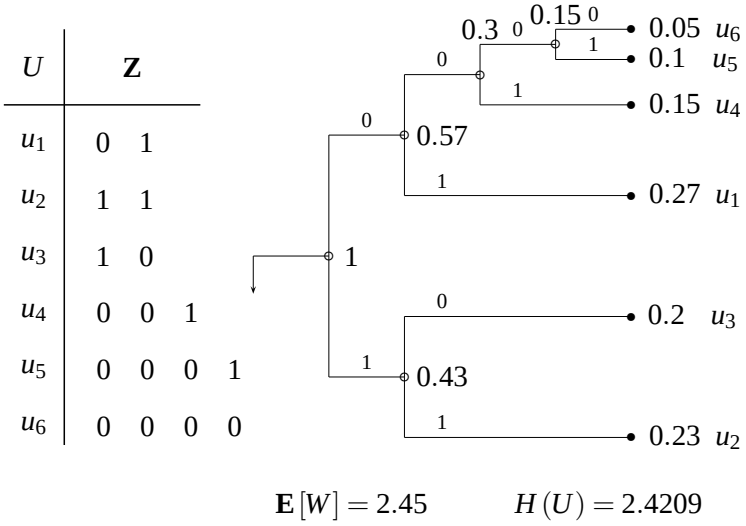
Szabályaink szerint az eljárást a két legkisebb valószínűséggel felcímkézett terminális csomóponttal kezdjük, azokkal, amelyek valószínűsége $P_U(u_6)=0.05$ és $P_U(u_5)=0.1$. Ezután e két csomópontot közösítjük, és létrehozunk egy új aktív csomópontot $P_U(u_6)+P_U(u_5)=0.05+0.1=0.15$ valószínűséggel. Ezután a két eredeti csomópontot töröljük az aktív csomópontok listájáról, és az új csomópontot felvesszük a listára.

A következő lépésben kiválasztjuk a két legkisebb valószínűségű aktív csomópontot, ez esetünkben az előbb létrehozott új csomópont és a $P_U(u_4)=0.15$ valószínűségű eredeti csomópont. E kettő egyesítésével létrehozunk egy új csomópontot, amelynek éppen $P_U(u_6)+P_U(u_5)+P_U(u_4)=0.05+0.1+0.15=0.3$ lesz a valószínűsége. Ismét töröljük a két csomópontot az aktív csomópontok listájáról, és az új csomópontot felvesszük a listára.

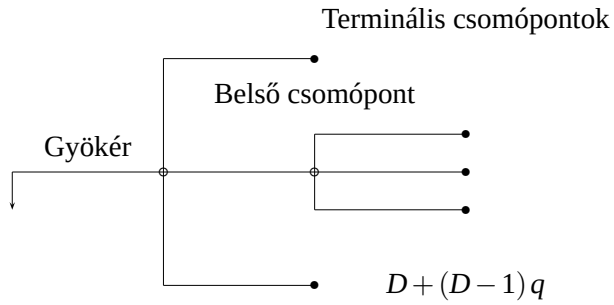
Az eljárást hasonló módon folytatjuk mindaddig, amig aktív csomópontot találunk. Az eljárás során egy valószínűségekkel felcímkézett gyökeres fát kapunk, amiről a kódszavak leolvashatók. Az ábrán megadtuk a létrehozott kód jellemző paramétereit, a $\mathbf{E}[W]$ és a $H(U)$ értékét.

Nem bináris Huffman-kód

Az előbb tárgyalt feladat után most foglalkozzunk a forráshoz nem bináris kódszavakat rendelő



3.12. ábra. Példa a bináris Huffman-kód előállítására



3.13. ábra. A 3.3. Segédtétel illusztrációja, $D = 3$, $q = 1$

Huffman-kód generálásával. A feladat megoldása előtt most is mondjunk ki néhány segédtételt.

3.3. Segédtétel

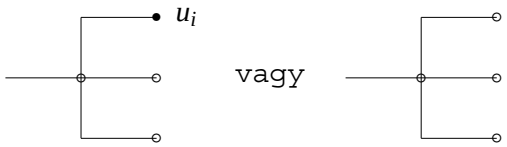
Egy D szintű gyökeres fa terminális csomópontjainak a száma $D + (D-1)\,q$, ahol q a belső (nem terminális) csomópontok száma a gyökéren kívül. A 3.3. segédtétel állítását a 3.13. ábrán illusztráljuk.

A segédtétel igen egyszerűen igazolható, mivel nyilvánvaló, hogy a gyökérből elindulva az első lépésben éppen D számú terminális csomópontot kapunk, majd egy újabb elágazáskor ismét D számú új terminális csomópont keletkezik, viszont az a korábbi terminális csomópont, amelyikből az elágazás kiindult belső csomóponttá válik, azaz minden újabb elágazás esetén a terminális csomópontok száma $D-1$-gyel, a belső csomópontok száma pedig 1-gyel nő. Ezzel az állítást bebizonyítottuk.

3.4. Segédtétel

Az U valószínűségi változóhoz rendelt optimális D szintű prefix-free kódot tartalmazó fán legfeljebb $D-2$ nem használt terminális csomópont van, és ezek távolsága a gyökértől maximális és egyforma. A 3.4. segédtétel állítását a 3.14. ábrán illusztráljuk.

A 3.4. segédtétel az ábra alapján igen egyszerűen belátható, ugyanis, ha a nem bináris fa utolsó elágazásánál csak az egyik terminális csomóponthoz rendelünk kódszót, vagy egyikhez sem (az ábrán az üres körrel jelzett terminális csomóponthoz nem tartozik kódszó (forrásszimbólum), míg a tele körrel jelzett csomóponthoz az u_i forrásszimbólum tartozik), akkor az u_i-hez tartozó kódszó utolsó



- • Használt csomópont
- ◦ Nem használt csomópont

3.14. ábra. A 3.4. segédtétel illusztrációja, $D = 3$

kódbetűje elhagyható, illetve erre az elágazásra nincsen szükség, tehát az adott kódszó egy betűvel rövidebb lehet. Mivel ilyen eset csak az ábrán bemutatott kétféle helyzetben jöhet létre, ebből az következik, hogy optimális prefix-free kód esetén nem lehet D vagy $D-1$ számú nem használt terminális csomópont a kódhoz rendelt gyökeres fán, azaz a nem használt terminális csomópontok száma legfeljebb $D-2$ értékű lehet.

A nem használt terminális csomópontok optimális prefix-free kód esetén természetesen a gyökértől a legtávolabb vannak, ellentétes esetben a kód nem lehet optimális. Ugyanis a nem használt terminális csomópontok távolsága a gyökértől nem növeli az átlagos szóhossz értékét (ezekhez 0 valószínűséget rendelünk), viszont, ha egy nem használt terminális csomópont közelebb lenne a gyökérhez, akkor egy nullánál nagyobb valószínűségű kódszóhoz kellene rendelni a gyökértől maximális távolságban lévő terminális csomópontot, ami biztosan nagyobb átlagos hosszúságú, tehát nem optimális kódhoz vezetne. Ezzel az állítást bebizonyítottuk.

A fenti két segédltétel segítségével K és D ismeretében az U valószínűségi változóhoz rendelt optimális D szintű prefix-free kódot tartalmazó fa **nem használt terminális csomópontjainak a száma** meghatározható.

3.5. Segédtétel

A K értékkészletű U valószínűségi változóhoz rendelt optimális D szintű prefix-free kódot tartalmazó fa nem használt terminális csomópontjainak a száma az

$$r = \mathbf{R}_{D-1}\left[(K-D)(D-2)\right] \tag{3.31}$$

kifejezéssel határozható meg, ahol $\mathbf{R}_i(j)$ j-nek az i-vel történő egész értékű osztása utáni maradék.

Bizonyítás

Jelöljük r-rel a nem használt terminális csomópontok számát, legyen az U valószínűségi változó értékkészletének a mérete K, és legyen a kód ABC-jének a mérete D. Ekkor a nem használt terminális csomópontok száma az

$$r = \texttt{terminális csomópontok száma} - K = [D + q(D-1)] - K \tag{3.32}$$

kifejezéssel határozható meg. Emellett tudjuk, hogy optimális kód esetén

$$0 \le r < (D-1), \tag{3.33}$$

amiből

$$D + (q-1)(D-1) < K \le D + q(D-1). \tag{3.34}$$

Felhasználva a terminális csomópontok számára vonatkozó összefüggést az

$$r = [D + q(D-1)] - K, \tag{3.35}$$

illetve átrendezés után a

$$D-K=-q\,(D-1)+r \tag{3.36}$$

kifejezéshez jutunk. Felhasználva azt a tényt, hogy $0\leq r<(D-1)$, megállapíthatjuk, hogy r értéke nem más, mint $(D-K)$-nak $(D-1)$-gyel történő egész értékű osztása utáni maradék, amit az

$$r=\mathbf{R}_{D-1}\,(D-K) \tag{3.37}$$

kifejezéssel jelölünk.

Mivel az egész értékű osztás utáni maradék nem változik akkor, ha $(D-K)$-hoz hozzáadunk egy olyan számot, ami $(D-1)$-gyel maradék nélkül osztható, r értéke az

$$r=\mathbf{R}_{D-1}\left[D-K+(K-D)\,(D-1)\right]=\mathbf{R}_{D-1}\left[(K-D)\,(D-2)\right] \tag{3.38}$$

egyszerű összefüggéssel meghatározható. Ezzel az állítást bebizonyítottuk.

3.6. Segédtétel

A K értékkészletű U valószínűségi változóhoz hozzárendelhető egy olyan optimális D-szintű ABC-vel rendelkező prefix-free kód, amelynek a $(D-r)$ legkisebb valószínűségű kódaszava maximális hosszúságú, és csak az utolsó betűben különbözik egymástól.

A 3.6. segédtétel a 3.2. segédtételhez hasonlóan egyszerűen igazolható. Tételezzük fel, hogy a forrás által előállított szimbólumokat az előállítás valószínűségei szerint sorbaállítottuk, azaz

$$P_U\,(u_K)\leq P_U\,(u_{K-1})\leq ...\leq P_U\,(u_1)\,, \tag{3.39}$$

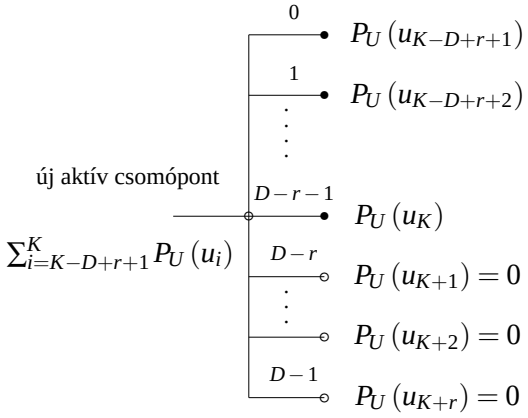
és legyen z_i, $(i=(K-D+r+1)\ \texttt{vagy}\ i=(K-D+r+2)\ \texttt{vagy},...,\texttt{vagy}\ i=K)$ a kódoló által előállított optimális prefix-free kód egyik leghosszabb kódszava. Nyílvánvaló, hogy a $D-r$ számú legkisebb valószínűségű forrásszimbólumhoz rendelt kódszónak kell a leghosszabbnak lenni, különben az átlagos kódszóhossz nem lehet minimális. Ugyanakkor a 3.5. segédltétel következményeképpen a D szintű fa r számú terminális csomópontját nem használjuk, így az utolsó elágazás után csak $D-r$ számú terminális csomóponthoz rendelünk kódszót. Ily módon a $D-r$ számú legkisebb valószínűségű forrásszimbólumhoz rendelt kódszó azonos hosszúságú és olyan terminális csomópontokhoz tartozik, amelyek csak az utolsó lépésben ágaznak el egymástól, azaz ezek a kódszavak csak az utolsó kódbetűben különböznek egymástól. Ezzel az állítást bebizonyítottuk.

A nem bináris Huffman-kód algoritmusa

Ezek alapján módunk van arra, hogy létrehozzuk azt az algoritmust, amely lehetővé teszi a nem bináris Huffman-kód előállítását. A feladat nem jelent mást, mint egy olyan optimális D szintű ABC-vel rendelkező nem bináris prefix-free kód generálását, amelynek az átlagos kódszóhossza, $\mathbf{E}\,[W]$ adott $P_U\,(u_i)$ és K esetében minimális. Az úthossz segédtétel alapján tehát olyan valószínűségekkel felcímkézett D szintű gyökeres fát kell konstruálnunk, amely éppen K terminális csomóponttal rendelkezik, és amelyre igaz, hogy a belső csomópontok valószínűségeinek az összege (beleértve a gyökeret is) minimális.

A nem bináris Huffman-algoritmus az alábbi lépésekből áll:

- Jelöljünk ki K terminális csomópontot és rendeljük hozzájuk az $u_1,u_2,...,u_K$ forrásszimbólumokat úgy, hogy a forrásszimbólumok az előállítási valószínűségeik alapján csökkenő sorrendben legyenek rendezettek ($P_U\,(u_1)\geq P_U\,(u_2)\geq,...,\geq P_U\,(u_{K-1})\geq P_U\,(u_K)$). Nevezzük ezeket a csomópontokat aktív csomópontnak.
- Határozzuk meg a nem használt terminális csomópontok számát az $r=\mathbf{R}_{D-1}\left[(K-D)\,(D-2)\right]$ kifejezés segítségével.
- * Képezzünk egy új csomópontot oly módon, hogy összekötjük a $(D-r)$ legkisebb valószínűségű aktív csomópontot, és címkézzük fel ezt az új csomópontot a $(D-r)$ aktív csomópont valószínűségeinek az összegével (lásd a 3.15. ábrát). Töröljük a $(D-r)$ csomópontot az aktív csomópontok listájáról, és vegyük fel a listára az új csomópontot.



3.15. ábra. A nem bináris Huffman-algoritmus második lépésének az illusztrációja

- Ha nincs már aktív csomópont, akkor az utolsónak generált új csomóponthoz rendeljük hozzá a gyökeret, és fejezzük be az algoritmust. Ha van még aktív csomópont, akkor előbb állítsuk be az $r = 0$ értéket, majd térjünk vissza a *-gal jelölt lépéshez.

Példa a nem bináris Huffman-kód generálására

Legyenek a $K = 6$ értékkészletű forrás adatai a következők: $P_U(u_6) = 0.05,\ P_U(u_5) = 0.1,\ P_U(u_4) = 0.15,\ P_U(u_3) = 0.2,\ P_U(u_2) = 0.23,\ P_U(u_1) = 0.27$, legyen $D = 3$, és az a feladatunk, hogy a Huffman-algoritmus felhasználásával hozzunk létre optimális $D = 3$ szintű prefix-free kódot.

A kód generálását a 3.16. ábrával illusztráljuk:

Szabályaink szerint az eljárást úgy kezdjük, hogy kiszámítjuk a nem használt terminális csomópontok számát az $r = \mathbf{R}_{D-1}[(K-D)(D-2)]$ kifejezés alapján, ami most az $r = \mathbf{R}_2[3 \times 1] = 1$ értéket adja. Az algoritmust a $D-r = 2$ számú legkisebb valószínűséggel felcímkézett terminális csomóponttal kezdjük, azokkal, amelyek valószínűsége $P_U(u_6) = 0.05$ és $P_U(u_5) = 0.1$. Ezután e két terminális csomópontot közösítjük egy nem használt (nulla valószínűségű) csomóponttal, és egy új elágazást (csomópontot) hozunk létre, amelynek a valószínűsége $P_U(u_6) + P_U(u_5) + 0 = 0.05 + 0.1 + 0 = 0.15$ értékű lesz. Ezután a két kezdő és a nem használt csomópontot töröljük az aktív csomópontok listájáról, és az új csomópontot felvesszük a listára, majd r értékét nullára állítjuk.

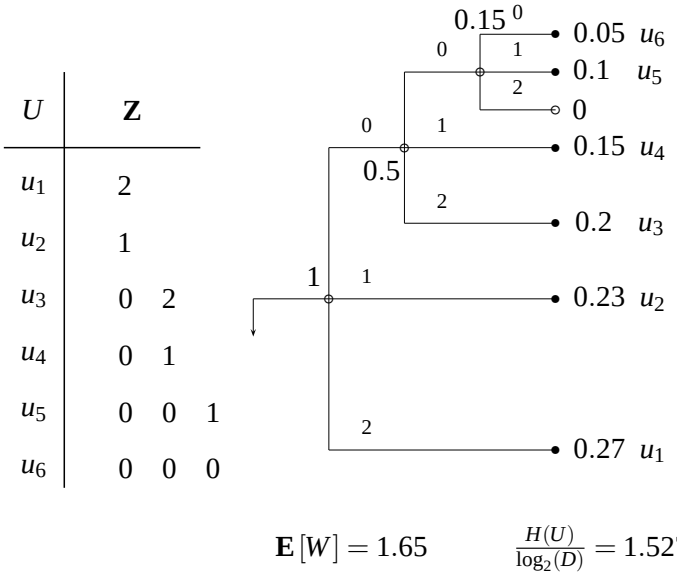
A következő lépésben kiválasztjuk a $D = 3$ számú legkisebb valószínűségű aktív csomópontot, ez esetünkben az előbb létrehozott új csomópont, a $P_U(u_4) = 0.15$ és a $P_U(u_3) = 0.2$ valószínűségű eredeti csomópont. E három egyesítésével létrehozunk egy új csomópontot, amelynek éppen $P_U(u_6) + P_U(u_5) + P_U(u_4) + P_U(u_3) = 0.05 + 0.1 + 0.15 + 0.2 = 0.5$ lesz a valószínűsége. Ismét töröljük a három csomópontot az aktív csomópontok listájáról, és az új csomópontot felvesszük a listára.

Ezután az eljárást hasonló módon folytatjuk mindaddig, amig aktív csomópontot találunk. Az eljárás során egy valószínűségekkel felcímkézett gyökeres fát kapunk, amiről a kódszavak leolvashatók. Az ábrán megadtuk a létrehozott kód jellemző paramétereit, a $\mathbf{E}[W]$ és a $H(U)/\log_2(D)$ értékét.

3.6. Diszkrét memóriamentes források változó hosszúságú kódolása

Ebben a fejezetben a korábban kimondott tételekre támaszkodva olyan források kódolásával foglalkozunk, amelyek a kimenetükön független sorozatokat generálnak, tehát a forrás által generált szimbólumsorozat elemei független valószínűségi változók.

3.2. Definíció



3.16. ábra. Példa a nem bináris Huffman-kód előállítására, $D = 3$, $K = 6$

Diszkrét memóriamentes forrásról (DMS) beszélünk abban az esetben, ha a forrás kimenetén megjelenő U_1, U_2, ..., U_L sorozat egyes elemei azonos eloszlású független diszkrét valószínűségi változók.

Kódolás üzenetblokkból változó hosszúságú kódba, a diszkrét memóriamentes források kódolási tétele

Egy diszkrét memóriamentes forrás L hosszúságú blokkjához rendelt D szintű ABC-vel rendelkező optimális prefix-free kódra teljesülnek az alábbi feltételek:

$$\frac{\mathbf{E}[W]}{L} < \frac{H(U)}{\log(D)} + \frac{1}{L}, \tag{3.40}$$

és

$$\frac{\mathbf{E}[W]}{L} \geq \frac{H(U)}{\log(D)}. \tag{3.41}$$

Bizonyítás

Jelöljük **V=**$[U_1, U_2, ..., U_L]$-lel a forrás kimenetén megjelenő L hosszúságú sorozatot, és legyen $H(\mathbf{V})$ ennek a vektor valószínűségi változónak az entrópiája. Mivel a sorozat egyes elemei független valószínűségi változók

$$H(\mathbf{V}) = H(U_1, U_2, ..., U_L) = H(U_1) + H(U_2) + H(U_3) + ... + H(U_L) = LH(U), \tag{3.42}$$

ugyanis a korábban belátott összefüggés alapján egy vektor valószínűségi változó együttes entrópiája a

$$H(U_1, U_2, ..., U_L) = H(U_1) + H(U_2 \mid U_1) + H(U_3 \mid U_2, U_1) + ... + H(U_L \mid U_{L-1}, ..., U_1) \tag{3.43}$$

kifejezéssel számítható, ugyanakkor

$$H\left(U_i \mid \mathbf{U}'\right) \leq H(U_i), \tag{3.44}$$

és az egyenlőség akkor és csakis akkor áll fent, ha U_i és $\mathbf{U}$ statisztikailag függetlenek egymástól, ami esetünkben teljesül.

A Shannon-Fano kódkonstrukció alapján korábban megállapíthatjuk, hogy egy $\mathbf{V}$ valószínűségi változóhoz rendelt optimális D méretű ABC-vel rendelkező prefix-free kód teljesíti az alábbi egyenlőtlenséget:

$$\frac{H(\mathbf{V})}{\log(D)} \leq \mathbf{E}[W] < \frac{H(\mathbf{V})}{\log(D)} + 1, \tag{3.45}$$

és behelyettesítve ebbe az egyenletbe a

$$H(\mathbf{V}) = LH(U), \tag{3.46}$$

kifejezést a

$$\frac{LH(U)}{\log(D)} \leq \mathbf{E}[W] < \frac{LH(U)}{\log(D)} + 1, \tag{3.47}$$

összefüggést kapjuk, amit elosztva L-lel a tétel állításához jutunk. Ezzel a tételt bebizonyítottuk.

Megjegyzés

A fenti tételből következik, hogy a forrás blokkhosszának, L-nek a növelésével az egy forráskarakterre jutó kódkarakterek átlagos értéke, $\mathbf{E}[W]/L$ aszimptotikusan a $H(U)/\log(D)$ lehetséges minimális értékhez tart, ami azt jelenti, hogy a Huffman-kód aszimptotikusan optimális kód.

3.7. Diszkrét memóriamentes források blokkódolása

A diszkrét memóriamentes források (DMS) blokkódolása azt jelenti, hogy a forrás kimeneti sorozataihoz állandó hosszúságú kódszavakat rendelünk. Nyilvánvaló, hogy ilyenkor optimális kód esetén a kódszavakhoz változó hosszúságú üzeneteket kell rendelni. A 3.17. ábrán megadtuk a rendszer modelljét. A modellben a diszkrét memóriamentes forrás kimenetén a

$$\mathbf{V} = [U_1,\ U_2, ..., U_Y], \tag{3.48}$$

vektor jelenik meg, ahol U_i egy K értékkészletű $P_U(u)$ eloszlásfüggvénnyel rendelkező valószínűségi változó (a DMS kimenete), Y az aktuális üzenet hossza,

$$\mathbf{Z} = [X_1,\ X_2, ..., X_N], \tag{3.49}$$

pedig a kódoló kimentén megjelenő kódszó, ahol X_j az aktuális kódszó j-dik karaktere, amely egy D értékkészletű ABC-ből veszi fel az értékeit, és N a kódszavak állandó hossza.

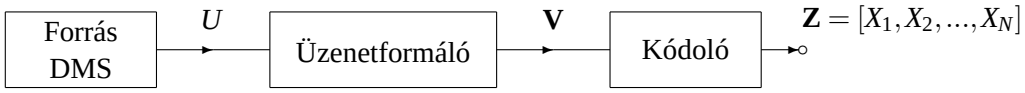
A rendszerben a diszkrét memóriamentes forrás kimenetére kapcsolódik az üzenetformáló, amelynek az a feladata, hogy egy adott szabály szerint a forrás kimenetén megjelenő jelekből olyan változó hosszúságú üzeneteket alakítson ki, melyeket az állandó N hosszúságú kódszavakhoz rendelünk. A működés egyenes következménye, hogy az üzenetek hossza Y a forrás sztochasztikus viselkedéséből következően valószínűségi változó.

A fent leírt kódolási eljárás minőségi mérőszáma az átlagos egy forrásszimbólumra eső D ABC-jű kódkaraktarek átlagos száma:

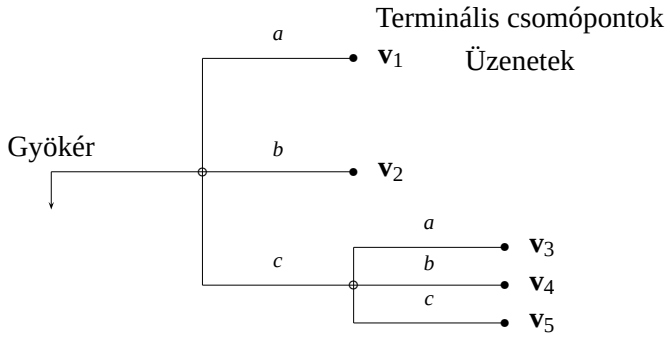
$$\frac{N}{\mathbf{E}[Y]}. \tag{3.50}$$

Optimális kódolás esetén ennek a hányadosnak minimális értéket kell felvenni, ami azt jelenti, hogy a $\mathbf{E}[Y]$ értékét kell maximalizálni. A rendszerben tehát az üzenetformáló egységnek kulcsszerepe van az optimális kód kialakításában: úgy kell az állandó hosszúságú kódszavakhoz rendelt üzeneteket megválasztani, hogy az üzenetek átlagos hossza maximális legyen, ugyanakkor teljesüljön az a feltétel is, hogy az üzenetformáló az egymás után érkező forrásszimbólum-folyamból az üzeneteket egyértelműen ki tudja választani. Ez azt jelenti, hogy most az alábbi követelményeket kell teljesíteni:

Követelmények



3.17. ábra. A diszkrét memóriamentes források blokkódolásának a modellje



3.18. ábra. Egy szabályos üzenethalmaz szerkezete

- Az kódolónak olyan üzeneteket kell előállítani, amelyek egyértelműen kötődnek egy-egy N hosszúságú kódszóhoz. Ez azt jelenti, hogy ugyanaz az üzenet nem tartozhat egynél több kódszóhoz.
- Nem lehet egyetlen olyan üzenet sem, amelyik előzménye, prefix-e valamilyen másik üzenetnek. Ha ez a feltétel nem teljesül, akkor az egymást követő üzeneteket az üzenetformáló nem tudja egyértelmű azonosítani, és azokat kódszavakhoz rendelni.

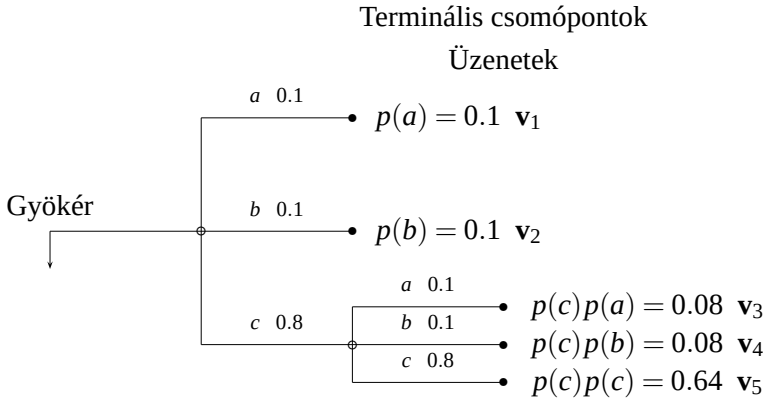
Mindebből az következik, hogy most nem a kódszavakat, hanem az üzeneteket kell elhelyezni egy gyökeres fán, oly módon, hogy minden üzenet a fa egy-egy terminális csomópontjáához (leveléhez) tartozzék. A feladat megoldásához először definiáljuk a **szabályos üzenethalmaz** fogalmát.

3.3. Definíció

Szabályos üzenethalmazról beszélünk abban az esetben, ha teljesülnek a 3.18. ábrán megadott feltételek, azaz minden belső csomópont azonos módon ágazik el éppen a forrás $P_U(u)$ eloszlásának megfelelően. Az ábrán minden elágazásban az $a,\ b,\ c$ karakterek jelenhetnek meg, mivel az U valószínűségi változó ezeket az értékeket veheti fel, és ezek valószínűsége rendre $P_U(a) = p(a)$, $P_U(b) = p(b)$, $P_U(c) = p(c)$.

A szabályos üzenethalmazt hordozó fát valószínűségekkel is fel tudjuk címkézni a 3.19. ábra szerint. A korábbiakból következik, hogy a szabályos üzenethalmazt hordozó gyökeres fára igazak az alábbi összefüggések:

- A fa terminális entrópiája:
$$H_\tau = H(\mathbf{V}), \tag{3.51}$$
mivel a fa terminális csomópontjaihoz most a $\mathbf{V}$ üzeneteket rendeltük, így a fa terminális entrópiája az üzenetek entrópiájával egyenlő.
- A fa i-dik belső csomópontjához tartozó elágazási entrópia:
$$H_i = H(U), \tag{3.52}$$
mivel a fa éppen a forrás statisztikája szerint ágazik el minden belső csomópontban, így minden elágazási entrópia a forrás entrópiájával egyenlő.



3.19. ábra. Egy szabályos üzenethalmaz valószínűségekkel

- A **V** üzenetvektor entrópiája:

$$H(\mathbf{V}) = H(U)\sum_{i=1}^{N'} p_i' \,, \tag{3.53}$$

ahol p_i' az i-dik nem terminális csomópont valószínűsége, N' a nem terminális csomópontok száma beleértve a gyökeret is, és ez az egyenlőség nem más, mint a korábban megismert összefüggés az elágazási és terminális entrópiák között abban az esetben, ha minden elágazási entrópia azonos értékű.

3.3. Tétel

Egy K értékkészletű, $H(U)$ entrópiájú diszkrét memóriamentes forráshoz tartozó szabályos üzenetvektor $H(\mathbf{V})$ entrópiája kielégíti az alábbi egyenlőséget:

$$H(\mathbf{V}) = H(U)\,\mathbf{E}(Y)\,, \tag{3.54}$$

ahol $\mathbf{E}(Y)$ az üzenetvektor átlagos hossza. A tétel az úthossz segédtétellel közvetlenül bizonyítható.

Példa

Vizsgáljuk meg a 3.20. ábrán bemutatott példát, és számítsuk ki a $H(U)$ és $H(\mathbf{V})$ értékeket.

- A forrás entrópiája

$$H(U) = -0.1\log_2(0.1) - 0.3\log_2(0.3) - 0.6\log_2(0.6) = 1.295\ \texttt{bit}, \tag{3.55}$$

- Az üzenetvektor átlagos hossza

$$\mathbf{E}(Y) = 1 + 0.6 = 1.6, \tag{3.56}$$

- Az üzenetvektor entrópiája

$$H(\mathbf{V}) = H(U)\,\mathbf{E}(Y) = 1.6 \times 1.295 = 2.072\ \texttt{bit}. \tag{3.57}$$

A diszkrét memóriamentes források kódolási tételének megfordítása

Bármely diszkrét memóriamentes forrás szabályos üzenethalmazának D szintű ABC-vel készített prefix-free kódjára érvényes, hogy az átlagos kódhossz ($\mathbf{E}[W]$) és az átlagos üzenethossz ($\mathbf{E}[Y]$) arányának az alsó korlátja a

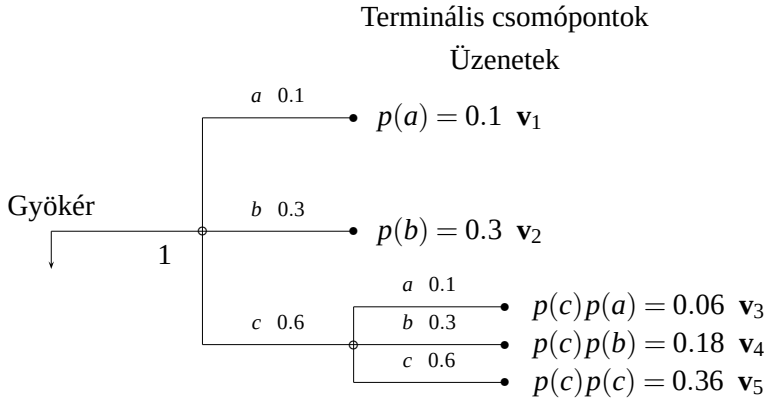
$$\frac{\mathbf{E}[W]}{\mathbf{E}[Y]} \geq \frac{H(U)}{\log(D)} \tag{3.58}$$

kifejezéssel adott.

Bizonyítás

Mivel a diszkrét memóriamentes forrásokra a 3.3. Tétel alapján érvényes a

$$H(\mathbf{V}) = H(U)\,\mathbf{E}(Y) \tag{3.59}$$



3.20. ábra. Példa a 3. Tételre

összefüggés, és a 3.2. Tétel szerint

$$\mathbf{E}[W] \geq \frac{H(\mathbf{V})}{\log(D)}, \tag{3.60}$$

a tétel állítása egyszerű behelyettesítéssel bizonyítható.

3.8. Tunstall-kódok, optimális blokk kódok

Célunk olyan algoritmus kidolgozása, amely segítségével egy adott K értékkészletű diszkrét memóriamentes forrás változó hosszúságú optimális prefix-free üzeneteihez blokk kódot tudunk hozzárendelni. Ha a blokk kód hossza N ($\mathbf{E}[W] = N$), akkor az optimális kódoláshoz a

$$\frac{\mathbf{E}[W]}{\mathbf{E}[Y]} = \frac{N}{\mathbf{E}[Y]} \tag{3.61}$$

értékét kell minimalizálni, vagyis a $\mathbf{E}[Y]$ értéket kell maximalizálni. A feladatot ismét valószínűségekkel felcímkézett fa típusú gráfok segítségével oldjuk meg. Az algoritmus felépítése előtt határozzuk meg az üzenetek számát.

Egy szabályos üzenethalmazban az üzenetek száma az

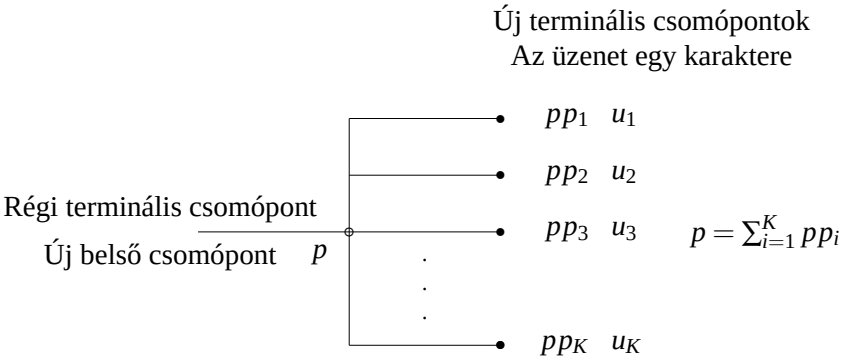
$$M = K + q(K-1), \quad q \geq 0 \tag{3.62}$$

kifejezés segítségével határozható meg, ahol M az üzenetek száma, q a belső csomópontok száma a gyökér nélkül, K a forrás értékkészletének a mérete.

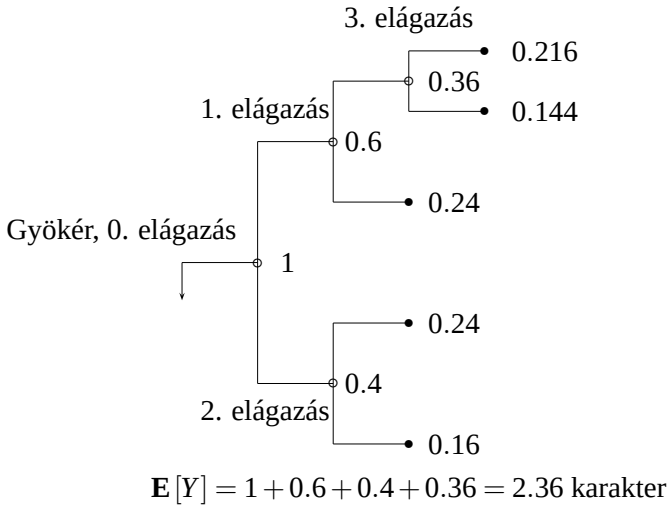
A szabályos üzenethalmazhoz rendelt, valószínűségekkel felcímkézett fa egyik elágazását a 3.21. ábrán illusztráljuk, ahol u_i a forrás által előállított U valószínűségi változó egyik lehetséges értéke, $P_U(u_i) = p_i, \;\; i = 1,2,...,K$ pedig az U valószínűségi eloszlása. Az ábra alapján az állítás egyszerűen belátható, hiszen nyilvánvaló, hogy a gyökérből elindulva az első lépésben éppen K számú terminális csomópontot kapunk, majd egy újabb elágazáskor $K-1$ számú új terminális csomópont keletkezik, viszont az a korábbi terminális csomópont, amelyikből az elágazás kiindult belső csomóponttá válik, azaz minden újabb elágazás esetén a terminális csomópontok száma $K-1$-gyel, a belső csomópontok száma pedig 1-gyel nő.

3.4.Definíció

Egy $M = K + q(K-1)$ elemből álló üzenethalmazt egy K értékkészletű diszkrét memóriamentes forráshoz tartozó Tunstall-üzenethalmaznak nevezünk akkor, ha a hozzá rendelt gyökeres fát úgy állítottuk elő, hogy a gyökértől indulva a q számú elágazást generáltunk oly módon, hogy a következő



3.21. ábra. Példa egy szabályos üzenethalmaz egyik elágazására



3.22. ábra. Példa egy Tunstall-üzenethelmaz generálására

elágazást mindig a legnagyobb valószínűségű terminális csomópontból indítottuk el. Az eljárásra a 3.22. ábrán mutatunk be egy példát.

Tunstall-segédtétel

Egy K értékkészletű diszkrét memóriamentes forráshoz rendelt szabályos üzenethalmaz akkor és csak akkor Tunstall-üzenethalmaz, ha a K szintű gyökeres fa minden belső csomópontja legalább olyan valószínűségű, mint bármelyik terminális csomópont.

Bizonyítás

A tétel első része egyszerűen következik a Tunstall-üzenethalmaz definíciójából, mivel az üzenethalmazhoz rendelt gyökeres fát úgy hoztuk létre, hogy minden lépésben kiválasztottuk a legnagyobb valószínűségű terminális csomópontot, és azt ágaztattuk tovább. Ebből nyilvánvaló, hogy sem a megmaradó eredeti terminális csomópontok, sem pedig az újonnan létrehozott terminális csomópontok valószínűsége nem lehet nagyobb az új belső (eredetileg terminális) csomóponténál.

A tétel második részét a következőképpen igazolhatjuk. Tételezzük fel, hogy van egy Tunstall-üzenethalmazhoz rendelt K szintű gyökeres fánk, és gondolatban vágjunk le a fáról K olyan ágat, amely a legnagyobb valószínűségű belső csomópontból ágazott el. q-szor végrehajtva ezt a műveletet eljutunk a fa kiterjesztett gyökeréig, azaz azokhoz az elágazásokhoz, amelyek a gyökértől indultak el. Viszont ha innen kiindulva ujra létrehozzuk a fát oly módon, hogy minden új elágazást a legnagyobb valószínűségű terminális csomópontból indítunk el, akkor természetesen az eredeti Tunstall-üzenethalmazhoz rendelt K szintű gyökeres fát kapjuk vissza. Ezzel a Tunstall-segédtételt bebizonyítottuk.

3.4. Tétel

Egy diszkrét memóriamentes forráshoz rendelt M elemű szabályos üzenethalmaz átlagos hosszúsága ($\mathbf{E}[Y]$) akkor és csakis akkor maximális az összes lehetséges M elemű szabályos üzenethalmazok terében, ha az üzenethalmaz Tunstall-üzenethalmaz.

Bizonyítás

Tekintsünk egy diszkrét memóriamentes forráshoz rendelt végtelen mélységű K szintű gyökeres fát (lásd a 3.23. ábrát), és vegyük figyelembe a következő tulajdonságait:

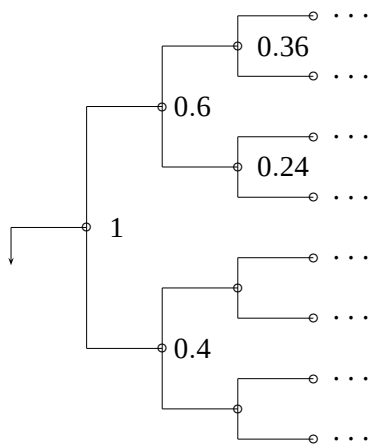
- A fa bármely csomópontjából elágazó részfára igaz, hogy annak minden csomópontja kisebb valószínűségű, mint az kiindulási csomópont valószínűsége.
- A szabályos üzenethalmaz minden csomópontja egyúttal csomópontja a végtelen mélységű K szintű gyökeres fának is.

A Tunstall-segédtételből következik, hogy egy $M = K + q(K-1)$ elemet tartalmazó szabályos üzenethalmaz akkor és csak akkor Tunstall-üzenethalmaz, ha annak a $q+1$ számú belső csomópontja a $q+1$ legnagyobb valószínűségű csomópont. Ezért a Tunstall-üzenethalmaz belső csomópontjai (beleértve a gyökeret is) valószínűségének az összege nagyobb, mint bármely más hasonló méretű belső csomóponthalmazé. Ebből pedig az úthossz segédtétel alapján következik, hogy az átlagos üzenethosszat éppen a Tunstall-üzenethalmaz maximalizálja. Ezzel a tételt bebizonyítottuk.

A Tunstall-algoritmus

Ezek alapján módunk van arra, hogy létrehozzuk azt az algoritmust, amely a Tunstall-kód előállítását lehetővé teszi. A feladat nem jelent mást, mint egy olyan optimális K szintű ABC-vel rendelkező prefix-free üzenethalmaz generálását, amelynek az átlagos szóhossza $\mathbf{E}[Y]$ adott $P_U(u)$ és K esetében maximális. Az úthossz segédtétel alapján tehát olyan valószínűségekkel felcímkézett K szintű gyökeres fát kell konstruálnunk, amely éppen $M = K + q(K-1)$ terminális csomóponttal rendelkezik, és amelyre igaz, hogy a belső csomópontok valószínűségeinek az összege (beleértve a gyökeret is) maximális.

Az algoritmus pontos definiálása előtt határozzuk meg a szükséges elágazások számát, q értékét úgy, hogy az üzenetek átlagos szóhossza $\mathbf{E}[Y]$ legyen maximális. Legyen adott N a kódszavak hossza, D a kód ABC és K a forrás ABC a mérete.



3.23. ábra. A 4. Tétel bizonyításának az illusztrálása

A korábbiakból tudjuk, hogy az üzenetek száma az

$$M = K + q(K-1) \tag{3.63}$$

kifejezés segítségével számítható. Tudjuk azt is, hogy a kódszavak száma kötött kódszóhossz (N) és adott méretű kód ABC (D) esetén éppen D^N, ezért biztos, hogy fent kell állnia az alábbi egyenlőtlenségnek:

$$0 \leq D^N - M = D^N - K - q(K-1) < K-1, \tag{3.64}$$

mivel biztosan minden kódszóhoz üzenetet célszerű rendelni, ezért az átlagos szóhossz maximalizálásához a kódszavak számát, ezzel együtt a szabályos üzenethalmazhoz rendelt gyökeres fa elágazásainak a számát addig kell növelni, amíg ez a feltétel teljesíthető. A feladatot pedig akkor oldottuk meg, ha a nem használt kódszavak száma (r) nullánál nagyobb és kisebb, mint $K-1$, azaz

$$D^N - K = q(K-1) + r, \qquad 0 \leq r < K-1. \tag{3.65}$$

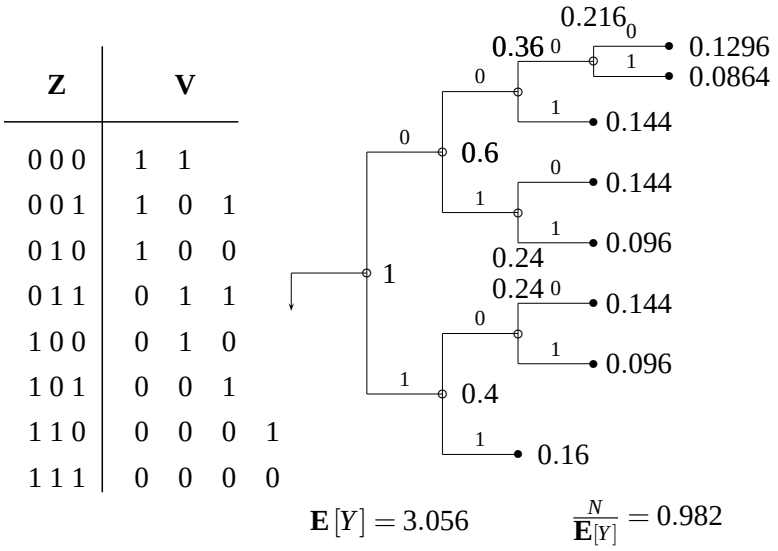
Az egyenlet alapján q egyszerűen meghatározható, mivel értéke az az egész szám ahányszor $K-1$ megvan $D^N - K$-ban.

A Tunstall-algoritmus az alábbi lépésekből áll:

- Ellenőrizzük, hogy a kódszavak száma nagyobb-e K-nál ($D^N > K$). Ha ez nem teljesül, akkor a kódszavak száma egyetlen üzenetkarakter kódolására sem elegendő, tehát az algoritmus sikertelen. Ha az eredmény pozitív, akkor határozzuk meg q értékét oly módon, hogy $D^N - K$ osszuk $K-1$-gyel, és határozzuk meg e szám egész értékét.
- Kunstruáljunk egy $M = K + q(K-1)$ elemű Tunstall-üzenethalmazt q számú elágazással és $P_U(u)$ elágazási valószínűségi eloszlással.
- Rendeljük hozzá kölcsönösen egyértelműen az N hosszúságú, D szintű ABC-vel rendelkező kódszavakat a Tunstall-üzenethalmaz egyes üzeneteihez (megjegyzendő, hogy ez a hozzárendelés tetszőleges sorrendű lehet).

Példa

Alkalmazzuk a Tunstall algoritmust bináris memóriamentes forrás esetén, ha $K = 2$, $P_U(0) = 0.6$, $P_U(1) = 0.4$, $N = 3$ és $D = 2$. Az optimális üzenethalmaz konstrukcióját a 3.24. ábrán adtuk meg, kiegészítve a kódolásra jellemző minőségi paraméterekkel, $\mathbf{E}[Y]$ és $N/\mathbf{E}[Y]$ értékével. A



3.24. ábra. Példa a Tunstall-algoritmus alkalmazására

példa érdekessége, hogy egy bináris forrás változó hosszúságú üzeneteihez fix hosszúságú bináris kódszavakat rendeltünk, és jól látható, hogy az egy üzenetbitre jutó átlagos kódbit értéke 0.982, azaz az optimális forráskódolás képes arra, hogy a bináris bitek átlagos számát csökkentse a kódolatlan átvitelhez képest. Azt is érdemes megjegyezni, hogy e nyereség forrása az, hogy a bináris forrás entrópiája nem maximális, azaz $P_U(0) \neq 0.5$. Ha a kódolást maximális entrópiájú forrás esetében végeztük volna el, akkor az optimális Tunstall-algoritmussal sem tudtunk volna nyereséget elérni.

3.5. Tétel

Egy K ABC méretű diszkrét memóriamentes forrás szabályos üzenethalmazához rendelt optimális N hosszúságú, D ABC-jű kódszavakból álló blokk kód esetén az $N/\mathbf{E}[Y]$ arány kielégíti az alábbi egyenlőtlenséget:

$$\frac{H(U)}{\log(D)} \leq \frac{N}{\mathbf{E}[Y]} < \frac{H(U)}{\log(D)} + \frac{\log(2/P_{min})\log(K)}{(N\log(D)-\log(K))\log(D)}, \tag{3.66}$$

ahol $H(U)$ a forrás egy karakterének az entrópiája, $P_{min} = \min_u P_U(u)$ a forrás legkisebb valószínűséggel generált szimbólumának a valószínűsége.

Bizonyítás

A baloldali egyenlőtlenség univerzálisan igaz a diszkrét memóriamentes források kódolási tétele alapján, a jobboldali egyenlőtlenséget az alábbiakban igazoljuk.

Egy szabályos üzenethalmaz legkisebb valószínűségű üzenetének (terminális csomópontjának) a valószínűsége felírható a

$$pP_{min} \leq \frac{1}{M} \tag{3.67}$$

alakban, ahol p egy belső csomópont valószínűsége a szabályos üzenethalmazhoz rendelt gyökeres fán. Az állítás biztosan igaz, hiszen a legkisebb valószínűségű üzenet is valamely belső csomópont egyik elágazásához tartozik, és biztos, hogy az üzenet utolsó karakterében a forrás a legkisebb valószínűségű szimbóluma található. Ezen kívül biztosan igaz, hogy a legkisebb valószínűségű üzenet valószínűsége nem lehet nagyobb $1/M$-nél, hiszen összesen M üzenet van. A fenti egyenletből átrendezés után azt kapjuk, hogy

$$p \leq \frac{1}{MP_{min}}, \tag{3.68}$$

és a Tunstall-segédtételből tudjuk, hogy Tunstall-üzenethalmaz esetén az üzenethalmazhoz rendelt gyökeres fa minden belső csomópontja nem kisebb valószínűségű, mint a fa bármely terminális csomópontja, és a terminális csomópontokhoz az üzeneteket rendeltük. Éppen ezért az üzenetek valószínűségeire igaz a

$$p_{\mathbf{V}}(\mathbf{v}) \leq \frac{1}{MP_{min}} \tag{3.69}$$

minden $\mathbf{v}$ esetén. A fenti egyenlőtlenség mindkét oldalának logaritmusát képezve a

$$-\log(p_{\mathbf{V}}(\mathbf{v})) \geq \log(M) - \log(1/P_{min}) \tag{3.70}$$

kifejezést kapjuk, amiből $p_{\mathbf{V}}(\mathbf{v})$-vel való szorzás és $\mathbf{v}$ szerinti összegzés után a

$$H(\mathbf{V}) \geq \log(M) - \log(1/P_{min}) \tag{3.71}$$

egyenlőtlenséghez jutunk.

Optimális kódolás esetén a kódolt üzenetek számát a lehető legnagyobbra kell választani, ami annyit jelent, hogy az elágazások számát, q-t maximalizálni kell. Mivel az üzenetek száma $M = K + q(K-1)$ és q maximális biztosan igaz, hogy

$$M + (K-1) > D^N \tag{3.72}$$

ahol N a kódszavak hossza és D^N a kódszavak száma.

Emellett tudjuk, hogy $M \geq K$, ezért

$$2M > D^N, \quad \texttt{vagy} \quad \log(M) > N\log(D) - \log(2), \tag{3.73}$$

amit felhasználva a

$$H(\mathbf{V}) > N\log(D) - \log(2/P_{min}) \tag{3.74}$$

kifejezést kapjuk.

A 3.3. Tétel szerint $H(\mathbf{V}) = \mathbf{E}[Y]H(U)$, amit behelyettesítve a fenti egyenlőtlenségbe az

$$\frac{N}{\mathbf{E}[Y]} < \frac{H(U)}{\log(D)} + \frac{\log(2/P_{min})}{\mathbf{E}[Y]\log(D)} \tag{3.75}$$

egyenlőtlenséghez jutunk.

Ezután a tétel igazolásához csak a $\mathbf{E}[Y]$-ra kell még egy jó becslést adnunk, ami az alábbi megfontolásokból egyenesen adódik.

Tudjuk, hogy egy L forráskarakterből álló sorozatban a lehetséges üzenetek száma K^L, és ha ezeket az üzeneteket N hosszúságú kódszavakkal akarjuk kódolni, akkor triviális kódolás (egyszerű hozzárendelés) esetén igaznak kell lenni az alábbi egyenlőtlenségnek:

$$K^L \leq D^N < K^{L+1}, \tag{3.76}$$

amiből

$$L > \frac{N\log(D)}{\log(K)} - 1. \tag{3.77}$$

Optimális kódolásnál viszont az üzenetek átlagos szóhossza biztosan nem kisebb, mint L, a triviális kódolás esetén kapott átlagos szóhossz, így

$$\mathbf{E}[Y] \geq L > \frac{N\log(D) - \log(K)}{\log(K)}. \tag{3.78}$$

Ezt behelyettesítve az előző egyenlőtlenségbe a tételt bebizonyítottuk.

Megjegyzés

A fenti tételből következik, hogy a kód blokkhosszának, N-nek a növelésével az egy átlagos forráskarakterre jutó kódkarakterek értéke, $N/\mathbf{E}[Y]$ aszimptotikusan a $H(U)/\log(D)$ lehetséges minimális értékhez tart, ami azt jelenti, hogy a Tunstall-kód aszimptotikusan optimális kód.

4. fejezet

Blokkból blokkba kódolás, a tipikus sorozatok tulajdonságai

A korábbi fejezetekben részletesen foglalkoztunk a források kódolásával, sőt két optimális kódolási eljárást is megismertettünk. Figyelmünk eddig az alábbi esetekre terjedt ki:

- Állandó hosszúságú üzenetblokk változó hosszúságú kódba kódolása (Huffman-algoritmus),
- Változó hosszúságú üzenetblokk állandó hosszúságú kódba kódolása (Tunstall-algoritmus),
- Változó hosszúságú üzenetblokk változó hosszúságú kódba kódolása (A diszkrét memóriamentes források kódolási tételének megfordítása).

A fenti témakörökben részben általános tételeket mondtunk ki, részben gyakorlati eljárásokat is adtunk a kódolási feladat megoldására. Nem tárgyaltuk azonban a lehetséges negyedik esetet, az:

- Állandó hosszúságú üzenetblokk állandó hosszúságú kódba kódolását.
  Hogy ezzel miért nem foglalkoztunk, annak két magyarázata is van:
- Nyilvánvaló ugyanis, hogy ebben az esetben a kódolási feladat triviálisan megoldható, mivel optimális algoritmus kidolgozása helyett elegendő teljesíteni a

$$D^{N-1} < K^L \leq D^N \tag{4.1}$$

  egyenlőtlenséget, ahol L az üzenetblokk hossza, K a forrás ABC-jének a mérete, N a kódszó hossza és D a kód ABC-jének a mérete. Az egyenlőtlenség azt fejezi ki, hogy adott L, K és D esetén N értékét úgy kell megválasztani, hogy elegendő kódszó álljon rendelkezésünkre az összes K^L számú üzenet kódolására, viszont hatékony (optimális) kódolás esetén a szükségesnél hosszabb kódot nem szabad választani a

$$\frac{\mathbf{E}[W]}{\mathbf{E}[Y]} = \frac{N}{L} \tag{4.2}$$

  hányados minimalizálása érdekében. Ebből pedig az következik, hogy ebben az esetben a forrás entrópiája $H(U)$ a kódolási folyamatban nem játszik szerepet, vagyis a kódolás hírközléselméleti szempontból nem releváns.
- Jobban körüljárva a feladatot a kérdésre adhatunk egy kicsit összetettebb választ is. Ez pedig nem más, mint **a veszteségmentes és veszteséges kódolás** megkülönböztetése. A korábbi kódolási eljárások esetében feltételként kikötöttük, hogy csak olyan megoldást fogadunk el, ahol a kódszavakból az elküldött üzenet hiba és veszteség nélkül visszaállítható, azaz csak veszteségmentes kódolásokkal foglalkoztunk. Ezzel szemben vezessük be a veszteséges kódolás fogalmát, amikor ez a feltétel nem teljesül, tehát az üzenetek visszaállításánál megengedünk hibákat is, ha ezeknek a hibáknak a száma egy "elfogadható" mértéket nem halad meg.

(a) 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1

(b) 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1

(c) 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0

4.1. ábra. A bináris memóriamentes forrás három lehetséges $L = 20$ hosszúságú sorozata

A következőkben az állandó hosszúságú üzenetblokkok állandó hosszúságú kódba kódolásával foglalkozunk veszteséges forráskódolás esetén. A téma megalapozása érdekében bevezetjük a tipikus sorozatok fogalmát.

4.1. A tipikus sorozatok fogalma

A tipikus sorozatok fogalmának tárgyalását kezdjük egy illusztratív példa elemzésével.

Példa

Legyen egy bináris memóriamentes forrás, aminek egy $L = 20$ hosszúságú sorozatát figyeljük meg, és legyen $P_U(0) = 3/4$ és $P_U(1) = 1/4$. A 4.1. ábrán példaképpen megadtuk a forrás $L = 20$ hosszúságú sorozatainak három realizációját.

Az ábrán megadott sorozatok valószínűsége az alábbi formában adható meg:

$$P_{U_1 \ldots U_{20}}(u_1, ..., u_{20}) = (3/4)^z (1/4)^{20-z} = (1/4)^{20} (3)^z, \tag{4.3}$$

ahol z a sorozatban lévő 0-k száma. Ebből az egyes sorozatok valószínűségeire az alábbi összefüggések adódnak:

- (a) $P_{(a)} = (1/4)^{20}$,
- (b) $P_{(b)} = (1/4)^{20}(3)^{14}$,
- (c) $P_{(c)} = (1/4)^{20}(3)^{20}$.

Mindebből arra a következtetésre juthatunk, hogy a forrásra a három sorozat közül a legjellemzőbb a (c) jelű, hiszen annak a legnagyobb a valószínűsége, ugyanis például:

$$\frac{P_{(c)}}{P_{(b)}} = \frac{(1/4)^{20}(3)^{20}}{(1/4)^{20}(3)^{14}} = (3)^6, \tag{4.4}$$

tehát a (c) sorozat valószínűsége jóval nagyobb, mint a (b) sorozaté.

Ennek ellenére, ha bárkit megkérdeznénk arról, hogy melyik sorozat jellemzi leginkább a forrás tulajdonságait, akkor természetesen azt válaszolná, hogy a (b), mivel a forrás 0 és 1 értékeket egyaránt előállít, és azt várjuk, hogy ezek tipikusan olyan gyakorisággal jelenjenek meg a forrás kimenetén, amilyen a valószínűségük. Éppen ezért tudjuk, hogy a (c) sorozat kevésbé jellemzi a forrás statisztikai tulajdonságait, mint a (b).

A **nagy számok törvénye** ugyanis kimondja, hogy ha egy véletlen eseményt sokszor megismétlünk egymástól függetlenül, akkor egy p valószínűségű elemi esemény relatív gyakorisága nagy valószínűséggel a p értékhez lesz igen közel. Természtes érzékünk erre a törvényre támaszkodik, amikor a (b) sorozatot ítéljük a forrás statisztikájára nézve a leginkább tipikusnak, mivel

- (a) $z/20 = 0/20 << 3/4$,
- (b) $z/20 = 14/20 \approx 3/4$,
- (c) $z/20 = 20/20 >> 3/4$.

A következőkben ennek a fogalomnak adjuk meg a pontos matematikai definícióját.

A tipikus sorozatok definíciója

Tekintsük egy diszkrét memóriamentes forrás K szintű véges ABC-vel rendelkező és $P_U(u)$ valószínűségi eloszlású U kimenetét, amely az $\{a_1, a_2, ..., a_K\}$ értékkészletből veszi fel az értékeit. Vizsgáljuk meg a forrás kimenetén megjelenő U üzenetnek egy L hosszúságú sorozatát, az $\mathbf{U} = [U_1, U_2, ..., U_L]$ vektort, amelynek az egyedi realizációi a $\mathbf{u}$ vektorok.

Jelöljük $n_{a_i}(\mathbf{u})$-val azt a számot, ahányszor az a_i előfordul az $\mathbf{u}$ vektorban, azaz legyen ez a szám az a_i betű gyakorisága az $\mathbf{U}$ valószínűségi változó sorozat egy realizációjában.

Legyen ε egy tetszőleges pozitív szám, és tételezzük fel, hogy ismerjük az n_{a_i} gyakoriságokat minden forrásbetűre, akkor a diszkrét memóriamentes forrás egy L hosszúságú $\mathbf{U} = \mathbf{u}$ sorozata ε-tipikus, ha

$$(1-\varepsilon) P_U(a_i) \leq \frac{n_{a_i}(\mathbf{u})}{L} \leq (1+\varepsilon) P_U(a_i) \quad \texttt{minden} \quad 1 \leq i \leq K \quad \texttt{esetén}, \tag{4.5}$$

ami annyit jelent, hogy egy ε-tipikus sorozatnál a fenti egyenlőtlenségnek minden lehetséges üzenetbetű esetén teljesülni kell.

Példa

Vizsgáljuk meg a 4.1. ábrán megadott egyes sorozatokat ε-tipikusság szempontjából. Legyen $\varepsilon = 1/3$. Az ε-tipikusság feltétele ebben az esetben az alábbi egyenlőtlenségek teljesülése:

- $(a_1 = 0)$

$$\left(\frac{2}{3}\right)\left(\frac{3}{4}\right) \leq \frac{n_0(\mathbf{u})}{20} \leq \left(\frac{4}{3}\right)\left(\frac{3}{4}\right),$$

$$10 \leq n_0(\mathbf{u}) \leq 20, \tag{4.6}$$

és

- $(a_2 = 1)$

$$\left(\frac{2}{3}\right)\left(\frac{1}{4}\right) \leq \frac{n_1(\mathbf{u})}{20} \leq \left(\frac{4}{3}\right)\left(\frac{1}{4}\right),$$

$$4 \leq n_1(\mathbf{u}) \leq 6 < \frac{20}{3}. \tag{4.7}$$

Vizsgáljuk meg, hogy az egyenlőtlenségek mely sorozat esetében teljesülnek.

- (a)
  $a_1 = 0$

$$10 > n_0(\mathbf{u}) = 0 < 20, \tag{4.8}$$

  és
  $a_2 = 1$

$$4 < n_1(\mathbf{u}) = 20 > 6, \tag{4.9}$$

- (b)
  $a_1 = 0$

$$10 < n_0(\mathbf{u}) = 14 < 20, \tag{4.10}$$

  és
  $a_2 = 1$

$$4 < n_1(\mathbf{u}) = 6 = 6, \tag{4.11}$$

- (c)
  $a_1 = 0$

$$10 < n_0(\mathbf{u}) = 20 = 20, \tag{4.12}$$

  és

$a_2 = 1$

$$4 > n_1(\mathbf{u}) = 0 < 6, \tag{4.13}$$

amiből megállapítható, hogy a (b) sorozat $\varepsilon = 1/3$-tipikus, viszont az (a) és a (c) sorozat nem. Egyébként nyilvánvaló, hogy egy tipikus sorozat nem tartalmazhat olyan a_i betűt, amelynek a valószínűsége $P_U(a_i) = 0$.

A tipikus sorozatok további elemzése előtt idézzünk vissza néhány olyan matematikai összefüggést, amelyek az elkövetkező vizsgálatokhoz elengedhetetlenül szükségesek.

4.2. A Csebisev-egyenlőtlenség és a nagy számok gyenge törvénye

A fejezetben összefoglalunk néhány olyan valószínűségszámítási egyenlőtlenséget, amelyek a tipikus sorozatokkal kapcsolatos elméleti vizsgálatok szempontjából fontosak, és amelyeket a következő fejezetekben ténylegesen használni fogunk.

- **Csebisev-egyenlőtlenség**
  Legyen X egy valós értékű valószínűségi változó véges $m_X = \mathbf{E}[X]$ várható értékkel és $Var(X) = \mathbf{E}\left[(X-m_X)^2\right]$ szórásnégyzettel. Jelöljük A-val azt az eseményt, hogy $|X-m_X| \geq \varepsilon$ és A^c-vel ennek az eseménynek a komplementerét. Ekkor

$$Var(X) = \mathbf{E}\left[(X-m_X)^2 \mid A\right]\Pr(A) + \mathbf{E}\left[(X-m_X)^2 \mid A^c\right]\Pr(A^c) \geq \mathbf{E}\left[(X-m_X)^2 \mid A\right]\Pr(A), \tag{4.14}$$

  ezért

$$Var(X) \geq \mathbf{E}\left[(X-m_X)^2 \mid A\right]\Pr(A) \geq \varepsilon^2 \Pr(A), \tag{4.15}$$

  amiből a Csebisev-egyenlőtlenség direkt módon következik

$$\Pr(|X-m_X| \geq \varepsilon) \leq \frac{Var(X)}{\varepsilon^2}. \tag{4.16}$$

  A Csebisev-egyenlőtlenség tehát felső becslést ad arra, hogy egy valószínűségi változó eltérésének az abszolút értéke a várható értéktől mekkora eséllyel nagyobb egy előre megadott ε küszöbnél.

- **A szórásnégyzet három tulajdonsága**
  (a) $Var(X) = \mathbf{E}\left[X^2\right] - m_X^2$,
  (b) Ha $Y = cX$, akkor $Var(Y) = c^2 Var(X)$, mivel

$$\mathbf{E}\left[Y^2\right] - m_Y^2 = c^2\mathbf{E}\left[X^2\right] - c^2 m_X^2 \tag{4.17}$$

  (c) Ha X és Y függetlenek, akkor

$$Var(X+Y) = Var(X) + Var(Y), \tag{4.18}$$

  és az állítás akkor is igaz, ha X és Y csak korrelálatlanok.

- **A nagy számok gyenge törvénye**
  Tekintsük az alábbi

$$S_N = \frac{1}{N}(X_1 + X_2 + \ldots + X_N) \tag{4.19}$$

  úgynevezett mintaátlagot, ahol $X_i, \quad i = 1,2,\ldots,N$ független azonos eloszlású valószínűségi változók sorozata m_X közös várható értékkel és $Var(X)$ közös szórásnégyzettel. A korábbiak alapján az S_N mintaátlag várható értéke a

$$\mathbf{E}[S_N] = m_X, \tag{4.20}$$

és

$$Var(S_N) = \frac{1}{N} Var(X). \tag{4.21}$$

Alkalmazzuk ezután a mintaátlagra a Csebisev-egyenlőtlenséget, miszerint

$$\Pr(|S_N - m_X| \geq \varepsilon) \leq \frac{Var(X)}{N\varepsilon^2}, \tag{4.22}$$

vagy

$$\Pr(|S_N - m_X| < \varepsilon) \geq 1 - \frac{Var(X)}{N\varepsilon^2}. \tag{4.23}$$

Ez az utóbbi egyenlőtlenség kimondja, hogy bármilyen kis értékű $\varepsilon > 0$ esetén

$$\lim_{N\to\infty} \Pr(|S_N - m_X| < \varepsilon) = 1 \tag{4.24}$$

és ebből a nagy számok gyenge törvénye közvetlenül adódik

$$p \lim_{N\to\infty} S_N = m_X, \tag{4.25}$$

amely kimondja, hogy egy véletlen kísérlet többszöri független végrehajtása esetén a mintaátlag aszimptotikusan a valószínűségi változó várható értékéhez tart.

- **A nagy számok gyenge törvényének egy speciális alkalmazása**
  Alkalmazzuk a nagy számok gyenge törvényét indikátor valószínűségi változókra, ahol

$$X = \begin{cases} 1, & \texttt{ha } A \texttt{ bekövetkezik} \\ 0, & \texttt{ha } A^c \texttt{ bekövetkezik} \end{cases}. \tag{4.26}$$

  Ilyenkor igazak az alábbi összefüggések:
  (a) $P_X(1) = \Pr(A), \quad P_X(0) = 1 - \Pr(A),$
  (b) $\mathbf{E}(X) = \Pr(A), \quad \mathbf{E}(X^2) = \Pr(A)$, mivel $X^2 = X$,
  (c) $Var(X) = \Pr(A)(1 - \Pr(A))$.
  Hajtsuk végre ezután a véletlen kísérletet N-szer, azaz állítsuk elő az $X_1, X_2, ..., X_N$ sorozatot, amely független azonos eloszlású valószínűségi változók vektora, és számítsuk ki az A esemény bekövetkezésének a relatív gyakoriságát, az

$$S_N = \frac{N_A}{N} \tag{4.27}$$

  értéket, ahol N_A az A esemény bekövetkezésének a száma az N számú kísérletből.
  A nagy számok gyenge törvénye szerint

$$\Pr\left(\left|\frac{N_A}{N} - \Pr(A)\right| \geq \varepsilon\right) \leq \frac{\Pr(A)(1 - \Pr(A))}{N\varepsilon^2}, \tag{4.28}$$

  vagy

$$\Pr\left(\left|\frac{N_A}{N} - \Pr(A)\right| < \varepsilon\right) \geq 1 - \frac{\Pr(A)(1 - \Pr(A))}{N\varepsilon^2}, \tag{4.29}$$

  amiből

$$\lim_{N\to\infty} \Pr\left(\left|\frac{N_A}{N} - \Pr(A)\right| < \varepsilon\right) = 1, \tag{4.30}$$

  vagyis a relatív gyakoriság aszimptotikusan a valószínűséghez tart.

4.3. A tipikus sorozatok tulajdonságai

Visszatérve a tipikus sorozatok definíciójához elemezzük a K szintű $\{a_1, a_2, ..., a_K\}$ ABC-vel rendelkező diszkrét memóriamentes forrás kimenetén megjelenő L hosszúságú $\mathbf{U} = \{U_1, U_2, ..., U_L\}$ üzenetvektor tulajdonságait. Legyen a forrás üzeneteinek valószínűségi eloszlása $P_U(u_i)$, $i = 1, 2, ..., K$. Jelöljük az $\mathbf{U}$ vektor egyedi realizációit az $\mathbf{u} = \{u_1, u_2, ..., u_L\}$ vektorral, és jelölje $n_{a_i}(\mathbf{u})$ az a_i betű számosságát az $\mathbf{u}$ vektoron belül.

Egy adott $\mathbf{u}$ realizáció valószínűségét a

$$P_{\mathbf{U}}(\mathbf{u}) = \prod_{j=1}^{L} P_U(u_j) = \prod_{i=1}^{K} [P_U(a_i)]^{n_{a_i}(\mathbf{u})} \tag{4.31}$$

kifejezéssel számolhatjuk, kihasználva azt, hogy a diszkrét memóriamentes forrás az egyes üzeneteket függetlenül állítja elő.

Az ε-tipikus sorozatoknál minden üzenetbetűre érvényes az

$$(1-\varepsilon) L P_U(a_i) \leq n_{a_i}(\mathbf{u}) \leq (1+\varepsilon) L P_U(a_i) \tag{4.32}$$

egyenlőtlenség.

Behelyettesítve a jobboldali egyenlőtlenséget az $\mathbf{u}$ vektor valószínűségének az összefüggésébe, az alábbi egyenlőtlenséghez jutunk

$$P_{\mathbf{U}}(\mathbf{u}) \geq \prod_{i=1}^{K} [P_U(a_i)]^{(1+\varepsilon)LP_U(a_i)} = \prod_{i=1}^{K} 2^{(1+\varepsilon)LP_U(a_i)\log_2(P_U(a_i))} = 2^{(1+\varepsilon)L\sum_{i=1}^{K} P_U(a_i)\log_2(P_U(a_i))} = 2^{-(1+\varepsilon)LH(U)}. \tag{4.33}$$

Megismételve ugyanezt a műveletet a baloldali egyenlőtlenség esetén a

$$P_{\mathbf{U}}(\mathbf{u}) \leq 2^{-(1-\varepsilon)LH(U)} \tag{4.34}$$

összefüggést kapjuk.

A tipikus sorozatok első jellemző tulajdonsága

A két egyenlőtlenség összevonásával kimondhatjuk a tipikus sorozatok első jellemző tulajdonságát, miszerint minden tipikus sorozatra érvényes a

$$2^{-(1+\varepsilon)LH(U)} \leq P_{\mathbf{U}}(\mathbf{u}) \leq 2^{-(1-\varepsilon)LH(U)} \tag{4.35}$$

egyenlőtlenség.

Ezután az kívánjuk beláttatni, hogy abban az esetben, ha L minden határon túl nő, akkor majdnem biztos, hogy a diszkrét memóriamentes forrás kimenetén minden sorozat ε-tipikus. Jelöljük B_i-vel azt az eseményt, hogy az aktuális $\mathbf{u}$ üzenetsorozat az a_i betűvel kapcsolatban nem teljesíti az ε-tipikus sorozattal kapcsolatos feltételt (így természetesen a sorozat nem tipikus sorozat), azaz

$$(1-\varepsilon) L P_U(a_i) > n_{a_i}(\mathbf{u}) \tag{4.36}$$

vagy

$$n_{a_i}(\mathbf{u}) > (1+\varepsilon) L P_U(a_i), \tag{4.37}$$

azaz ebben az esetben

$$\left| \frac{n_{a_i}}{L} - P_U(a_i) \right| > \varepsilon P_U(a_i). \tag{4.38}$$

Határozzuk meg ezután a B_i esemény valószínűségét, felhasználva a Csebisev-egyenlőtlenséget, miszerint

$$\Pr(B_i) = \Pr\left(\left| \frac{n_{a_i}}{L} - P_U(a_i) \right| > \varepsilon P_U(a_i) \right) \leq \frac{[1-P_U(a_i)]\,P_U(a_i)}{L\varepsilon^2 P_U^2(a_i)} = \frac{[1-P_U(a_i)]}{L\varepsilon^2 P_U(a_i)}, \tag{4.39}$$

ugyanis ε helyett most $\varepsilon P_U(a_i)$ a küszöbérték.

Ha P_{min}-mal jelöljük a

$$P_{min} = \min_i P_U(a_i) > 0 \tag{4.40}$$

értéket, vagyis a forrás legkisebb, de még pozitív valószínűségű betűjének a valószínűségét, akkor egyszerűen belátható, hogy

$$\Pr(B_i) < \frac{1}{L\varepsilon^2 P_{min}}. \tag{4.41}$$

Jelöljük F-fel azt az eseményt, hogy az adott $\mathbf{u}$ sorozat nem ε-tipikus, azaz van legalább egy olyan üzenetbetű, amelyre nem teljesülnek az ε-tipikusság feltételei. Ez azt jelenti, hogy

$$F = \bigcup_{i=1}^{K} B_i. \tag{4.42}$$

Ennek alapján

$$\Pr(F) = \Pr\left(\bigcup_{i=1}^{K} B_i\right) \leq \sum_{i=1}^{K} \Pr(B_i) < \frac{K}{L\varepsilon^2 P_{min}}, \tag{4.43}$$

és a kifejezésből világosan látszik, hogy annak a valószínűsége, hogy egy tetszőleges $\mathbf{u}$ sorozat nem ε-tipikus a nullához tart, ha L minden határon túl nő.

A tipikus sorozatok második jellemző tulajdonsága

A fentiek alapján kimondhatjuk, hogy L növekedésével a diszkrét memóriamentes forrás kimenetén majdnem biztos, hogy csak ε-tipikus sorozat jelenik meg, azaz

$$1 - \Pr(F) > 1 - \frac{K}{L\varepsilon^2 P_{min}}. \tag{4.44}$$

A következő célunk az ε-tipikus sorozatok számának M-nek a közelítő becslése.

M felső korlátjának meghatározásához felhasználjuk azt a tényt, hogy minden lehetséges $\mathbf{u}$ sorozatot figyelembe véve, a $P_{\mathbf{U}}(\mathbf{u})$ valószínűségek összege természetesen 1-gyel egyenlő. Felhasználva a tipikus sorozatok első jellemző tulajdonságát felírhatjuk az alábbi összefüggést

$$1 = \sum_{\texttt{minden}\ \mathbf{u}\text{-ra}} P_{\mathbf{U}}(\mathbf{u}) \geq \sum_{\texttt{minden}\ \varepsilon\text{-tipikus}\ \mathbf{u}\text{-ra}} P_{\mathbf{U}}(\mathbf{u}) \geq M 2^{-(1+\varepsilon)LH(U)}, \tag{4.45}$$

amiből az

$$M \leq 2^{(1+\varepsilon)LH(U)} \tag{4.46}$$

felső korlátot kapjuk.

M alsó korlátjának meghatározásához először ismét a tipikus sorozatok első jellemző tulajdonságát használjuk fel, ugyanis tudjuk, hogy egy $\mathbf{u}$ ε-tipikus sorozat valószínűsége

$$P_{\mathbf{U}}(\mathbf{u}) \leq 2^{-(1-\varepsilon)LH(U)}, \tag{4.47}$$

vagyis az összes ε-tipikus sorozat valószínűségeinek az összege bizosan kisebb, mint $M2^{-(1-\varepsilon)LH(U)}$.

A tipikus sorozatok második jellemző tulajdonságából viszont tudjuk, hogy annak a valószínűsége, hogy egy sorozat ε-tipikus azonos

$$1 - \Pr(F) = \sum_{\texttt{minden}\ \varepsilon\text{-tipikus}\ \mathbf{u}\text{-ra}} P_{\mathbf{U}}(\mathbf{u}), \tag{4.48}$$

és erre érvényes a

$$1 - \frac{K}{L\varepsilon^2 P_{min}} < 1 - \Pr(F) = \sum_{\texttt{minden}\ \varepsilon\text{-tipikus}\ \mathbf{u}\text{-ra}} P_{\mathbf{U}}(\mathbf{u}) \leq M 2^{-(1-\varepsilon)LH(U)}, \tag{4.49}$$

egyenlőtlenség, amiből M-re a

$$M > \left(1 - \frac{K}{L\varepsilon^2 P_{min}}\right) 2^{(1-\varepsilon)LH(U)} \tag{4.50}$$

alsó korlát adódik.

A tipikus sorozatok harmadik jellemző tulajdonsága

Ezek alapján kimondhatuk a tipikus sorozatok harmadik jellemző tulajdonságát is, miszerint az ε-tipikus sorozatok száma, M beleesik az

$$\left(1 - \frac{K}{L\varepsilon^2 P_{min}}\right) 2^{(1-\varepsilon)LH(U)} < M \leq 2^{(1+\varepsilon)LH(U)} \tag{4.51}$$

tartományba.

Érdemes megjegyezni, hogy ennek alapján, ha L elegendően nagy és ε elegendően kicsi, akkor az ε-tipikus sorozatok száma az

$$M \cong 2^{LH(U)}, \tag{4.52}$$

a B_i esemény valószínűsége pedig az

$$\Pr(B_i) \cong 2^{-LH(U)} \tag{4.53}$$

kifejezéssel közelíthető.

4.4. A diszkrét memóriamentes források blokkból blokkba kódolása

Alakítsunk ki veszteséges kódolási szabályt, ami szerint a kódolást a következőképpen végezzük el:

- Először döntsük el, hogy a forrás által előállított **u** sorozat ε-tipikus vagy nem.
- Rendeljünk kölcsönösen egyértelműen kódszavakat az ε-tipikus sorozatokhoz, azaz csak az ilyen üzenetvektorokat kódoljuk és vigyük át a csatonán.
- Válasszunk ki egy tetszőleges kódszót, amit akkor küldünk, ha az aktuális **u** sorozat nem ε-tipikus.

Ha a forrás ABC-je K, a kód ABC-je pedig D méretű, akkor az összesen $M+1$ számú üzenet kódolásához optimális esetben úgy kell N hosszúságú kódszavakat választanunk, hogy teljesüljön az

$$D^{N-1} < M+1 \leq D^N, \tag{4.54}$$

azaz a

$$D^{N-1} \leq M \tag{4.55}$$

egyenlőtlenség. Ez utóbbi mindkét oldalának a logaritmusát véve az

$$(N-1)\log_2(D) \leq \log_2(M) \leq (1+\varepsilon)LH(U) \tag{4.56}$$

kifejezéshez jutunk, amiből a kódolás hatékonyságát mérő N/L értékre az alábbi felső korlátot kapjuk

$$\frac{N}{L} \leq \frac{H(U)}{\log_2 D} + \frac{\varepsilon H(U)}{\log_2 D} + \frac{1}{L}. \tag{4.57}$$

A korábbiakból egyenesen következik, hogy a kódolás veszteségének a valószínűsége éppen $\Pr(F)$, ahol F annak az eseménynek a valószínűsége, hogy egy **u** sorozat nem tipikus.

A diszkrét memóriamentes források blokkból blokkba kódolásának a tétele

Egy K szintű ABC-vel rendelkező diszkrét memóriamentes forrás üzeneteinek D szintű ABC-vel rendelkező N hosszúságú blokkba kódolása esetén, ha veszteségeket is megengedünk a fent ismertetett algoritmus alapján, akkor az egy forrásszimbólumra eső kódszimbólumok számának a felső korlátja:

$$\frac{N}{L} < \frac{H(U)}{\log_2 D} + \varepsilon_1, \tag{4.58}$$

és a veszteség valószínűségének a felső korlátja:

$$\Pr(F) < \varepsilon_2, \tag{4.59}$$

ahol mind ε_1, mind ε_2 nullához tart, ha L minden határon túl nő. Ebből adódóan megállapítható, hogy a kódolás aszimptotikusan optimális.

5. fejezet

Csatornakódolás zajos csatornában

Ebben a fejezetben azokat az elméleti alapokat foglaljuk össze, amelyek a zajjal terhelt csatornában történő adatátvitelre vonatkoznak. Ehhez elsősorban a zajos csatorna fogalmát és matematikai leírását kell tisztázni.

5.1. Bevezetés

Először fogalmazzuk meg azt, hogy elméleti szempontból mit is jelent a csatorna. A csatorna blokkvázlatát a 5.1. ábrán adtuk meg, ahol

- $X_1, X_2, ..., X_i, ...$ a csatorna bemenetén, és
- $Y_1, Y_2, ..., Y_i, ...$ a csatorna kimenetén megjelenő szimbólumsorozat.
- Jelöljük ezen kívül $A = \{a_1, a_2, ..., a_j, ...\}$-val a bemenet, $B = \{b_1, b_2, ...b_j, ...\}$-vel pedig a kimenet véges vagy megszámlálhatóan végtelen ABC-jének az elemeit.

A hírközléselméletben a zajos csatorna annyit jelent, hogy a csatornában az adó (bemenet) és a vevő (kimenet) közötti kapcsolatot valamilyen, az adótól és vevőtől nem függő, és általában azok által nem ismert véletlen folyamat (például zaj, zavar) hatása befolyásolja. Éppen ezért a csatornát a bemeneti és kimeneti szimbólumok közötti statisztikus kapcsolatot leíró feltételes valószínűségi eloszlással lehet jellemezni. E feltételes valószínűségi eloszlás tulajdonságai alapján az alábbi csatornákat szokás megkülönböztetni:

- Ha a csatorna kimenete csak a bemenet és a kimenet korábbi szimbólumaitól függ, vagyis

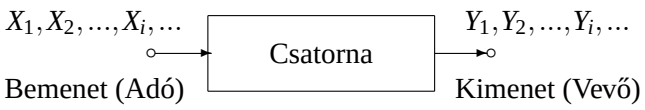
$$P(y_n \mid x_1, x_2, ..., x_{n-1}, x_n, x_{n+1}..., y_1, y_2, ..., y_{n-1}, y_{n+1}, ...) = P(y_n \mid x_1, x_2, ..., x_{n-1}, x_n, y_1, y_2, ..., y_{n-1}), \tag{5.1}$$

  akkor a csatornát **kauzálisnak** nevezzük.

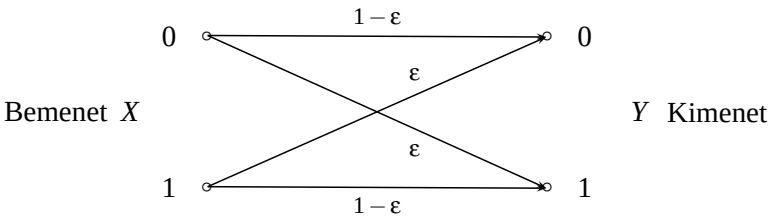
- Ha

$$P(y_n \mid x_1, x_2, ..., x_{n-1}, x_n, y_1, y_2, ..., y_{n-1}) = P_{Y|X}(y_n \mid x_n), \tag{5.2}$$

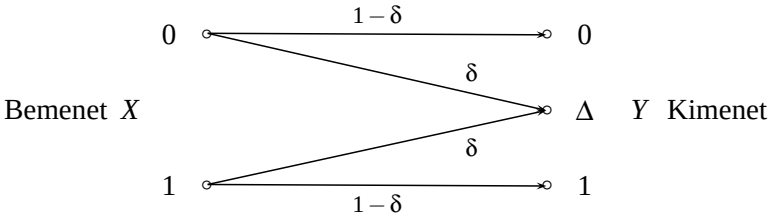
  akkor **memóriamentes csatornáról** beszélünk, mivel a csatorna aktuális kimenete (y_n) csak az aktuális bemenettől (x_n) függ.



5.1. ábra. A zajos csatorna blokkvázlata



5.2. ábra. A bináris szimmetrikus csatorna (BSC)



5.3. ábra. A bináris törléses csatorna (BEC)

- Ha a csatorna tulajdonságai nem függenek az "időtől", azaz az igénybevétel sorszámától, n-től, vagyis

$$P_{Y|X}(y_n \mid x_n) = P_{Y|X}(y \mid x), \tag{5.3}$$

akkor **időinvariáns csatornáról** beszélünk.

- Ha a csatorna bemenete nem függ a kimeneten korábban megjelenő szimbólumoktól, csak a bemenet korábbi értékeitől, azaz

$$P(x_n \mid x_1, x_2, ..., x_{n-1}, y_1, y_2, ..., y_{n-1}) = P(x_n \mid x_1, x_2, ..., x_{n-1}), \tag{5.4}$$

akkor **visszacsatolásmentes csatornáról** van szó.

Két fontos példa a memóriamentes csatornára

- **A bináris szimmetrikus csatornában** (lásd a 5.2. ábrát)

$$P_{Y|X}(0 \mid 0) = P_{Y|X}(1 \mid 1) = 1-\varepsilon \quad \text{és} \quad P_{Y|X}(0 \mid 1) = P_{Y|X}(1 \mid 0) = \varepsilon, \tag{5.5}$$

tehát a hiba mértéke ε.

- **A bináris törléses csatornában** (lásd a 5.3. ábrát)

$$P_{Y|X}(0 \mid 0) = P_{Y|X}(1 \mid 1) = 1-\delta \quad \text{és} \quad P_{Y|X}(\Delta \mid 1) = P_{Y|X}(\Delta \mid 0) = \delta, \tag{5.6}$$

ami annyit jelent, hogy a Δ-val jelölt törlés valószínűsége éppen δ.

5.1. Tétel

A **diszkrét memóriamentes és visszacsatolásmentes csatornára** érvényes az alábbi összefüggés:

$$P(y_1, y_2, ..., y_n \mid x_1, x_2, ..., x_n) = \prod_{i=1}^{n} P_{Y|X}(y_i \mid x_i), \tag{5.7}$$

azaz a kimeneti szimbólumsorozat feltételes eloszlása (feltéve, hogy a bemeneti sorozat ismert) szorzat alakban írható fel, ahol az egyes szorzótényezők az egyes kimeneti szimbólumok feltételes eloszlásai, ha a hozzájuk tartozó bemeneti szimbólum adott.

Bizonyítás

Tudjuk, hogy a korábban megismert láncszabály szerint a bemeneti és kimeneti sorozatok együttes eloszlása felírható feltételes eloszlások szorzataként az alábbi alakban:

$$P(x_1, x_2, ..., x_n, y_1, y_2, ..., y_n) = \prod_{i=1}^{n} P(x_i \mid x_1, x_2, ..., x_{i-1}, y_1, y_2, ..., y_{i-1}) P(y_i \mid x_1, x_2, ..., x_i, y_1, y_2, ..., y_{i-1}). \tag{5.8}$$

Ha figyelembe vesszük, hogy a csatorna memóriamentes és visszacsatolásmentes, akkor a definíciókat felhasználva a

$$P(x_1,x_2,...,x_n,y_1,y_2,...,y_n) = \prod_{i=1}^{n} P(x_i \mid x_1,x_2,...,x_{i-1}) P_{Y|X}(y_i \mid x_i) =$$

$$= \prod_{i=1}^{n} P(x_i \mid x_1,x_2,...,x_{i-1}) \prod_{i=1}^{n} P_{Y|X}(y_i \mid x_i) = P(x_1,x_2,...,x_n) \prod_{i=1}^{n} P_{Y|X}(y_i \mid x_i), \tag{5.9}$$

kifejezést kapjuk, amiből a két oldalnak $P(x_1,x_2,...,x_n)$-val való osztása után a

$$P(y_1,y_2,...,y_n \mid x_1,x_2,...,x_n) = \frac{P(x_1,x_2,...,x_n,y_1,y_2,...,y_n)}{P(x_1,x_2,...,x_n)} = \prod_{i=1}^{n} P_{Y|X}(y_i \mid x_i) \tag{5.10}$$

összefüggéshez jutunk. Ezzel a tételt bebizonyítottuk.

Példa

Alkalmazzuk a fenti tételt a bináris szimmetrikus csatorna (BSC) esetén. Mint korábban láttuk

$$P_{Y|X}(y \mid x) = \begin{cases} 1-\varepsilon, & \texttt{ha } x = y \\ \varepsilon, & \texttt{ha } x \neq y \end{cases}. \tag{5.11}$$

Ezt felhasználva:

$$P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}) = (1-\varepsilon)^{N-d(\mathbf{x},\mathbf{y})} \varepsilon^{d(\mathbf{x},\mathbf{y})} = (1-\varepsilon)^N \left(\frac{\varepsilon}{1-\varepsilon}\right)^{d(\mathbf{x},\mathbf{y})}. \tag{5.12}$$

5.2. A csatorna kapacitása

Először adjuk meg a csatornakapacitás definícióját.

5.1. Definíció

Legyen egy diszkrét memóriamentes csatorna (DMC) feltételes valószínűségi eloszlása $P_{Y|X}(y \mid x)$, és tételezzük fel, hogy az adó a csatorna bemenetén szabadon megválaszthatja a bemeneti X üzenet $P_X(x)$ valószínűségi eloszlását. Ekkor a diszkrét memóriamentes csatorna C **kapacitása** nem más, mint az X és Y valószínűségi változók $I(X;Y)$ kölcsönös információjának maximuma, amit optimális bemeneti eloszlás $P_X(x)$ mellett lehet elérni, azaz:

$$C = \max_{P_X} [I(X;Y)] = \max_{P_X} [H(Y) - H(Y \mid X)]. \tag{5.13}$$

A csatorna kapacitásának a kiszámítása néhány speciális csatorna esetén

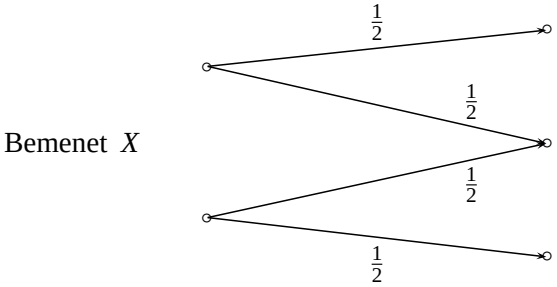
A csatorna kapacitását általános esetben zárt alakban nem lehet kiszámítani, mivel az $I(X;Y)$ kölcsönös információ $P_X(x)$ szerinti maximumának a megkeresése általában igen komplex feladat. Van azonban néhány olyan egyszerű csatorna, amelynél ez az optimumkeresés zárt alakban megoldható akkor, ha a csatorna teljesít néhány speciális feltételt. A következőkben ezeket a feltételeket fogjuk elemezni. Jelöljük az X bemenet ABC-jének a méretét K-val, az Y kimenetét pedig J-vel.

5.2. Definíció

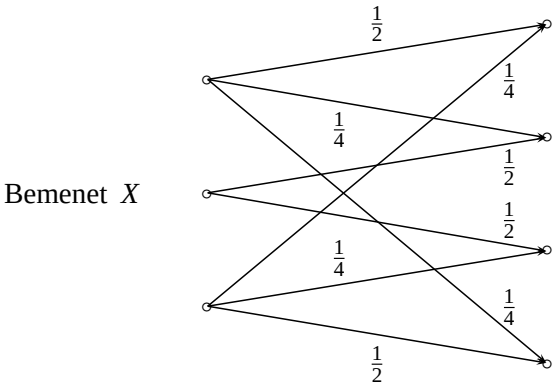
Egyenletes diszperzív csatornáról beszélünk akkor, ha minden bemenetről kiinduló J számú átmenet ugyanolyan feltételes valószínűségi eloszlású, függetlenül attól, hogy az átmenet melyik bemeneti betűtől indult el (lásd az 5.4. ábrát).

Egyenletesen fókuszáló csatornáról beszélünk, ha a bemenetről minden egyes kimenethez érkező K számú átmenet ugyanazt a K számú feltételes valószínűségi értéket veszi fel, függetlenül attól, hogy melyik kimeneti betűről van szó (lásd az 5.5. ábrát).

5.1. Segédtétel



5.4. ábra. Példa az egyenletesen diszperzív csatornára



5.5. ábra. Példa az egyenletesen fókuszáló csatornára

Függetlenül az $P_X(x)$ bemenet eloszlásától egyenletesen diszperzív csatorna esetén az Y feltételes entrópiájára igaz, hogy

$$H(Y \mid X) = -\sum_{j=1}^{J} p_j \log(p_j), \tag{5.14}$$

ahol $p_1, p_2, ..., p_J$ egy tetszőleges bemeneti betűtől induló átmenetek valószínűségeinek az értéke.

Bizonyítás

A bemenet egy betűjét, a_k kiválasztva az Y feltételes entrópiája, feltéve, hogy $X = a_k$ az alábbi formában írható fel:

$$H(Y \mid X = a_k) = -\sum_{j=1}^{J} p_j \log(p_j), \tag{5.15}$$

és az egyenletesen diszperzív csatorna definíciójából következik, hogy ez minden $a_k, \quad k = 1, 2, ..., J$ esetében azonos. Felhasználva a $H(Y \mid X)$ definícióját a

$$H(Y \mid X) = \sum_{j=1}^{J} H(Y \mid X = a_k) P_X(a_k) = H(Y \mid X = a_k) \sum_{j=1}^{J} P_X(a_k) = H(Y \mid X = a_k) = -\sum_{j=1}^{J} p_j \log(p_j), \tag{5.16}$$

amivel a segédtételt bebizonyítottuk.

Példa

Az általunk mintának használt két csatorna, a bináris szimmetrikus és a bináris törléses csatorna esetén a $H(Y \mid X)$-re az alábbi értékek adódnak:

- Bináris szimmetrikus csatornában:

$$H(Y \mid X) = -\varepsilon \log(\varepsilon) - (1-\varepsilon) \log(1-\varepsilon) = h(\varepsilon). \tag{5.17}$$

- Bináris törléses csatornában:

$$H(Y \mid X) = -\delta \log(\delta) - (1-\delta)\log(1-\delta) = h(\delta). \tag{5.18}$$

Az 5.1. Segédtétel következménye

Tetszőleges egyenletesen diszperzív csatorna kapacitását a

$$C = \max_{P_X}[H(Y)] + \sum_{j=1}^{J} p_j \log(p_j) \tag{5.19}$$

kifejezéssel határozhatjuk meg, ahol $p_1, p_2, ..., p_J$ egy tetszőleges bemeneti betűtől induló átmenetek valószínűségeinek az értéke.

5.2. Segédtétel

Ha egy K szintű bemenettel és J szintű kimenettel rendelkező diszkrét memóriamentes csatorna egyenletesen fókuszáló, akkor egyenletes eloszlású bemenethez $(P_X(x) = 1/K)$ egyenletes eloszlású kimenet $(P_Y(y) = 1/J)$ tartozik.

Bizonyítás

A peremeloszlások számítási szabálya és a feltételes eloszlás definíciója alapján

$$P_Y(y) = \sum_x P_{X,Y}(x,y) = \sum_x P_{Y|X}(y \mid x) P_X(x) = \frac{1}{K} \sum_x P_{Y|X}(y \mid x), \tag{5.20}$$

viszont ez az összeg az egyenletesen fókuszáló tulajdonság következtében minden kimenet esetén azonos függetlenül a J számú $Y = y$ aktuális értéktől.

Az 5.2. Segédtétel következménye

Az 5.2. Segédtétel alapján egy K bemenetű egyenletesen fókuszáló diszkrét memóriamentes csatornában fennáll, hogy

$$\max_{P_X}[H(Y)] = \log(J), \tag{5.21}$$

és ez a maximum a

$$P_X(x) = \frac{1}{K} \quad \texttt{minden } x\texttt{-re} \tag{5.22}$$

egyenletes bemeneti eloszláshoz tartozik.

5.2 Tétel

Egy **erősen szimmetrikus** (egyenletesen diszperzív és egyenletesen fókuszáló) diszkrét memóriamentes K bemenetű és J kimenetű csatorna kapacitása

$$C = \log(J) + \sum_{j=1}^{J} p_j \log(p_j), \tag{5.23}$$

és ez a kapacitás egyenletes a

$$P_X(x) = \frac{1}{K} \quad \texttt{minden } x\texttt{-re} \tag{5.24}$$

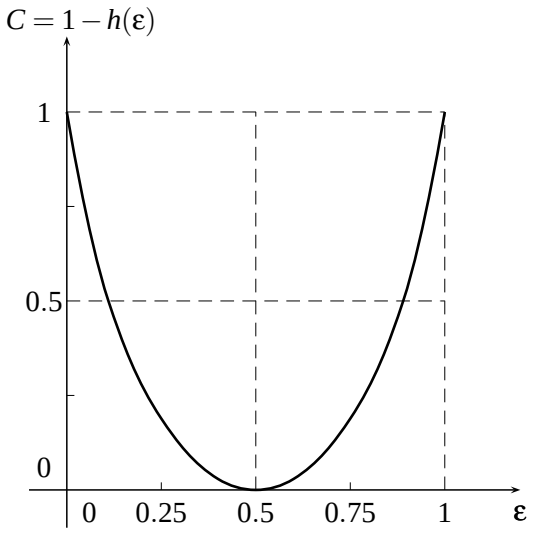
bemeneti eloszlás esetén érhető el.

Példa

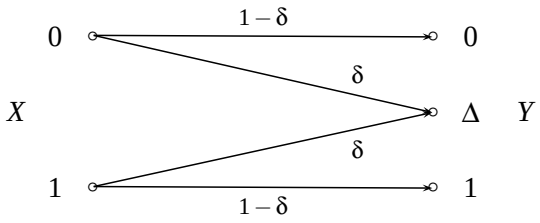
A bináris szimmetrikus csatorna (BSC) teljesíti az erősen szimmetrikus csatorna mindkét feltételét, azaz egyenletesen diszperzív és egyenletesen fókuszáló is, ezért a kapacitását az 5.2 Tétel alapján igen egyszerűen meg lehet határozni:

$$C = 1 + \varepsilon \log(\varepsilon) + (1-\varepsilon)\log(1-\varepsilon) = 1 - h(\varepsilon). \tag{5.25}$$

A függvényt az 5.6. ábrán adtuk meg. Az ábra alapján megállapítható, hogy maximális hibaarány, $\varepsilon = 0.5$ esetén a csatorna kapacitása nulla, míg $\varepsilon = 0$ vagy $\varepsilon = 1$ esetén a kapacitás maximális. Érdekes



5.6. ábra. A bináris szimmetrikus csatorna kapacitása az ε függvényében



5.7. ábra. A bináris törléses csatorna (BEC)

megjegyezni, hogy az utóbbi esetben a csatorna egyszerű logikai inverterként működik, ezért a bemenet egyértelműen meghatározza a kimenetet, ami a kölcsönös információt maximalizálja, ugyanis ilyenkor $H(Y \mid X) = 0$, így

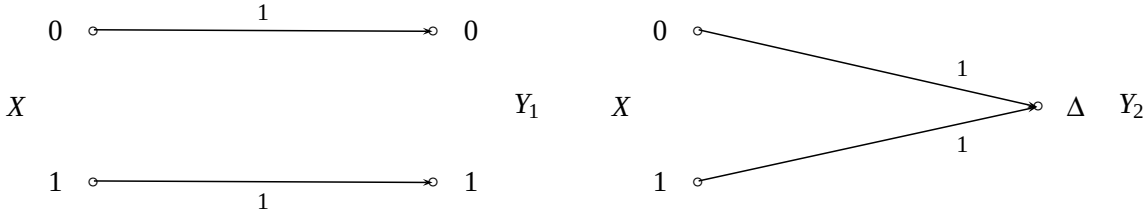
$$C = \max_{P_X} [I(X;Y)] = \max_{P_X} [H(Y) - H(Y \mid X)] = \max_{P_X} [H(Y)] = \log(J), \tag{5.26}$$

ha Y egyenletes eloszlású.

Felvetődik a kérdés, hogy megadható-e zárt alakban a bináris törléses csatorna kapacitása. A válasz a kérdésre igen, de a kapacitás konkrét meghatározása előtt még néhány fogalmat tisztázni kell.

A "szimmetria" általános definíciója

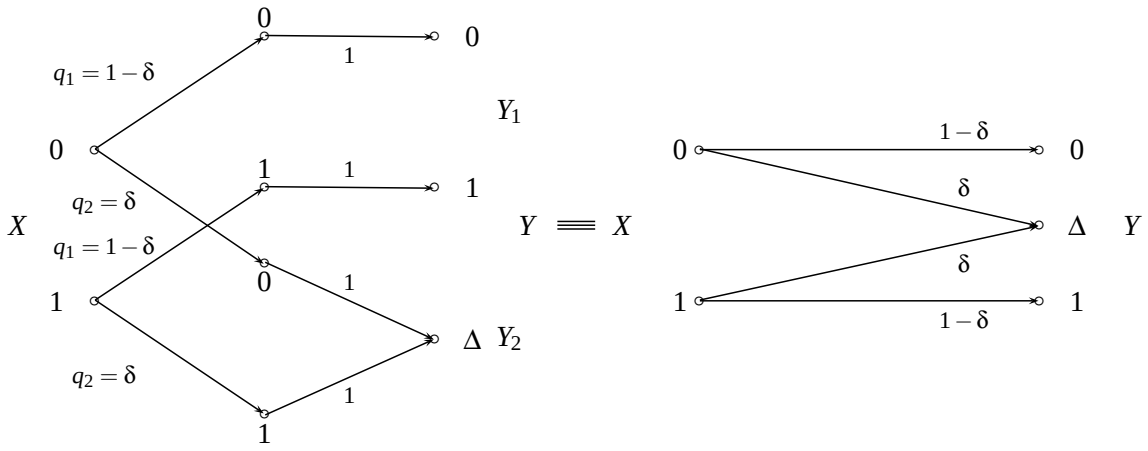
A definíciót a bináris törléses csatorna példájával illusztráljuk (lásd az 5.7. ábrát). Az ábrából észrevehető, hogy ez a csatorna két igen egyszerű erősen szimmetrikus csatornára bontható az 5.8. ábra szerint. A baloldali csatorna kapacitása 1, a jobboldalié pedig 0, és annak a valószínűsége, hogy



$C_1 = 1$ $C_2 = 0$

$q_1 = 1 - \delta$ $q_2 = \delta$

5.8. ábra. A bináris törléses csatorna (BEC) szimmetrikus felbontása



5.9. ábra. A bináris törléses csatorna (BEC) szimmetrikus felbontásának ekvivalenciája az eredeti csatornával

a rendszer a baloldali csatornára "kapcsol" egyenlő $1-\delta$-val, illetve, hogy a jobboldali csatornára "kapcsol" egyenlő δ-val.

A példa alapján megfogalmazhatjuk a csatorna szimmetrikusságának általános definícióját.

A 5.9. ábra alapján egy csatorna szimmetrikus, ha teljesülnek az alábbi feltételek:

- Felbontható a csatorna Y kimenetének az értékkészlete L számú egymással át nem fedő (ortogonális) $\{Y_i\}\quad i = 1,2,...,L$ részhalmazra oly módon, hogy az egyes részhalmazok és a bemenet között erősen szimmetrikus csatornák teremtik meg a kapcsolatot.
- Emellett az egyes erősen szimmetrikus csatornákat a $q_1, q_2, ..., q_L$ úgynevezett szelekciós valószínűségekkel választjuk ki.

Fontos megjegyezni, hogy ezek a feltételek csak igen speciális esetben teljesülnek, de a bináris törléses csatorna esetén igazak, mivel az 5.9. ábra szerint az Y értékkészletét sikerült az $Y_1 = \{0,1\}$ és a $Y_2 = \{\Delta\}$ részhalmazokra felbontani úgy, hogy ezek és a bemenet között az 5.8. ábrán bemutatott erősen szimmetrikus csatornák teremtik meg a kapcsolatot, ugyanakkor teljesül az is, hogy a két erősen szimmetrikus csatorna kiválasztási valószínűségei rendre $q_1 = 1-\delta$ és $q_2 = \delta$. Az eljárásból az is következik, hogy az i-dik erősen szimmetrikus csatorna kiválasztása esetén az Y kimenet Y_i részhalmazát is kiválasztottuk, azaz az i-dik erősen szimmetrikus részcsatorna kimenetén csak az Y_i elemei találhatók.

5.3. Tétel

A szimmetrikus diszkrét memóriamentes csatorna kapacitása

$$C = \sum_{i=1}^{L} q_i C_i, \tag{5.27}$$

ahol $\{C_i\}\quad i = 1,2,...,L$ az egyes erősen szimmetrikus részcsatornák kapacitása, $\{q_i\}\quad i = 1,2,...,L$ pedig az erősen szimmetrikus részcsatornák szelekciós valószínűsége.

Bizonyítás

A korábban ismertetett felbontási eljárás szerint a szimmetrikus diszkrét memóriamentes csatorna felbontható L számú erősen szimmetrikus részcsatornára, és az egyes részcsatornák $q_1, q_2, ..., q_L$ valószínűséggel kerülnek kiválasztásra. Legyen Z a szelekció véletlen eseményével kapcsolatos indikátor típusú valószínűségi változó, amely akkor veszi fel a $Z = i$ értéket, ha éppen az i-dik csatorna került kiválasztásra, azaz $P_Z(i) = q_i$.

A fentiek alapján tudjuk, hogy

$$H(Z \mid Y) = 0, \tag{5.28}$$

mivel Y egyértelműen meghatározza Z értékét, ugyanis az $\{Y_i\}\quad i=1,2,...,L$ részhalmazok ortogonálisak.

Helyettesítsük be ezt az eredményt az együttes entrópiára vonatkozó ismert összefüggésbe

$$H(YZ)=H(Y)+H(Z\mid Y)=H(Y), \tag{5.29}$$

ugyanakkor az együttes entrópiát a

$$H(YZ)=H(Z)+H(Y\mid Z)=H(Z)+\sum_{i=1}^{L}H(Y\mid Z=i)P_Z(i)=H(Z)+\sum_{i=1}^{L}H(Y\mid Z=i)q_i \tag{5.30}$$

kifejezés segítségével is meghatározhatjuk, amiből

$$H(Y)=H(Z)+\sum_{i=1}^{L}H(Y\mid Z=i)q_i. \tag{5.31}$$

Ezekhez a lépésekhez hasonlóan tudjuk azt is, hogy

$$H(Z\mid XY)=0, \tag{5.32}$$

mivel Y, így X és Y együttesen is egyértelműen meghatározzák Z értékét.

Ha ezt az eredményt behelyettesítjük a feltételes együttes entrópiára vonatkozó ismert összefüggésbe, akkor a

$$H(YZ\mid X)=H(Y\mid X)+H(Z\mid XY)=H(Y\mid X), \tag{5.33}$$

kifejezéshez jutunk, ugyanakkor a feltételes együttes entrópiát a

$$H(YZ\mid X)=H(Z\mid X)+H(Y\mid XZ)=H(Z\mid X)+\sum_{i=1}^{L}H(Y\mid X,Z=i)P_Z(i)=$$

$$=H(Z\mid X)+\sum_{i=1}^{L}H(Y\mid X,Z=i)q_i \tag{5.34}$$

kifejezés segítségével is meghatározhatjuk, amiből

$$H(Y\mid X)=H(Z\mid X)+\sum_{i=1}^{L}H(Y\mid X,Z=i)q_i. \tag{5.35}$$

Tudjuk azonban, hogy a csatornák közötti szelekció csak a csatornában lejátszódó véletlen eseményektől függ és független a csatorna bemenetétől, ezért

$$H(Z\mid X)=H(Z), \tag{5.36}$$

mivel az X és Z függetlenek egymástól, íly módon

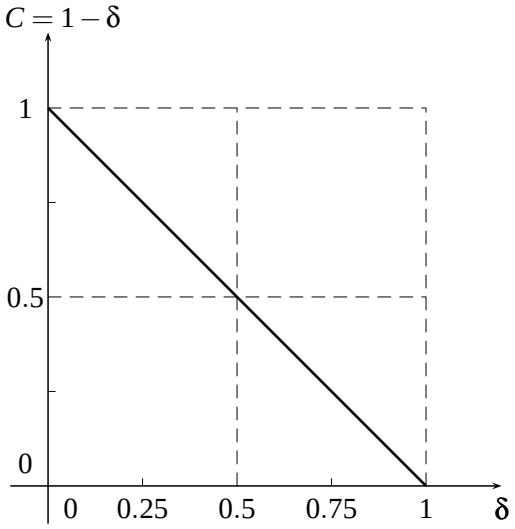
$$H(Y\mid X)=H(Z)+\sum_{i=1}^{L}H(Y\mid X,Z=i)q_i. \tag{5.37}$$

Használjuk fel ezután a kölcsönös információ definícióját, miszerint

$$I(X;Y)=H(Y)-H(Y\mid X), \tag{5.38}$$

és helyettesítsük be ebbe a kifejezésbe az előbb kapott összefüggéseket:

$$I(X;Y)=H(Z)+\sum_{i=1}^{L}H(Y\mid Z=i)q_i-H(Z\mid X)-\sum_{i=1}^{L}H(Y\mid X,Z=i)q_i=$$



5.10. ábra. A bináris törléses csatorna kapacitása a δ függvényében

$$= H(Z) + \sum_{i=1}^{L} H(Y \mid Z=i)\, q_i - H(Z) - \sum_{i=1}^{L} H(Y \mid X, Z=i)\, q_i = \sum_{i=1}^{L} [H(Y \mid Z=i) - H(Y \mid X, Z=i)]\, q_i. \tag{5.39}$$

Ha az i-dik csatornát egyedül vizsgáljuk, akkor a kapacitására igaz az alábbi összefüggés

$$I_i(X;Y) = H(Y \mid Z=i) - H(Y \mid X, Z=i) \le C_i, \tag{5.40}$$

és az egyenlőség az erősen szimmetrikus részcsatornában akkor áll fent, ha a bemenet egyenletes eloszlású, és az kölcsönös információ várható értéke ekkor a

$$I(X;Y) = \sum_{i=1}^{L} I_i(X;Y)\, q_i = \sum_{i=1}^{L} [H(Y \mid Z=i) - H(Y \mid X, Z=i)]\, q_i \le C \tag{5.41}$$

kifejezéssel határozható meg.

Mivel az egyenletes bemeneti eloszlás minden erősen szimmetrikus részcsatorna kölcsönös információját egyszerre maximalizálja a fentiekből egyenesen következik, hogy

$$C = \max_{P_X} I(X;Y) = \sum_{i=1}^{L} C_i q_i, \tag{5.42}$$

amivel a tételt bebizonyítottuk.

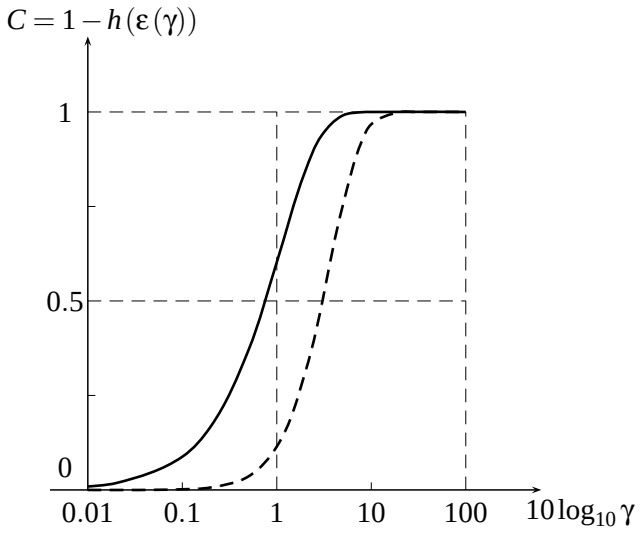
Példa

Az ismertetett tétel alapján a bináris törléses csatorna kapacitása egyszerűen számítható, mivel

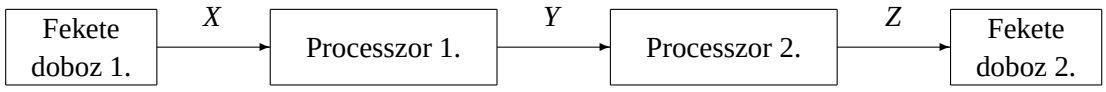
$$C = C_1 q_i + C_2 q_2 = 1\,(1-\delta) + 0\,\delta = 1-\delta. \tag{5.43}$$

A kapacitás értékét az 5.10. ábrán adjuk meg a δ függvényében.

A kapacitás kalkulációjához érdekességképpen adjuk meg egy bináris szimmetrikus fehér Gauss-zajos csatorna kapacitását optimális koherens és nem koherens vétel esetén, ha az ε hibaarány az $\varepsilon = \frac{1}{2}\operatorname{erfc}\left(\sqrt{\gamma}\right)$, illetve az $\varepsilon = \frac{1}{2}\exp\left(-\frac{\gamma}{2}\right)$ kifejezés szerint függ a γ jel-zaj viszonytól. Az eredményeket az 5.11. ábrázoltuk, ahol a koherens csatorna adatait folytonos, a nem koherens csatornáét szaggatott vonallal adtuk meg.



5.11. ábra. A bináris szimmetrikus fehér Gauss-zajos csatorna kapacitása a γ jel-zaj viszony függvényében koherens és nem koherens optimális vevő esetén



$P(z \mid xy) = P(z \mid y)$ Markov-lánc

5.12. ábra. Az adatfeldolgozási segédtétel illusztrációja

5.3. Az adatfeldolgozási segédtétel és a Fano-segédtétel

A következőkben azt kívánjuk megvizsgálni, hogy az információ átvitele során az adatok statisztikai kapcsolata milyen módon változik, illetve arra milyen korlátok érvényesek. Ennek érdekében kimondunk két fontos segédtételt, amelyek a zajos csatornával kapcsolatos általános tételek előkészítését szolgálják.

Az adatfeldolgozási segédtétel

Az 5.12. ábrán megadott általános adatátviteli rendszerre érvényesek az alábbi állítások

$$I(X;Z) \leq I(X;Y). \tag{5.44}$$

és

$$I(X;Z) \leq I(Y;Z), \tag{5.45}$$

ha fennáll az, hogy Z csak y-on keresztül függ X-től, azaz $P(z \mid xy) = P(z \mid y)$, tehát X, Y és Z Markov-láncot alkot. Az fenti egyenlőtlenségek annyit jelentenek, hogy függetlenül a processzorokban elvégzett tetszőleges adatfeldolgozástól az X és Z valószínűségi változók kölcsönös információja biztosan nem nagyobb, mint az X és Y, illetve az Y és Z kölcsönös információja.

Bizonyítás

Ha az X, Y és Z valószínűségi változók Markov-láncot alkotnak, akkor fennáll a

$$H(Z \mid XY) = H(Z \mid Y) \tag{5.46}$$

összefüggés. Ugyanakkor tudjuk, hogy

$$H(Z \mid XY) \leq H(Z \mid X), \tag{5.47}$$

így

$$I(X;Z) = H(Z) - H(Z \mid X) \leq H(Z) - H(Z \mid XY). \tag{5.48}$$

Ebből a Markov-tulajdonság felhasználásával az

$$I(X;Z) \leq H(Z) - H(Z \mid XY) = H(Z) - H(Z \mid Y) = I(Y;Z), \tag{5.49}$$

kifejezést kapjuk, amivel a segédtétel első állítását bebizonyítottuk.

A segédtétel második állításának igazolásához felírhatjuk, hogy

$$I(X;Z) = H(X) - H(X \mid Z) \leq H(X) - H(X \mid YZ) = I(X;YZ), \tag{5.50}$$

és mivel

$$I(X;YZ) = H(X) - H(X \mid YZ) = H(X) - H(X \mid Y) + H(X \mid Y) - H(X \mid YZ) = I(X;Y) + I(X;Z \mid Y), \tag{5.51}$$

egyszerűen belátható, hogy

$$I(X;Z) \leq I(X;YZ) = I(X;Y) + I(X;Z \mid Y) = I(X;Y) + H(Z \mid Y) - H(Z \mid XY) = I(X;Y), \tag{5.52}$$

amivel a segédtétel második részét is bebizonyítottuk.

A továbbiakban az a fő célunk, hogy kapcsolatot teremtsünk a hibaarány és a csatorna bemenetén és kimenetén lévő jelek feltételes entrópiája között. Erre azért van szükség, hogy előkészítsük a zajos csatornákra vonatkozó fontos kódolási tétel kimondását.

Legyen U egy tetszőleges valószínűségi változó és $\widehat{U}$ ennek a változónak a becslése, és adjunk felső korlátot a $H\left(U \mid \widehat{U}\right)$ feltételes entrópiára. A Fano-segédtétel ismertetéséhez vezessük be az $\widehat{U} \neq U$ hiba fogalmát, amelynek a valószínűsége $P_e = Pr\left(\widehat{U} \neq U\right)$.

A Fano-segédtétel

Ha U és $\widehat{U}$ egyaránt L ABC-vel rendelkező valószínűségi változók, akkor

$$H\left(U \mid \widehat{U}\right) \leq h(P_e) + P_e \log_2(L-1), \tag{5.53}$$

ahol $H\left(U \mid \widehat{U}\right)$ bitekben van megadva.

Bizonyítás

Legyen Z a hiba indikátora, azaz

$$Z = \begin{cases} 0, & \texttt{ha } U = \widehat{U} \\ 1, & \texttt{ha } U \neq \widehat{U} \end{cases}. \tag{5.54}$$

Nyilvánvaló, hogy Z entrópiája a bináris entrópia függvénnyel adható meg, így

$$H(Z) = h(P_e). \tag{5.55}$$

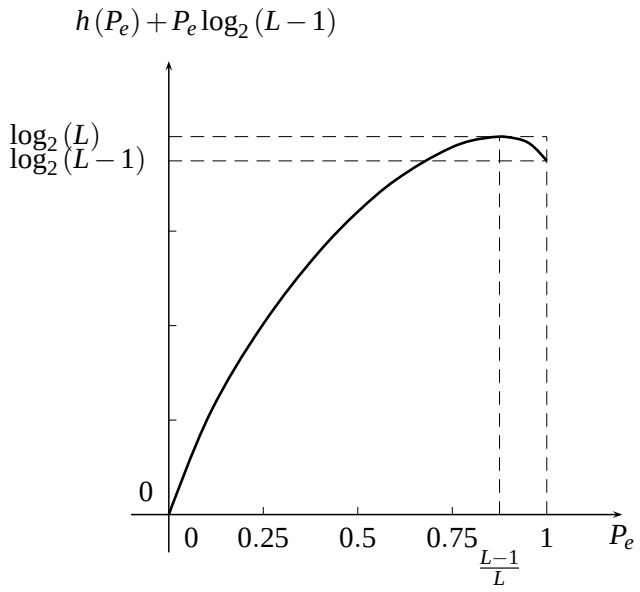
Írjuk fel ezután az U és Z valószínűségi változók együttes feltételes entrópiáját, ha az $\widehat{U}$ valószínűségi változó adott:

$$H\left(UZ \mid \widehat{U}\right) = H\left(U \mid \widehat{U}\right) + H\left(Z \mid U\widehat{U}\right) = H\left(U \mid \widehat{U}\right), \tag{5.56}$$

mivel Z definíciójából következik, hogy U és $\widehat{U}$ együttes ismerete egyértelműen meghatározza Z-t, vagyis $H\left(Z \mid U\widehat{U}\right) = 0$.

Ezt az eredményt felhasználva a

$$H\left(U \mid \widehat{U}\right) = H\left(UZ \mid \widehat{U}\right) = H\left(Z \mid \widehat{U}\right) + H\left(U \mid \widehat{U}Z\right) \leq H(Z) + H\left(U \mid \widehat{U}Z\right) \tag{5.57}$$



5.13. ábra. A Fano-segédtétel illusztrációja

egyenlőtlenséghez jutunk, mivel korábbról tudjuk, hogy tetszőleges X, Y és V valószínűségi változók esetén igaz az alábbi két állítás:

$$H(XY \mid V) = H(X \mid V) + H(Y \mid XV) \quad \text{és} \quad H(X \mid V) \leq H(X). \tag{5.58}$$

Visszatérve a Z valószínűségi változó definíciójához tudjuk, hogy

$$H\left(U \mid \widehat{U}, Z = 0\right) = 0, \tag{5.59}$$

mivel $Z = 0$ esetén $\widehat{U}$ egyértelműen meghatározza U-t, és

$$H\left(U \mid \widehat{U}, Z = 1\right) \leq \log_2(L-1), \tag{5.60}$$

mivel $Z = 1$ esetén adott $\widehat{U}$ mellett U éppen $L-1$ lehetséges értéket vehet fel (L értékből ugyanis $L-1$ olyan eset van, amikor $U \neq \widehat{U}$), és az entrópia maximuma éppen $\log_2(L-1)$.

Felhasználva a fenti összefüggéseket a $H\left(U \mid \widehat{U}Z\right)$-re a

$$H\left(U \mid \widehat{U}Z\right) \leq \Pr(Z=1)\log_2(L-1) + \Pr(Z=0)\times 0 = P_e \log_2(L-1) \tag{5.61}$$

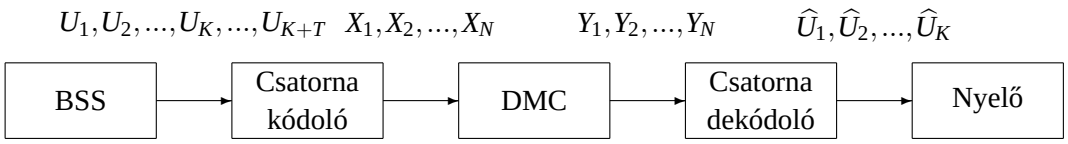
felső korlát adódik, és ebből az 5.57. egyenlet alapján a

$$H\left(U \mid \widehat{U}\right) \leq h(P_e) + P_e \log_2(L-1) \tag{5.62}$$

kifejezéshez jutunk, amivel a segédtételt bebizonyítottuk.

A Fano-segédtétel jobb oldalán szereplő kifejezést az 5.13. ábrán adtuk meg a P_e függvényében.

Az ábra alapján megállapítható, hogy a függvény az $P_e = (L-1)/L$ helyen veszi fel a $\log_2(L)$ értékű maximumát, a $P_e = 1$ helyen pedig $\log_2(L-1)$ értékű.



5.14. ábra. Az adatátviteli rendszer általános felépítése

5.4. A zajos diszkrét memóriamentes csatorna kódolási tételének a megfordítása

Vizsgáljuk meg a 5.14. ábrán megadott általános adatátviteli struktúrát, ahol

- A forrás szimmetrikus bináris és memóriamentes (BSS),
- A csatorna diszkrét és memóriamentes (DMC),
- $U_i \ \ (i=1,2,...,K+T)$ a forrás kimenetén megjelenő bináris valószínűségi változók sorozata, $K+T$ azoknak a forrásszimbólumoknak a száma, amelyekhez a csatorna kódoló egy N blokkhosszúságú kódszót rendel,
- $\widehat{U}_i \ \ (i=1,2,...,K)$ a csatorna dekódoló kimenetén megjelenő bináris valószínűségi változók sorozata, az $U_i \ \ (i=1,2,...,K)$ sorozat becslése,
- X_i és $Y_i \ \ (i=1,2,...,N)$ rendre a csatorna i-dik bemeneti és kimeneti szimbóluma, N a kódszó hossza,
- és $R=K/N$ [bit/igénybevétel] az átviteli sebesség, amit az egy csatornaszimbólumra jutó forrásbitek számával mérünk.

Renszerünkben tehát a csatorna kódoló $K+T$ számú $\{U_i\}$ forrásbithez N hosszúságú kódszavakat rendel, és azokat N lépésben, kódbetűnként átviszi a diszkrét memóriamentes csatornán, majd a csatorna kimenetén megjelenő szimbólumokból a csatorna dekódoló előállítja az $\left\{\widehat{U}_i\right\}$ sorozatot, az $\{U_i\}$ sorozat becslését.

Az 5.14. ábra elemzése előtt lássuk be, hogy

$$I\left(U_1,U_2,...,U_K,...,U_{K+T};\widehat{U}_1,\widehat{U}_2,...,\widehat{U}_K\right)\leq I\left(U_1,U_2,...,U_K;\widehat{U}_1,\widehat{U}_2,...,\widehat{U}_K\right), \tag{5.63}$$

ami azért igaz, mert az $U_1,U_2,...,U_K$ valószínűségi változó vektor az $U_1,U_2,...,U_K,...,U_{K+T}$ valószínűségi változó vektorból processzálással állítható elő oly módon, hogy az második vektor $U_{K+1},...,U_{K+T}$ elemeit az eredeti vektorból töröljük. Emellett igaz, hogy az $U_1,U_2,...,U_K$ vektor csak az $U_1,...,U_{K+T}$ vektortól függ, így közöttük fennáll a Markov-lánc tulajdonság.

Alkalmazva az adatfeldolgozási segédtételt felírható, hogy

$$I\left(U_1,U_2,...,U_K,...,U_{K+T};\widehat{U}_1,\widehat{U}_2,...,\widehat{U}_K\right)\leq I\left(U_1,U_2,...,U_K;\widehat{U}_1,\widehat{U}_2,...,\widehat{U}_K\right)\leq$$

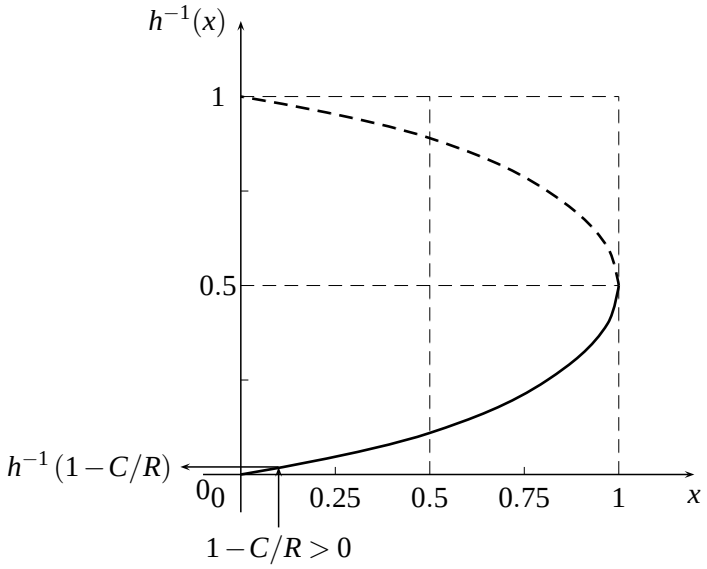
$$\leq I\left(X_1,X_2,...,X_N;\widehat{U}_1,\widehat{U}_2,...,\widehat{U}_K\right)\leq I\left(X_1,X_2,...,X_N;Y_1,Y_2,...,Y_N\right), \tag{5.64}$$

ezért

$$I\left(U_1,U_2,...,U_K;\widehat{U}_1,\widehat{U}_2,...,\widehat{U}_K\right)\leq I\left(X_1,X_2,...,X_N;Y_1,Y_2,...,Y_N\right). \tag{5.65}$$

Ezután felhasználva, hogy diszkrét memóriamentes csatornában

$$H\left(Y_1,Y_2,...,Y_N\mid X_1,X_2,...,X_N\right)=\sum_{i=1}^{N}H\left(Y_i\mid X_i\right) \tag{5.66}$$



5.15. ábra. A bináris entrópia függvény inverze, ha $x \geq 0$ és $h(x) \leq 0.5$

és, hogy

$$H(Y_1, Y_2, ..., Y_N) \leq \sum_{i=1}^{N} H(Y_i), \tag{5.67}$$

behelyettesítések után az

$$I\left(U_1, U_2, ..., U_K; \widehat{U}_1, \widehat{U}_2, ..., \widehat{U}_K\right) \leq I(X_1, X_2, ..., X_N; Y_1, Y_2, ..., Y_N) =$$

$$= H(Y_1, Y_2, ..., Y_N) - H(Y_1, Y_2, ..., Y_N \mid X_1, X_2, ..., X_N) = H(Y_1, Y_2, ..., Y_N) - \sum_{i=1}^{N} H(Y_i \mid X_i) \leq$$

$$\leq \sum_{i=1}^{N} [H(Y_i) - H(Y_i \mid X_i)] = \sum_{i=1}^{N} I(X_i; Y_i) \leq NC \tag{5.68}$$

egyenlőtlenséghez jutunk, mivel a kapacitás definíciójából $I(X_i; Y_i) \leq C, \;\; i = 1, 2, ..., N$.

A hosszadalmas levezetés végeredményeképpen bebizonyítottuk, hogy esetünkben az $U_1, U_2, ..., U_K$ és $\widehat{U}_1, \widehat{U}_2, ..., \widehat{U}_K$ vektorok közötti kölcsönös információ nem lehet nagyobb, mint a csatorna kapacitásának az N-szerese, azaz

$$I\left(U_1, U_2, ..., U_K; \widehat{U}_1, \widehat{U}_2, ..., \widehat{U}_K\right) \leq NC. \tag{5.69}$$

Vezessük be ezután a bithibaarány fogalmát:

$$P_b = \frac{1}{K} \sum_{i=1}^{K} P_{e_i}, \tag{5.70}$$

ahol

$$P_{e_i} = \Pr\left(\widehat{U}_i \neq U_i\right). \tag{5.71}$$

A feladatunk most az, hogy kimutassuk, hogy abban az esetben, ha $R \geq C$, a bithibaaránynak van egy

pozitív alsó korlátja, ami azt jelenti, hogy a kapacitásnál nagyobb átviteli sebességnél a bithibaarány nem lehet nulla, azaz ilyen átviteli sebességgel nem lehet hiba nélkül kommunikálni.

Felhasználva, a kölcsönös információ definícióját, miszerint tetszőleges X és Y valószínűségi változók esetén

$$I(X;Y) = H(X) - H(X \mid Y), \tag{5.72}$$

és azt, hogy bináris szimmetrikus memóriamentes forrás esetén $H(U_1,U_2,...,U_K) = K$, felírható az alábbi egyenlőtlenség

$$H\left(U_1,U_2,...,U_K \mid \widehat{U}_1,\widehat{U}_2,...,\widehat{U}_K\right) = H(U_1,U_2,...,U_K) - I\left(U_1,U_2,...,U_K;\widehat{U}_1,\widehat{U}_2,...,\widehat{U}_K\right) =$$

$$= K - I\left(U_1,U_2,...,U_K;\widehat{U}_1,\widehat{U}_2,...,\widehat{U}_K\right) \geq K - NC = N(R-C), \tag{5.73}$$

ugyanakkor a láncszabály alkalmazásával

$$H\left(U_1,U_2,...,U_K \mid \widehat{U}_1,\widehat{U}_2,...,\widehat{U}_K\right) = \sum_{i=1}^{K} H\left(U_i \mid \widehat{U}_1,\widehat{U}_2,...,\widehat{U}_K,U_1,U_2,...,U_{i-1}\right) \leq \sum_{i=1}^{K} H\left(U_i \mid \widehat{U}_i\right). \tag{5.74}$$

A Fano-segédtételből bináris esetben tudjuk, hogy $H\left(U_i \mid \widehat{U}_i\right) \leq h(P_{e_i})$, így az utóbbi két egyenlőtlenség kombinálásával

$$\sum_{i=1}^{K} H\left(U_i \mid \widehat{U}_i\right) \leq \sum_{i=1}^{K} h(P_{e_i}). \tag{5.75}$$

Ezek alapján

$$\frac{1}{K}\sum_{i=1}^{K} h(P_{e_i}) \geq \frac{N}{K}(R-C) = \frac{1}{R}(R-C) = 1 - \frac{C}{R}. \tag{5.76}$$

Kihasználva, hogy bármilyen alulról homorú (konvex) $f(x)$ függvény esetén fennáll a

$$\frac{1}{K}\sum_{i=1}^{K} f(x_i) \leq f\left(\frac{1}{K}\sum_{i=1}^{K} x_i\right), \tag{5.77}$$

ezért

$$\frac{1}{K}\sum_{i=1}^{K} h(P_{e_i}) \leq h\left(\frac{1}{K}\sum_{i=1}^{K} P_{e_i}\right) = h(P_b), \tag{5.78}$$

amiből nyilvánvaló, hogy

$$h(P_b) \geq 1 - \frac{C}{R}. \tag{5.79}$$

Mindezek alapján kimondhatjuk a zajos diszkrét memóriamentes csatorna kódolási tételének a megfordítását.

A zajos diszkrét memóriamentes csatorna kódolási tételének a megfordítása

Ha egy bináris szimmetrikus forrás (BSS) egy C kapacitású visszacsatolásmentes diszkrét memóriamentes csatornán (DMC) át R [bit/igénybevétel] átviteli sebességgel küldi az üzeneteit a vevőhöz, akkor a bithibaarány alsó korlátját a

$$P_b \geq h^{-1}\left(1 - \frac{C}{R}\right) \quad \texttt{ha} \quad R > C \tag{5.80}$$

összefüggés határozza meg, feltéve, hogy $R > C$, mivel a bináris entrópia függvény inverze csak a $[0,1]$ intervallumban értelmezhető.

A tétel illusztrálása céljából az 5.15. ábrán megadtuk a $h(x)$ függvény inverzét, és mivel a P_b bithibaarány nem lehet nagyobb $1/2$-nél, elegendő figyelembe venni a kétértékű inverz függvény alsó

ágát. A tétel tehát annyit állít, hogy, ha $1-C/R>0$, akkor a P_b bithibaarány alsó korlátja pozitív, vagyis a hibaarány nem lehet nulla. Másképpen fogalmazva, egy C kapacitású csatornán $R>C$ átviteli sebességgel nem lehet hibamentesen kommunikálni.

A teljesség érdekében a fenti tételre támaszkodva részletes bizonyítás nélkül mondjuk ki a zajos diszkrét memóriamentes csatorna kódolási tételét.

A zajos diszkrét memóriamentes csatorna kódolási tétele

Ha egy bináris szimmetrikus forrás (BSS) egy C kapacitású visszacsatolásmentes diszkrét memóriamentes csatornán (DMC) át $R=K/N$ [bit/igénybevétel] átviteli sebességgel küldi az üzeneteit a vevőhöz N hosszúságú blokk kódot alkalmazva, akkor tetszőleges $\varepsilon>0$ és $R<C$ esetén a bithibaarány

$$P_B<\varepsilon \tag{5.81}$$

ha N elegendően nagy, ahol

$$P_B=\Pr\left(\widehat{U}_1,\widehat{U}_2,...,\widehat{U}_K\neq U_1,U_2,...,U_K\right) \tag{5.82}$$

a blokkhibavalószínűség, és $P_B/K\leq P_b\leq P_B$.

A tétel tehát kimondja, hogy egy C kapacitású csatornán $R<C$ átviteli sebességgel aszimptotikusan hibamentesen lehet kommunikálni, ha a blokk kód hosszúsága (N) minden határon túl nő.

6. fejezet

A blokk kódolás elve és korlátai

A blokk kódolással működő rendszer általános felépítése a 6.1. ábrán látható.

Az ábrán megadott rendszerben az alábbi feltételek teljesülnek:

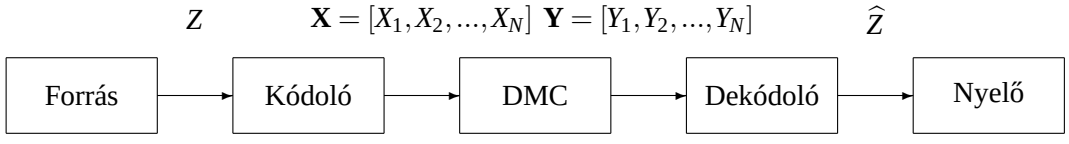
- A forrás diszkrét és memóriamentes (DMS),
- A csatorna diszkrét memóriamentes és visszacsatolás mentes (DMC),
- Z a forrás kimenetén megjelenő véletlen üzenet sorszáma, amelynek az értékkészlete M (ennyi az átviendő üzenetek száma), és a kódoló minden üzenethez egy N hosszúságú blokk kódszót rendel,
- $\mathbf{X} = [X_1, X_2, ..., X_N]$ a csatorna bemenetén (a kódoló kimenetén) megjelenő kódszó, melynek minden betűje egy L méretű ABC-ből veszi fel az értékeit,
- $\mathbf{Y} = [Y_1, Y_2, ..., Y_N]$ a csatorna kimenetén (a dekódoló bemenetén) megjelenő valószínűségi változó sorozat, amelynek minden szimbóluma egy J méretű ABC-ból veszi fel az értékeit,
- $\widehat{Z}$ a dekódoló kimenetén megjelenő jel, a Z üzenet becslése,
- és a korábbiakhoz hasonlóan $R = \log_2 M/N$ [bit/igénybevétel] most is az átviteli sebesség, amit az egy csatornaszimbólumra jutó forrásbitek számával mérünk.

A rendszer tulajdonságainak az elemzése előtt adjuk meg a Z valószínűségi változó pontos definícióját. Z a forrás üzeneteinek a sorszáma, tehát értékeit 1-től M-ig az egész számok halmazán veszi fel, azaz $Z = i$, ha a forrás éppen az i-dik üzenetet állította elő, és ehhez az üzenethez a kódoló éppen az $\mathbf{x}_i$ aktuális blokk kódszót rendeli. A Z valószínűségi változó valószínűségi eloszlása $P_Z(i) = \Pr(Z = i)$ azonos a forrás eloszlásával.

A renszerben a következő két fontos funkciót különböztethetjük meg:

- **Kódoló**, amely a forrás által előállított Z üzenetekhez az $\mathbf{X} = \mathbf{x}_Z$ N hosszúságú kódszavakat rendeli,
- **Dekódoló**, amely a csatorna kimenetén megjelenő N hosszúságú $\mathbf{Y} = [Y_1, Y_2, ..., Y_N]$ valószínűségi változó sorozat megfigyelése után döntést hoz a Z üzenet $\widehat{Z}$ becslésére a

$$\widehat{Z} = F(\mathbf{Y}) \tag{6.1}$$



6.1. ábra. A blokk kóddal működő adatátviteli rendszer általános felépítése

döntési függvény szerint, ami az $\mathbf{Y}$ vektor $\mathbf{B}^N$ értékkészletének N dimenziós terét képezi le az $[1,2,...,M]$ egész számok halmazára.

Példa

A rendszer működésének részletes analízise előtt vizsgáljunk meg egy egyszerű példát. Válasszuk az 5.7. ábrán megadott a bináris törléses csatornát, és legyen az üzenetek száma $M = 4$. Működjön a kódoló az alábbi kódolási táblázat szerint:

Z	$\mathbf{X}$
1	[0 0 0]
2	[0 1 1]
3	[1 0 1]
4	[1 1 0]

(6.2)

A táblázat alapján megállapítható, hogy az alkalmazott kódszavak közötti Hamming-távolság mindig kettő (Hamming-kód).

A következő táblázat pedig megadja a dekódoló döntési szabályát, azaz azt a leképzést, mely szerint az $\mathbf{Y}$ vektor megfigyelésével a dekódoló dönt $\widehat{Z}$-ra, és ezen keresztül az elküldött kódszó becslésére, $\widehat{\mathbf{X}} = \mathbf{x}_{\widehat{Z}}$-re.

$\mathbf{Y}$	$\widehat{Z} = F(\mathbf{Y})$	$\widehat{\mathbf{X}} = \mathbf{x}_{\widehat{Z}}$
[0 0 0]	1	[0 0 0]
[Δ 0 0]	1	[0 0 0]
[0 Δ 0]	1	[0 0 0]
[0 0 Δ]	1	[0 0 0]
[Δ Δ 0]	1	[0 0 0]
[Δ 0 Δ]	1	[0 0 0]
[0 Δ Δ]	1	[0 0 0]
[Δ Δ Δ]	1	[0 0 0]
[0 1 1]	2	[0 1 1]
[Δ 1 1]	2	[0 1 1]
[0 Δ 1]	2	[0 1 1]
[0 1 Δ]	2	[0 1 1]
[Δ Δ 1]	2	[0 1 1]
[Δ 1 Δ]	2	[0 1 1]
[1 0 1]	3	[1 0 1]
[Δ 0 1]	3	[1 0 1]
[1 Δ 1]	3	[1 0 1]
[1 0 Δ]	3	[1 0 1]
[1 Δ Δ]	3	[1 0 1]
[1 1 0]	4	[1 1 0]
[Δ 1 0]	4	[1 1 0]
[1 Δ 0]	4	[1 1 0]
[1 1 Δ]	4	[1 1 0]
[1 1 1]	1	[0 0 0]
[1 0 0]	1	[0 0 0]
[0 1 0]	1	[0 0 0]
[0 0 1]	1	[0 0 0]

(6.3)

Érdemes megjegyezni, hogy a kódoló és a dekódoló függvényét elvileg tetszőlegesen meg lehet választani. Példánkban is önkényesen választottuk ki mind a kódoló, mind pedig a dekódoló leképzési szabályait.

Érdekes kérdés ezután, hogy miként lehet optimális átviteli rendszert tervezni, egyáltalán mekkora az optimális megoldás komplexitása. Ehhez vizsgáljuk meg, hogy adott M, N, L és J értékek esetén hányféleképpen lehet a fenti táblázatokat kitölteni, vagyis hányféle átviteli rendszert lehet definiálni. A kódoló esetén az L^N számú lehetséges kódszót

$$K_1 = \left(L^N\right)^M \tag{6.4}$$

féleképpen lehet az M üzenethez rendelni, megengedve azt is, hogy több üzenethez ugyanazt a kódszót rendeljük. A dekódoló esetében pedig az M üzenetet

$$K_2 = M^{J^N} \tag{6.5}$$

féleképpen lehet az J^N számú $\mathbf{Y}$ vektorhoz rendelni. Ezek alapján a lehetséges különböző rendszerek számát a

$$K = K_1 K_2 = L^{NM} M^{J^N} \tag{6.6}$$

kifejezés adja, amiből nyilvánvaló, hogy az optimalizálási feladat igen összetett, a lehetséges rendszerek száma ugyanis a paraméterek exponenciális függvénye. Éppen ezért kritikus kérdés az optimális kódolási és dekódolási szabályok megfogalmazása, és az optimális eljárások megvalósíthatóságának a vizsgálata.

6.1. Kódolási és dekódolási kritériumok

A digitális információátviteli rendszerek minőségét legáltalánosabban a P_B blokkhibaaránnyal (illetve a P_b a bithibaaránnyal) lehet jellemezni, ahol

$$P_B = \Pr\left(\widehat{Z} \neq Z\right). \tag{6.7}$$

Optimális információátviteli rendszerről akkor beszélhetünk, ha adott csatorna esetén az összes lehetséges kódoló és dekódoló közül kiválasztjuk azt az egyetlen párt, melynél a hibaarány minimális. Sajnos előre leszögezhetjük, hogy univerzálisan érvényes optimális kódolási szabályt nem ismerünk, ezért foglalkozzunk inkább az optimális dekódolás lehetséges megoldásaival.

Lehetséges optimális dekódolási szabályok

- **Maximum a posteriori** (MAP) dekódolási szabályról beszélünk akkor, ha a P_B blokkhibavalószínűség értékét minimalizáljuk ismert P_Z kódszóeloszlás (forrásstatisztika) esetén.
- **Maximum likelihood** (ML) dekódolási szabályról beszélünk akkor, ha a P_B blokkhibavalószínűség értékét minimalizáljuk úgy, hogy a P_Z kódszóeloszlásról (forrásstatisztikáról) nincsen ismeretünk, ezért azt feltételezzük, hogy a kódszavak eloszlása egyenletes.
- **Minimax** dekódolási szabályról beszélünk akkor, ha a P_B blokkhibavalószínűség legrosszabb, maximális értékét minimalizáljuk, azaz teljesítjük, hogy a

$$(P_B)_{WC} = \max_{P_Z} P_B \tag{6.8}$$

  érték legyen minimális.

Érdemes megjegyezni, hogy gyakorlati rendszerekben leginkább a maximum likelihood rendszert használjuk, ahol egy adott "jól megválasztott" kódoló mellett egyenletes eloszlású kódszavakat feltételezve választjuk meg az optimális dekódolás módját az alábbiakban részletesen ismertetett módszer alkalmazásával.

6.2. A blokkhibavalószínűség minimalizálása, az optimális dekódolási szabály megfogalmazása

A korábbi definíciót felhasználva felírhatjuk az

$$1-P_B=\Pr\left(Z=\widehat{Z}\right)=\Pr\left(Z=F\left(\mathbf{Y}\right)\right) \tag{6.9}$$

összefüggést, ahol $F\left(\mathbf{Y}\right)$ a dekódolási függvény. Felhasználva a dekódolási függvény és a feltételes várható érték definícióját az

$$1-P_B=\sum_{\mathbf{y}}\Pr\left(Z=F\left(\mathbf{Y}\right)\mid\mathbf{Y}=\mathbf{y}\right)P_{\mathbf{Y}}\left(\mathbf{y}\right)=\sum_{\mathbf{y}}P_{Z|\mathbf{Y}}\left(F\left(\mathbf{y}\right)\mid\mathbf{y}\right)P_{\mathbf{Y}}\left(\mathbf{y}\right)=\sum_{\mathbf{y}}P_{Z\mathbf{Y}}\left(F\left(\mathbf{y}\right),\mathbf{y}\right), \tag{6.10}$$

ahol az összegzést az összes N hosszúságú $\mathbf{y}=[y_1,y_2,...,y_N]$ kimeneti szimbólomsorozatra végre kell hajtani.

Az együttes eloszlásra vonatkozó ismert

$$P_{Z\mathbf{Y}}\left(F\left(\mathbf{y}\right),\mathbf{y}\right)=P_{Z|\mathbf{Y}}\left(F\left(\mathbf{y}\right)\mid\mathbf{y}\right)P_{\mathbf{Y}}\left(\mathbf{y}\right)=P_{\mathbf{Y}|Z}\left(\mathbf{y}\mid F\left(\mathbf{y}\right)\right)P_Z\left(F\left(\mathbf{y}\right)\right) \tag{6.11}$$

azonosságot alkalmazva a fenti kifejezés az

$$1-P_B=\sum_{\mathbf{y}}P_{\mathbf{Y}|Z}\left(\mathbf{y}\mid F\left(\mathbf{y}\right)\right)P_Z\left(F\left(\mathbf{y}\right)\right)=\sum_{\mathbf{y}}P_{\mathbf{Y}|\mathbf{X}}\left(\mathbf{y}\mid\mathbf{x}_{F(\mathbf{y})}\right)P_Z\left(F\left(\mathbf{y}\right)\right) \tag{6.12}$$

formában írható át. Ennek az egyenletnek az alapján a hibavalószínűség akkor minimalizálható, ha

- **maximum a posteriori** (MAP) dekódolási szabály esetén minden $\mathbf{y}$ vektornál maximális a

  $$P_{\mathbf{Y}|\mathbf{X}}\left(\mathbf{y}\mid\mathbf{x}_i\right)P_Z\left(i\right), \tag{6.13}$$

  szorzat, tehát úgy kell megválasztani az $F\left(\mathbf{Y}\right)$ dekódolási függvényt, hogy ezt a szorzatot maximalizálja,

- Teljesen hasonló módon **maximum likelihood** (ML) dekódolási szabálynál a

  $$P_{\mathbf{Y}|\mathbf{X}}\left(\mathbf{y}\mid\mathbf{x}_i\right) \tag{6.14}$$

  értékét kell minden $\mathbf{y}$ vektor esetében maximálisra választani, vagyis így kell megkonstruálni az $F\left(\mathbf{Y}\right)$ dekódolási függvényt.

A döntési szabályokat a következőképpen lehet értelmezni. A csatorna kimenetén, a vevőben ismerjük a csatorna tulajdonságait, vagyis a zajos csatornát leíró $P_{\mathbf{Y}|\mathbf{X}}\left(\mathbf{y}\mid\mathbf{x}_i\right)$ vektorokra vonatkozó feltételes valószínűségi eloszlásfüggvényt (diszkrét memóriamentes csatornában természetesen elegendő a $P_{Y|X}\left(y\mid x_i\right)$ ismerete), és a lehetséges üzenetek halmazát, azaz az $\mathbf{X}$ valószínűségi változó vektor összes $\mathbf{x}_i,\quad i=1,2,...,M$ értékeit. A döntési szabály azt mondja ki, hogy az aktuálisan vett $\mathbf{y}'$ vektort be kell helyettesíteni az M különböző $P_{\mathbf{Y}|\mathbf{X}}\left(\mathbf{y}\mid\mathbf{x}_i\right)$ függvénybe, és arra az $\widehat{\mathbf{x}}_i$ üzenetre, illetve arra az i értékre kell dönteni, amelynél MAP dekódolási szabály esetén a $P_{\mathbf{Y}|\mathbf{X}}\left(\mathbf{y}'\mid\mathbf{x}\right)P_Z\left(i\right)$, ML dekódolási szabály esetén pedig a $P_{\mathbf{Y}|\mathbf{X}}\left(\mathbf{y}'\mid\mathbf{x}_i\right)$ kifejezés maximális.

6.3. A Bhattacharyya-korlát két kódszó esetén

A fogalmak jobb megértése érdekében először foglalkozzunk azzal az esettel, amikor az üzenetek száma $M=2$, tehát mindössze két N hosszúságú kódszót viszünk át a csatornán. Ekkor a feltételes blokkhibavalószínűséget, feltéve, hogy az i-dik üzenetet küldték a

$$P_{B|i}=\Pr\left(\widehat{Z}\neq Z\mid Z=i\right) \tag{6.15}$$

kifejezéssel számíthatjuk, amiből az átlagos blokkhibavalószínűség

$$P_B = \sum_{i=1}^{M} P_{B|i} P_Z(i) \tag{6.16}$$

értékűre adódik.

A további vizsgálatokhoz célszerű definiálni az $F(\mathbf{Y})$ döntési függvény által meghatározott a dekódolási vagy **döntési tartomány** fogalmát. i-dik döntési tartománynak nevezzük az $\mathbf{Y}$ vektor értékkészletének azon részhalmazát, melyben a döntési függvény felhasználásával éppen az i -dik üzenetre döntünk, azaz

$$\boldsymbol{D}_i = \left\{ \mathbf{y} : \mathbf{y} \in B^N \text{ és } F(\mathbf{y}) = i \right\}. \tag{6.17}$$

A döntési tartomány ismeretében a feltételes blokkhibavalószínűség is egyszerűen meghatározható a

$$P_{B|i} = \sum_{\mathbf{y} \notin \boldsymbol{D}_i} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i) \tag{6.18}$$

kifejezés segítségével, mivel hiba akkor történik, ha az i-dik üzenet küldése esetén nem i-re döntünk, vagyis a vett $\mathbf{y}$ vektor nem a $\boldsymbol{D}_i$ döntési tartományba esik.

Ha csak két üzenetünk van (M =2), akkor csak két döntési tartományunk van, tehát ha $\mathbf{y} \in \boldsymbol{D}_1$, akkor ebből az következik, hogy $\mathbf{y} \notin \boldsymbol{D}_2$, ezért

$$P_{B|2} = \sum_{\mathbf{y} \in \boldsymbol{D}_1} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_2). \tag{6.19}$$

Ugyanakkor maximum likelihood (ML) döntési szabály esetén igaz, hogy ha $\mathbf{y} \in \boldsymbol{D}_1$, akkor

$$P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_1) \geq P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_2), \tag{6.20}$$

amiből következik, hogy megszorozva az a $P_{B|2}$ blokkhibavalószínűség kifejezésének jobboldalát a

$$\sqrt{\frac{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_1)}{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_2)}} \geq 1 \tag{6.21}$$

értékkel, a blokkhibavalószínűségre a

$$P_{B|2} \leq \sum_{\mathbf{y} \in \boldsymbol{D}_1} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_2) \sqrt{\frac{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_1)}{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_2)}} = \sum_{\mathbf{y} \in \boldsymbol{D}_1} \sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_1) P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_2)} \tag{6.22}$$

felső korlátot kapjuk. A fenti eredményhez hasonlóan a másik üzenethez tartozó blokkhibavalószínűségre a

$$P_{B|1} \leq \sum_{\mathbf{y} \in \boldsymbol{D}_2} \sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_1) P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_2)} \tag{6.23}$$

felső korlát adódik, amiből az átlagos hibavalószínűségre a két feltételes blokkhibavalószínűség összege triviális felső korlátot ad:

$$P_B \leq P_{B|1} + P_{B|2} \leq \sum_{\mathbf{y}} \sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_1) P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_2)}. \tag{6.24}$$

Ez a felső korlát anélkül is kiszámítható, hogy ismernénk a döntési tartományokat, ugyanis itt az összegzést az $\mathbf{y}$ teljes értékkészletére el kell végezni, nem csak egy adott döntési tartományra.

Diszkrét memóriamentes csatorna esetén

$$P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}) = \prod_{n=1}^{N} P_{Y|X}(y_n \mid x_n), \tag{6.25}$$

ezért

$$P_B \le P_{B|1} + P_{B|2} \le \sum_{\mathbf{y}} \sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_1) P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_2)} = \sum_{\mathbf{y}} \sqrt{\prod_{n=1}^{N} P_{Y|X}(y_n \mid x_{1n}) P_{Y|X}(y_n \mid x_{2n})} =$$

$$= \sum_{y_1} \sum_{y_2} \ldots \sum_{y_N} \prod_{n=1}^{N} \sqrt{P_{Y|X}(y_n \mid x_{1n}) P_{Y|X}(y_n \mid x_{2n})} = \prod_{n=1}^{N} \sum_{y} \sqrt{P_{Y|X}(y \mid x_{1n}) P_{Y|X}(y \mid x_{2n})}. \qquad (6.26)$$

Bhattacharyya-korlát

Ha diszkrét memóriamentes csatornán bináris információt viszünk át két $\mathbf{x}_1$ és $\mathbf{x}_2$ N hosszúságú kódszóval, akkor a blokkhibavalószínűség felső korlátja a

$$P_{B|i} \le \prod_{n=1}^{N} \sum_{y} \sqrt{P_{Y|X}(y \mid x_{1n}) P_{Y|X}(y \mid x_{2n})}; \;\; i = 1,2, \qquad (6.27)$$

vagy legrosszabb esetben a

$$(P_B)_{wc} \le \prod_{n=1}^{N} \sum_{y} \sqrt{P_{Y|X}(y \mid x_{1n}) P_{Y|X}(y \mid x_{2n})} \qquad (6.28)$$

kifejezéssel határozható meg.

Speciális esetben, ha ismétléses kódot alkalmazunk, azaz

$$\mathbf{x}_1 = [0,0,\ldots,0] \quad \text{és} \quad \mathbf{x}_2 = [1,1,\ldots,1], \qquad (6.29)$$

akkor

$$P_{B|i} \le \left(\sum_{y} \sqrt{P_{Y|X}(y \mid 0) P_{Y|X}(y \mid 1)} \right)^{N} \;\; ; \;\; i = 1,2. \qquad (6.30)$$

Definiáljuk ezután az úgynevezett Bhattacharyya-távolság fogalmát.

Definíció

A csatorna bemenetén lévő két kódszó n-dik szimbóluma közötti Bhattacharyya-távolságnak nevezzük a

$$D_{B_n} = -\log_2 \sum_{y} \sqrt{P_{Y|X}(y \mid x_{1n}) P_{Y|X}(y \mid x_{2n})} \qquad (6.31)$$

értéket, ami $x_{1n} = 0$ és $x_{2n} = 1$ esetén

$$D_B = -\log_2 \sum_{y} \sqrt{P_{Y|X}(y \mid 0) P_{Y|X}(y \mid 1)}, \qquad (6.32)$$

ezért ismétléses kódnál, bináris kód-ABC-t feltételezve

$$P_{B|i} \le 2^{-ND_B}, \qquad (6.33)$$

illetve

$$(P_B)_{wc} \le 2^{-ND_B}. \qquad (6.34)$$

A Bhattacharyya-távolság tehát olyan speciális távolság, amely a csatorna bemenetén lévő két szimbólum közötti távolságot úgy határozza meg, hogy egyúttal figyelembe veszi azt is, hogy ez a két szimbólum hogyan jut át a csatornán. Ez azt jelenti, hogy a Bhattacharyya-távolság egyszerre ad felvilágosítást a két bemeneti szimbólum közötti különbségről és a csatorna viselkedéséről is. A Bhattacharyya-távolság az alábbi speciális tulajdonságokkal rendelkezik:

- A távolság nulla, ha a két bemeneti szimbólum azonos, mivel

$$D_{B_n} = -\log_2 \sum_y \sqrt{P_{Y|X}(y \mid x_{1n} = x') P_{Y|X}(y \mid x_{2n} = x')} =$$

$$= -\log_2 \sum_y P_{Y|X}\left(y \mid x'\right) = -\log_2 1 = 0. \tag{6.35}$$

- A távolság nem negatív, mivel a

$$\sum_i a_i b_i \leq \sqrt{\sum_i a_i^2} \sqrt{\sum_i b_i^2} \tag{6.36}$$

Cauchy-egyenlőtlenség szerint (egyenlőség akkor és csak akkor áll fent, ha $a_i = b_i$)

$$0 \leq \sum_y \sqrt{P_{Y|X}(y \mid x_{1n}) P_{Y|X}(y \mid x_{2n})} \leq \sqrt{\sum_y P_{Y|X}(y \mid x_{1n})} \sqrt{\sum_y P_{Y|X}(y \mid x_{2n})} = 1, \tag{6.37}$$

ezért

$$D_{B_n} \geq 0. \tag{6.38}$$

- A távolság akkor is nulla, ha a két bemeneti szimbólum különbözik egymástól, de a csatorna Y kimenete független a csatorna X bemenetétől, mivel a Cauchy-egyenlőtlenség

$$\sum_y \sqrt{P_{Y|X}(y \mid x_{1n}) P_{Y|X}(y \mid x_{2n})} \leq \sqrt{\sum_y P_{Y|X}(y \mid x_{1n})} \sqrt{\sum_y P_{Y|X}(y \mid x_{2n})} \tag{6.39}$$

összefüggésénél, bármely $x_{1n} \neq x_{2n}$ esetén, egyenlőség akkor és csak akkor áll fent, ha

$$P_{Y|X}(y \mid x_{1n}) = P_{Y|X}(y \mid x_{2n}) \tag{6.40}$$

minden y-ra.

Tudjuk viszont, hogy Y és X függetlensége esetén

$$P_{Y|X}(y \mid x) = P_Y(y), \tag{6.41}$$

minden x-re és y-ra, így elmondhatjuk, hogy ilyen csatornában bármely két bemeneti x_{1n} és x_{2n} szimbólum Bhattacharyya-távolsága nulla értékű. Érdemes megjegyezni, hogy annak a csatornának a kapacitása nulla értékű, melyben az Y valószínűségi változó független az X valószínűségi változótól, mivel

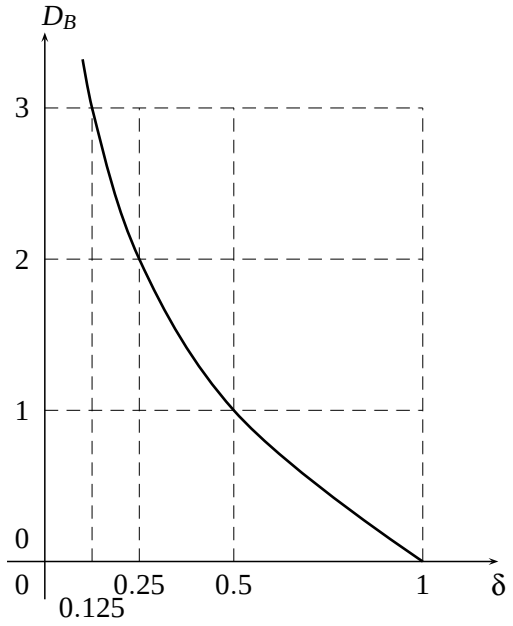
$$C = \max_{P_X} I(X;Y) = \max_{P_X} [H(Y) - H(Y \mid X)] = \max_{P_X} [H(Y) - H(Y)] = 0. \tag{6.42}$$

Ezért bináris bemenetű diszkrét memóriamentes csatornában a D_B Bhattacharyya-távolság akkor és csak akkor pozitív, ha a csatorna kapacitása is pozitív.

- Hibamentes csatorna esetén, ha $x_{1n} \neq x_{2n}$, a Bhattacharyya-távolság végtelen, mivel ilyenkor a $P_{Y|X}(y \mid x_{in}) \;\; i = 1,2$ mennyiségek közül legalább egy mindig 0 értékű.

Példa

Számítsuk ki az általunk korábban bevezetett két bináris mintacsatornában a D_B Bhattacharyya-távolság értékét.



6.2. ábra. A bináris törléses csatorna Bhattacharyya-távolsága a δ függvényében

- Bináris törléses csatornában (BEC)

$$\sum_y \sqrt{P_{Y|X}(y \mid 0) P_{Y|X}(y \mid 1)} = \sqrt{P_{Y|X}(0 \mid 0) P_{Y|X}(0 \mid 1)} +$$

$$+ \sqrt{P_{Y|X}(\Delta \mid 0) P_{Y|X}(\Delta \mid 1)} + \sqrt{P_{Y|X}(1 \mid 0) P_{Y|X}(1 \mid 1)} =$$

$$= \sqrt{(1-\delta)\times 0} + \sqrt{\delta^2} + \sqrt{0 \times (1-\delta)} = \delta, \tag{6.43}$$

ezért

$$D_B = -\log_2 \delta, \tag{6.44}$$

és

$$(P_B)_{wc} \leq 2^{N \log_2 \delta} = \delta^N. \tag{6.45}$$

Az eredmény a 6.2. ábrán látható.

- Bináris szimmetrikus csatornában (BSC)

$$\sum_y \sqrt{P_{Y|X}(y \mid 0) P_{Y|X}(y \mid 1)} = \sqrt{P_{Y|X}(0 \mid 0) P_{Y|X}(0 \mid 1)} + \sqrt{P_{Y|X}(1 \mid 0) P_{Y|X}(1 \mid 1)} =$$

$$= \sqrt{(1-\varepsilon)\varepsilon} + \sqrt{\varepsilon(1-\varepsilon)} = 2\sqrt{\varepsilon(1-\varepsilon)} \tag{6.46}$$

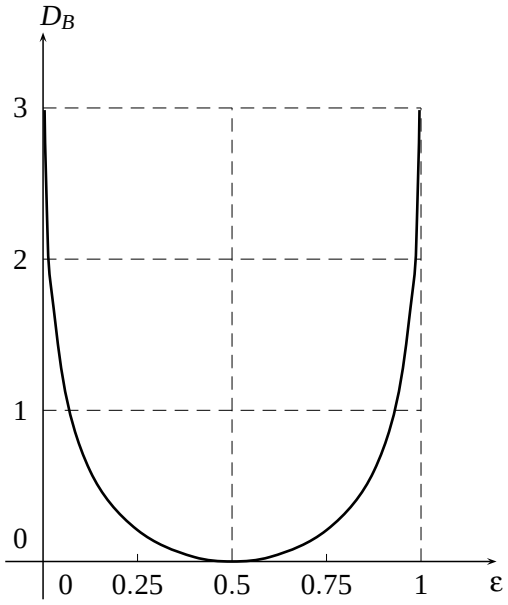
ezért

$$D_B = -\log_2 \left[2\sqrt{\varepsilon(1-\varepsilon)} \right], \tag{6.47}$$

és

$$(P_B)_{wc} \leq 2^{N \log_2 \left[2\sqrt{\varepsilon(1-\varepsilon)} \right]} = 2^N \left[\varepsilon(1-\varepsilon) \right]^{\frac{N}{2}}. \tag{6.48}$$

Az eredményeket a 6.3. ábrán adtuk meg, és az alábbi táblázatban kis ε-ok esetében összehasonlítottuk a hibaarány pontos értékét a Bhattacharyya-távolságból származtatott felső korláttal különböző N blokkhosszoknál.



6.3. ábra. A bináris szimmetrikus csatorna Bhattacharyya-távolsága az ε függvényében

N	Felső korlát	Pontos közelítés
1	$\approx 2\varepsilon^{\frac{1}{2}}$	$\approx \varepsilon$
2	$\approx 4\varepsilon$	$\approx 2\varepsilon$
3	$\approx 8\varepsilon^{\frac{3}{2}}$	$\approx 3\varepsilon^2$
4	$\approx 16\varepsilon^2$	$\approx 6\varepsilon^2$
5	$\approx 32\varepsilon^{\frac{5}{2}}$	$\approx 10\varepsilon^3$

(6.49)

6.4. A Bhattacharyya-korlát kettőnél több kódszó esetén

Kettőnél több kódszó esetén, ha a kódszavak (üzenetek) száma M, és a kódszavak rendre az $\mathbf{x}_2, \mathbf{x}_1, \ldots, \mathbf{x}_M$ vektorok, akkor a feltételes blokkhibavalószínűség a

$$P_{B|i} = \sum_{\mathbf{y} \notin \boldsymbol{D}_i} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i) = \sum_{\substack{j=1 \\ j \neq i}}^{M} \sum_{\mathbf{y} \in \boldsymbol{D}_j} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i) \tag{6.50}$$

összefüggéssel határozható meg.

A maximum likelihood (ML) döntési szabálynál ha az $\mathbf{y}$ vektor benne van a $\boldsymbol{D}_j$ döntési tartományban, akkor

$$P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j) \geq P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_k); \quad k \neq j, \tag{6.51}$$

ezért igaz, hogy ilyenkor

$$P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j) \geq P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i). \tag{6.52}$$

A célunk az, hogy adjunk egy felső korlátot a blokkhibavalószínűségre ebben az esetben is. A felső korlát meghatározását visszavezetjük a bináris esetre, amikor csak két kódszó állt a rendelkezésünkre. Válasszuk ki ehhez a művelethez az i-dik és j-dik kódszót, és tekintsük úgy a rendszert, mintha csak ez a két kódszavunk lenne. A továbblépés előtt definiáljunk egy új $\boldsymbol{D}'_j$ döntési tartományt, ami azzal

jellemezhető, hogy ebben a tartományban a j-dik kódszóhoz tartozó feltételes valószínűségi eloszlásfüggvény nagyobb az i-dik kódszóhoz tartozónál, de nem feltétlenül nagyobb a többi kódszóhoz tartozó feltételes valószínűségi eloszlásfüggvénynél, hiszen most ezeket nem is vesszük figyelembe. A $\boldsymbol{D}'_j$ döntési tartomány a

$$\boldsymbol{D}'_j = \left\{ \mathbf{y} : \mathbf{y} \in B^N \ \text{és} \ P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j) \geq P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i) \right\} \tag{6.53}$$

kifejezéssel definiálható, és ebből a definícióból nyilvánvaló, hogy

$$\boldsymbol{D}'_j \supseteq \boldsymbol{D}_j, \tag{6.54}$$

vagyis a $\boldsymbol{D}'_j$ tartomány magában foglalja az eredeti $\boldsymbol{D}_j$ tartományt.

Ennek a ténynek az a következménye, hogy

$$\sum_{\mathbf{y} \in \boldsymbol{D}_j} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i) \leq \sum_{\mathbf{y} \in \boldsymbol{D}'_j} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i), \tag{6.55}$$

és felhasználva a bináris esetre érvényes Bhattacharyya-korlátot

$$\sum_{\mathbf{y} \in \boldsymbol{D}_j} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i) \leq \sum_{\mathbf{y} \in \boldsymbol{D}'_j} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i) \leq \sum_{\mathbf{y}} \sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i) P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)}. \tag{6.56}$$

Ha ezt az utóbbi összefüggést behelyettesítjük a feltételes blokkhibavalószínűség kifejezésébe, akkor az úgynevezett úniós Bhattacharyya-korláthoz jutunk:

$$P_{B|i} \leq \sum_{\substack{j=1 \\ j \neq i}}^{M} \sum_{\mathbf{y}} \sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i) P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)}, \tag{6.57}$$

amit diszkrét memóriamentes csatornáknál a

$$P_{B|i} \leq \sum_{\substack{j=1 \\ j \neq i}}^{M} \prod_{n=1}^{N} \sum_{y} \sqrt{P_{Y|X}(y \mid x_{in}) P_{Y|X}(y \mid x_{jn})} \tag{6.58}$$

alakban adhatunk meg. Fontos megjegyezni, hogy ez a felső korlát a kódszavak számának növekedésével egyre kevésbé szoros, sőt a j szerinti összegzés miatt a felső korlát értéke nagyobb lehet, mint egy. Ezt a problémát oldja fel a következő fejezetben tárgyalt Gallager-korlát.

6.5. A Bhattacharyya-korlát általánosítása, a Gallager-korlát

Mint ahogy azt a korábbi fejezetekben már megmutattuk, a feltételes blokkhibavalószínűség értékét általában a

$$P_{B|i} = \sum_{\mathbf{y} \notin \boldsymbol{D}_i} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i) \tag{6.59}$$

egyenlőség alapján határozhatjuk meg. Azt is igaz, hogy, ha $\mathbf{y} \notin \boldsymbol{D}_i$, akkor van legalább egy olyan $j \neq i$ érték, ahol

$$P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j) \geq P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i). \tag{6.60}$$

Ennek alapján igen könnyen belátható, hogy $\mathbf{y} \notin \boldsymbol{D}_i$ esetén biztos, hogy

$$\left\{ \sum_{\substack{j=1 \\ j \neq i}}^{M} \left(\frac{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)}{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i)} \right)^s \right\}^{\rho} \geq 1 \quad \text{ha} \quad s \geq 0, \, \rho \geq 0, \tag{6.61}$$

mivel az adott döntési tartományban az összegben szerepel legalább egy

$$\frac{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)}{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i)} \tag{6.62}$$

hányados, ami nagyobb vagy egyenlő eggyel.

Átrendezés után a kifejezés $\mathbf{y} \notin \boldsymbol{D}_i$ esetén az

$$\left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i)\right)^{-\rho s} \left\{ \sum_{\substack{j=1 \\ j \neq i}}^{M} \left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)\right)^{s} \right\}^{\rho} \geq 1 \quad \texttt{ha} \quad s \geq 0,\ \rho \geq 0 \tag{6.63}$$

alakra hozható, amit behelyettesítve a feltételes blokkhibavalószínűség összefüggésbe a

$$P_{B|i} \leq \sum_{\mathbf{y} \notin \boldsymbol{D}_i} \left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i)\right)^{1-\rho s} \left\{ \sum_{\substack{j=1 \\ j \neq i}}^{M} \left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)\right)^{s} \right\}^{\rho} \tag{6.64}$$

felső korláthoz jutunk, ahol ρ és s tetszőleges nem negatív számok. A ρ és s megválasztásakor teljesítsünk egy speciális "szimmetria" feltételt, azaz legyen

$$s = \frac{1}{1+\rho} \ , \tag{6.65}$$

amiből

$$1 - \rho s = \frac{1}{1+\rho} \ , \quad \rho \geq 0 \tag{6.66}$$

és ezzel a választással írjuk végleges alakba a feltételes blokkhibavalószínűség felső korlátját.

Gallager-korlát

Ha M számú üzenetet viszünk át egy csatornán az N hosszúságú blokk kód $\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_M$ kódszavaival, és maximum likelihood (ML) dekódolási algoritmust használunk, akkor Gallager szerint a feltételes blokkhibavalószínűség felső korlátja a

$$P_{B|i} \leq \sum_{\mathbf{y}} \left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i)\right)^{\frac{1}{1+\rho}} \left\{ \sum_{\substack{j=1 \\ j \neq i}}^{M} \left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)\right)^{\frac{1}{1+\rho}} \right\}^{\rho} ; \quad \rho \geq 0 \tag{6.67}$$

kifejezéssel határozható meg, ami diszkrét memóriamentes csatorna esetében a

$$P_{B|i} \leq \prod_{n=1}^{N} \sum_{y} \left(P_{Y|X}(y \mid x_{in})\right)^{\frac{1}{1+\rho}} \left\{ \sum_{\substack{j=1 \\ j \neq i}}^{M} \left(P_{Y|X}(y \mid x_{jn})\right)^{\frac{1}{1+\rho}} \right\}^{\rho} ; \quad \rho \geq 0 \tag{6.68}$$

formában adható meg.

A Gallager-korlát a Bhattacharyya-korlát általánosítása és annál szorosabb felső becslést ad, ugyanis:

- $\rho = 1$ esetén visszakapjuk a korábban ismertetett

$$P_{B|i} \leq \sum_{\substack{j=1 \\ j \neq i}}^{M} \sum_{\mathbf{y}} \sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i)\, P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)} \tag{6.69}$$

Bhattacharyya-korlátot.

- A felső korlát ρ szerinti minimumát megkeresve pedig biztosan nem kapunk rosszabb felső becslést ennél.

- Érdemes megjegyezni, hogy az egyszerű úniós korlátnál ez a korlát azért jobb, mert a kódszavak számának, M-nek a növekedését ρ csökkenése képes kompenzálni, ugyanis felső korlát kifejezésében a j szerinti összeg ρ-dik hatványa szerepel, így a felső korlát M-mel nem nő arányosan.

6.6. Véletlen kódolás

Shannon már a korábban idézett 1948-as cikkében bevezette a véletlen kódolás módszerét, amellyel a csatornák általános tulajdonságait lehet jellemezni. Miért is célszerű ennek a módszernek az alkalmazása? A válasz a következő. Tudjuk, hogy az optimális adatátviteli rendszer megvalósításához egyszerre kell optimálisra választani a kódolót és a dekódolót is. A dekódoló optimális kialakítására ismerünk konstruktív módszereket (MAP, ML), sajnos a kódolóra nincsen optimalizálási eljárás. Ennek az a következménye, hogy egy konkrét csatorna átviteli tulajdonságairól optimális körülmények között nem tudunk határozott állításokat tenni, illetve csak kimerítő kereséssel lehetne a feladatot megoldani, ami nem polinomiális bonyolultságú probléma. A feladat megoldására Shannon a véletlen kódolás módszerét vezette be. Ez annyit jelent, hogy a csatornát az alábbi feltételekkel vizsgáljuk:

- A forrás üzeneteihez véleletlenül választunk N hosszúságú kódszavakat a lehetséges kódszavak halmazából egy adott választási (sorsolási) statisztika szerint, vagyis a kódolási szabályt véletlen választással helyettesítjük.

- A dekódolót a csatornához optimálisan illesztjük valamelyik optimális dekódolási eljárást alkalmazva.

- Minden véletlenül választott kód esetén becsüljük a rendszer blokkhibavalószínűségét, és meghatározzuk a hibaarány átlagát az összes lehetséges kódválasztás figyelembevételével.

Az eljárás előnye az, hogy így az optimális kódoló megválasztása nélkül is állításokat tehetünk a rendszer teljesítőképességével kapcsolatban, igaz, hogy csak az összes lehetséges kódoló átlagos tulajdonságaira vonatkozóan.

A véletlen kódolás többféle módszerrel is elvégezhető:

- Az összes N hosszúságú kódszó közül M különbözőt választunk, azaz azonos kódszavakat biztosan nem rendelünk különböző üzenetekhez. Ha a kódszavak ABC-je L méretű, akkor ezt a választást $\binom{L^N}{M}$ különböző módon lehet elvégezni adott

$$Q_{\mathbf{X}_1,\mathbf{X}_2,\ldots,\mathbf{X}_M}(\mathbf{x}_1,\mathbf{x}_2,\ldots,\mathbf{x}_M) \tag{6.70}$$

  "kiválasztási" valószínűségi eloszlással.

- Az összes N hosszúságú kódszó közül M-szer függetlenül azonos eloszlás szerint választunk kódszavakat, vagyis megengedjük azt az esetet is, hogy ugyanazt a kódszót rendeljük több üzenethez is. Ha a kódszavak ABC-je L méretű, akkor ezt a választást L^{NM} különböző módon lehet elvégezni a

$$Q_{\mathbf{X}_1,\mathbf{X}_2,\ldots,\mathbf{X}_M}(\mathbf{x}_1,\mathbf{x}_2,\ldots,\mathbf{x}_M) = \prod_{j=1}^{M} Q_{\mathbf{X}}(\mathbf{x}_j) \tag{6.71}$$

  "kiválasztási" valószínűségi eloszlással, ahol $Q_{\mathbf{X}}(\mathbf{x})$ az egy kódszó kiválasztásának a valószínűségi eloszlása.

- Az egyes kódszavak minden betűjét függetlenül azonos eloszlás szerint választjuk ki az L méretű ABC-ből, így a kódszavak "kiválasztási" valószínűségi eloszlását a

$$Q_{\mathbf{X}_1,\mathbf{X}_2,...,\mathbf{X}_M}(\mathbf{x}_1,\mathbf{x}_2,...,\mathbf{x}_M)=\prod_{j=1}^{M}Q_{\mathbf{X}}(\mathbf{x}_j)=\prod_{j=1}^{M}\prod_{n=1}^{N}Q_X(x_{jn}) \tag{6.72}$$

alakban adhatjuk meg, ahol $\mathbf{x}_j=\{x_{j1},x_{j2},...,x_{jN}\}$ a j-dik kódszó, és $Q_X(x)$ az egy betű "választásának" a valószínűségi eloszlása. Értelemszerűen itt is előfordulhat az, hogy kölönböző üzenetekhez azonos kódszavakat rendelünk.

6.7. Véletlen kódolás két kódszó esetén, a csatornák határsebessége (cut-off rate)

Vizsgáljuk meg ezután a bináris üzenetátvitel esetét, amikor két kódszavunk van, $\mathbf{x}_1$ és $\mathbf{x}_2$ ($M=2$). Tételezzük fel, hogy a két N hosszúságú kódszót egymástól függetlenül azonos

$$Q_{\mathbf{X}}(\mathbf{x}) \tag{6.73}$$

"kiválasztási" valószínűségi eloszlás szerint sorsoljuk. Ezért a két kódszó kiválasztásának az együttes eloszlása

$$Q_{\mathbf{X}_1,\mathbf{X}_2}(\mathbf{x}_1,\mathbf{x}_2)=Q_{\mathbf{X}}(\mathbf{x}_1)Q_{\mathbf{X}}(\mathbf{x}_2). \tag{6.74}$$

Ha minden kisorsolt kódszópár esetén ismerjük $P_{B_{wc}}(\mathbf{x}_1,\mathbf{x}_2)$-t, a blokkhibavalószínűség értékét a legrosszabb esetben, akkor ennek az átlagát a

$$\mathbf{E}\left[P_{B_{wc}}(\mathbf{x}_1,\mathbf{x}_2)\right]=\sum_{\mathbf{x}_1}\sum_{\mathbf{x}_2}P_{B_{wc}}(\mathbf{x}_1,\mathbf{x}_2)Q_{\mathbf{X}}(\mathbf{x}_1)Q_{\mathbf{X}}(\mathbf{x}_2) \tag{6.75}$$

összefüggéssel adhatjuk meg.

A Bhattacharyya-korlát alkalmazásával bináris esetben a $P_{B_{wc}}(\mathbf{x}_1,\mathbf{x}_2)$ felső korlátja

$$P_{B_{wc}}(\mathbf{x}_1,\mathbf{x}_2)\le\sum_{\mathbf{y}}\sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}\mid\mathbf{x}_1)P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}\mid\mathbf{x}_2)}, \tag{6.76}$$

ezért a várható érték felső korlátja

$$\mathbf{E}\left[P_{B_{wc}}(\mathbf{x}_1,\mathbf{x}_2)\right]\le\sum_{\mathbf{x}_1}\sum_{\mathbf{x}_2}\sum_{\mathbf{y}}\sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}\mid\mathbf{x}_1)P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}\mid\mathbf{x}_2)}Q_{\mathbf{X}}(\mathbf{x}_1)Q_{\mathbf{X}}(\mathbf{x}_2)=$$

$$=\sum_{\mathbf{y}}\sum_{\mathbf{x}_1}\sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}\mid\mathbf{x}_1)}Q_{\mathbf{X}}(\mathbf{x}_1)\sum_{\mathbf{x}_2}\sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}\mid\mathbf{x}_2)}Q_{\mathbf{X}}(\mathbf{x}_2)=\sum_{\mathbf{y}}\left[\sum_{\mathbf{x}}\sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}\mid\mathbf{x})}Q_{\mathbf{X}}(\mathbf{x})\right]^2. \tag{6.77}$$

Diszkrét memóriamentes csatornában, ha a kódszavak betűit függetlenül sorsoljuk, azaz

$$Q_{\mathbf{X}}(x_1,x_2,...,x_N)=\prod_{n=1}^{N}Q_X(x_n), \tag{6.78}$$

és

$$\sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}\mid\mathbf{x})}Q_{\mathbf{X}}(\mathbf{x})=\prod_{n=1}^{N}\sqrt{P_{Y|X}(y_n\mid x_n)}Q_X(x_n), \tag{6.79}$$

vagyis

$$\sum_{\mathbf{x}}\sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}\mid\mathbf{x})}Q_{\mathbf{X}}(\mathbf{x})=\sum_{x_1}\sum_{x_2}...\sum_{x_N}\prod_{n=1}^{N}\sqrt{P_{Y|X}(y_n\mid x_n)}Q_X(x_n)=\prod_{n=1}^{N}\sum_{x_n}\sqrt{P_{Y|X}(y_n\mid x_n)}Q_X(x_n), \tag{6.80}$$

akkor a $P_{B_{wc}}(\mathbf{x}_1,\mathbf{x}_2)$ várható értékének a felső korlátja:

$$\mathbf{E}\left[P_{B_{wc}}(\mathbf{x}_1,\mathbf{x}_2)\right] \leq \sum_{y_1}\sum_{y_2}\ldots\sum_{y_N}\left[\prod_{n=1}^{N}\sum_{x_n}\sqrt{P_{Y|X}(y_n\mid x_n)}Q_X(x_n)\right]^2 =$$

$$=\prod_{n=1}^{N}\sum_{y_n}\left[\sum_{x_n}\sqrt{P_{Y|X}(y_n\mid x_n)}Q_X(x_n)\right]^2 = \left[\sum_{y}\left[\sum_{x}\sqrt{P_{Y|X}(y\mid x)}Q_X(x)\right]^2\right]^N. \tag{6.81}$$

A blokkhibavalószínűség felső korlátja két kódszó esetén

Ha diszkrét memóriamentes csatornában bináris üzeneteket viszünk át, és az N hosszúságú kódszavak betűit a $Q_X(x)$ valószínűségi eloszlás szerint függetlenül választjuk ki, akkor a legrosszabb esetben a blokkhibavalószínűség várható értékének a felső korlátja a

$$\mathbf{E}\left[P_{B_{wc}}\right] \leq 2^{-N\left(-\log_2\sum_y\left[\sum_x\sqrt{P_{Y|X}(y|x)}Q_X(x)\right]^2\right)}, \tag{6.82}$$

vagy a

$$\mathbf{E}\left[P_{B_{wc}}\right] \leq 2^{-NR_0} \tag{6.83}$$

kifejezéssel határozható meg, ahol

$$R_0 = \max_Q\left(-\log_2\sum_y\left[\sum_x\sqrt{P_{Y|X}(y\mid x)}Q_X(x)\right]^2\right) = -\log_2\left(\min_Q\sum_y\left[\sum_x\sqrt{P_{Y|X}(y\mid x)}Q_X(x)\right]^2\right) \tag{6.84}$$

a csatorna határsebessége, az úgynevezett cut-off rate. Erősen szimmetrikus csatornák esetén az optimális érték az egyenletes $Q_X(x)$ eloszláshoz tartozik.

Példák

- Szimmetrikus bináris memóriamentes csatornában általában igaz, hogy

$$R_0 = -\log_2\sum_y\left[\frac{1}{2}\sqrt{P(y\mid 0)}+\frac{1}{2}\sqrt{P(y\mid 1)}\right]^2 =$$

$$=-\log_2\frac{1}{4}\sum_y\left[P(y\mid 0)+2\sqrt{P(y\mid 0)}\sqrt{P(y\mid 1)}+P(y\mid 1)\right] =$$

$$=1-\log_2\left[1+\sum_y\sqrt{P(y\mid 0)P(y\mid 1)}\right], \tag{6.85}$$

ezért

$$R_0 = 1-\log_2\left[1+2^{-D_B}\right] \tag{6.86}$$

ahol D_B a Bhattacharyya-távolság.

Bináris törléses csatornában (BEC):

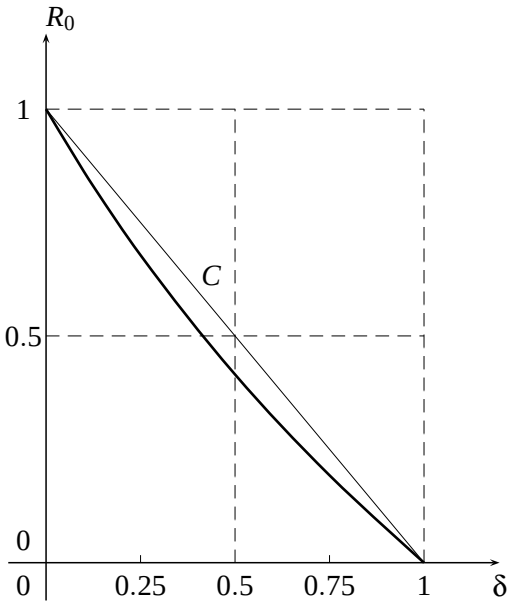
$$R_0 = 1-\log_2\left[1+\delta\right], \tag{6.87}$$

lásd a 6.4. ábrát.

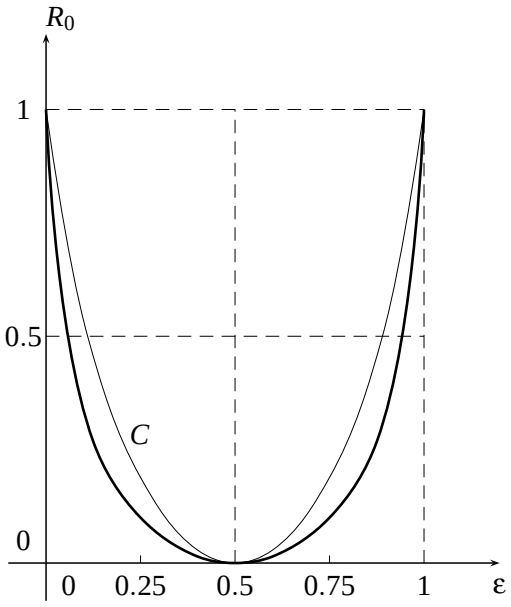
Bináris szimmetrikus csatornában (BSC):

$$R_0 = 1-\log_2\left[1+2\sqrt{\varepsilon(1-\varepsilon)}\right], \tag{6.88}$$

lásd a 6.5. ábrát.



6.4. ábra. A bináris törléses csatorna határsebessége a δ függvényében



6.5. ábra. A bináris szimmetrikus csatorna határsebessége az ε függvényében

Tetszőleges szimmetrikus csatornában:

$$R_0 = \log_2 L - \log_2 \left[1 + \frac{1}{L} \sum_x \sum_{\substack{x' \\ x' \neq x}} \sum_y \sqrt{P(y \mid x) P(y \mid x')} \right]. \tag{6.89}$$

- Bináris szimmetrikus csatorna esetén, mint láttuk

$$R_0 = 1 - \log_2 \left[1 + 2\sqrt{\varepsilon(1-\varepsilon)} \right], \tag{6.90}$$

amiből $\varepsilon = 0$ esetén, tehát a hibamentes csatornában $R_0 = 1$ adódik, így a legrosszabb esetben az átlagos blokkhibavalószínűség felső korlátjára a

$$\mathbf{E}\left[P_{B_{wc}}\right] \leq 2^{-N} \tag{6.91}$$

értéket kapjuk. Ez az eredmény első látásra meglepő, mivel a felső korláttól elvárható, hogy ideális csatorna esetén pontos értéket adjon. Nyilvánvaló ugyanis, hogy $\mathbf{x}_1 \neq \mathbf{x}_2$ esetén $P_B = 0$.

A véletlen kódolás viszont megengedi azt is, hogy a bináris átvitel két kódszava egyforma legyen, és tudjuk, hogy a betűnkénti véletlen kódszóválasztásnál ennek az eseménynek a valószínűsége

$$\Pr(\mathbf{x}_1 = \mathbf{x}_2) = 2^{-N}, \tag{6.92}$$

ezért az átlagos hibavalószínűség:

$$\mathbf{E}\left[P_{B_{wc}}\right] = 0 \times \Pr(\mathbf{x}_1 \neq \mathbf{x}_2) + 1 \times \Pr(\mathbf{x}_1 = \mathbf{x}_2) = 2^{-N}, \tag{6.93}$$

tehát a felső korlát pontos.

Megjegyzendő, hogy $\varepsilon = 0.5$ esetén, ha a csatorna kapacitása $C = 0$, a felső korlát

$$\mathbf{E}\left[P_{B_{wc}}\right] \leq 1. \tag{6.94}$$

6.8. Véletlen kódolás több kódszó esetén, a határsebesség értelmezése

Ha létezik egy blokk kód az $\{\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_M\}$ N hosszúságú kódszavakkal, és $M = 2^{NR}$, ahol R az átviteli sebesség, akkor érvényes a

$$P_{B|i} \leq \sum_{\substack{j=1 \\ j \neq i}}^{M} \sum_{\mathbf{y}} \sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i) P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)} \tag{6.95}$$

uniós Bhattacharyya-korlát, ezért véletlen kódválasztáskor

$$\mathbf{E}\left[P_{B|i}\right] \leq \sum_{\substack{j=1 \\ j \neq i}}^{M} \mathbf{E}\left[\sum_{\mathbf{y}} \sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i) P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)} \right]. \tag{6.96}$$

Ha a kódszavakat egymástól függetlenül azonos $Q_{\mathbf{X}}(\mathbf{x})$ sorsolási valószínűséggel választjuk meg, akkor

$$Q_{\mathbf{X}_i, \mathbf{X}_j}(\mathbf{x}_i, \mathbf{x}_j) = Q_{\mathbf{X}}(\mathbf{x}_i) Q_{\mathbf{X}}(\mathbf{x}_j) \tag{6.97}$$

minden $i \neq j$-re, ezért

$$\mathbf{E}\left[P_{B|i}\right] \leq \sum_{\substack{j=1 \\ j \neq i}}^{M} \sum_{\mathbf{x}_i} \sum_{\mathbf{x}_j} \sum_{\mathbf{y}} \sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i) P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)} Q_{\mathbf{X}}(\mathbf{x}_i) Q_{\mathbf{X}}(\mathbf{x}_j) =$$

$$= \sum_{\substack{j=1 \\ j\neq i}}^{M} \sum_{\mathbf{y}} \sum_{\mathbf{x}_i} \sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i)} Q_{\mathbf{X}}(\mathbf{x}_i) \sum_{\mathbf{x}_j} \sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)} Q_{\mathbf{X}}(\mathbf{x}_j) = \sum_{\substack{j=1 \\ j\neq i}}^{M} \sum_{\mathbf{y}} \left[\sum_{\mathbf{x}} \sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x})} Q_{\mathbf{X}}(\mathbf{x}) \right]^2 =$$

$$= (M-1) \sum_{\mathbf{y}} \left[\sum_{\mathbf{x}} \sqrt{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x})} Q_{\mathbf{X}}(\mathbf{x}) \right]^2, \tag{6.98}$$

minden $i = 1, 2, ..., M$ értékre.

A korábbi eredmények alapján diszkrét memóriamentes csatornában, ahol

$$P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}) = \prod_{n=1}^{N} P_{Y|X}(y_n \mid x_n) \tag{6.99}$$

a fenti kifejezés az alábbi alakban írható fel:

$$\mathbf{E}\left[P_{B|i}\right] \leq (M-1) \left[\sum_{y} \left[\sum_{x} \sqrt{P_{Y|X}(y \mid x)} Q_X(x) \right]^2 \right]^N, \tag{6.100}$$

amiből a határsebesség definícióját felhasználva a

$$\mathbf{E}\left[P_{B|i}\right] \leq (M-1)\, 2^{-NR_0} \tag{6.101}$$

összefüggéshez jutunk. Ezután figyelembe véve, hogy $(M-1) < M = 2^{NR}$ a

$$\mathbf{E}\left[P_{B|i}\right] \leq (M-1)\, 2^{-NR_0} < M 2^{-NR_0} = 2^{-N(R_0-R)} \tag{6.102}$$

felső korlátot kapjuk.

Véletlen blokk kódok úniós korlátja

Ha egy $M = 2^{NR}$ számú N hosszúságú kódszavakból álló blokk kód minden kódszavát betűnként függetlenül sorsoljuk ki azonos $Q_X(x)$ eloszlással, akkor az így kialakított összes lehetséges blokk kód átlagos blokkhibavalószínűségének a felső korlátja a

$$\mathbf{E}\left[P_B\right] \leq 2^{-N(R_0-R)} \tag{6.103}$$

kifejezéssel határozható meg.

A kifejezés tartalmát a következőképpen magyarázhatjuk:

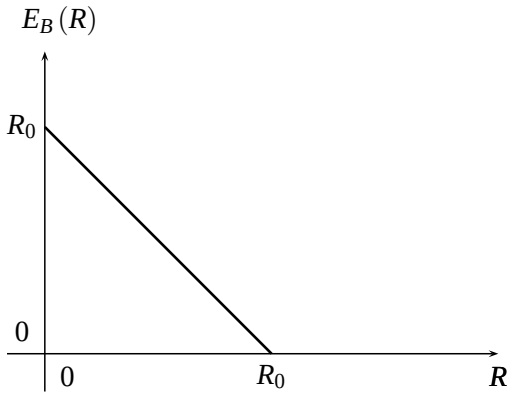
- Ha $R < R_0$, akkor N növelésével a $\mathbf{E}\left[P_B\right]$ felső korlátja nullához tart. Ebből az következik, hogy az R_0 határsebesség alatt a csatornában a blokkhossz növelésével aszimptotikusan hibamentesen lehet az adatokat továbbítani.

- Az előbbi állításból következik, hogy $R_0 < C$, mivel a diszkrét memóriamentes csatorna kódolási tételének a megfordítása szerint a kapacitás felett még aszimptotikusan sem lehet hibamentesen kommunikálni.

- Ezek alapján R_0 egy olyan, a csatorna minőségét jellemző paraméter, amely (i) megadja az átviteli sebesség felső korlátját, amely alatt a csatornában aszimptotikusan hibamentesen lehet kommunikálni, és (ii) véges átviteli sebességnél meghatározza az átlagos hibaarány felső korlátját is.

Mivel a $\mathbf{E}\left[P_B\right] \leq 2^{-N(R_0-R)}$ kifejezésben az $(R_0 - R)$ a kitevőben szerepel, ezért bevezetjük az úgynevezett Bhattacharyya-exponenst, amely

$$E_B(R) = R_0 - R, \tag{6.104}$$



6.6. ábra. A Bhattacharyya-exponens a csatorna átviteli sebességének a függvényében

értékű, és egyértelműen meghatározza azt, hogy véletlen kódolásnál az átlagos blokkhibavalószínűség felső korlátja hogyan függ az átviteli sebességtől. A Bhattacharyya-exponenst az R függvényében a 6.6. ábrán mutatjuk be.

A véletlen kódolási tétel Gallager-féle verziója

A korábbi fejezetekből tudjuk, hogy a Gallager-korlát optimális ρ érték esetén lényegesen szorosabb felső becslést ad, mint a Bhattacharyya-korlát. Alkalmazzuk tehát a

$$P_{B|i} \leq \sum_{\mathbf{y}} \left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_i)\right)^{\frac{1}{1+\rho}} \left\{ \sum_{\substack{j=1 \\ j\neq i}}^{M} \left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)\right)^{\frac{1}{1+\rho}} \right\}^{\rho}; \quad \rho \geq 0 \tag{6.105}$$

Gallager-korlátot véletlen kódolásnál a feltételes blokkhibavalószínűség meghatározására.

Tételezzük fel, hogy az aktuálisan átvitt kódszó az $\mathbf{x}_i = \mathbf{x}'_i$ rögzített értéket veszi fel, és számítsuk ki a feltételes blokkhibavalószínűség átlagos értékét véletlen kódolás esetén, ha a többi $\mathbf{x}_j$ $(i = 1,2,...,M, \quad i \neq j)$ kódszót véletlenül választjuk ki a lehetséges kódszavak halmazából valamilyen közös sorsolási valószínűségi eloszlás szerint. A várható érték ekkor a

$$\mathbf{E}\left[P_{B|i} \mid \mathbf{X}_i = \mathbf{x}'_i\right] \leq \sum_{\mathbf{y}} \left(P_{\mathbf{Y}|\mathbf{X}}\left(\mathbf{y} \mid \mathbf{x}'_i\right)\right)^{\frac{1}{1+\rho}} \mathbf{E}\left[\left\{ \sum_{\substack{j=1 \\ j\neq i}}^{M} \left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)\right)^{\frac{1}{1+\rho}} \right\}^{\rho} \mid \mathbf{X}_i = \mathbf{x}'_i \right]; \quad \rho \geq 0 \tag{6.106}$$

kifejezés segítségével határozható meg.

A következő átalakítás előtt korábbi tanulmányainkból bizonyítás nélkül idézzük vissza az úgynevezett Jensen-egyenlőtlenséget, ami a következőket mondja ki: ha X egy valószínűségi változó és az $f(x)$ függvény konvex, akkor

$$\mathbf{E}[f(X)] \leq f(\mathbf{E}[X]), \tag{6.107}$$

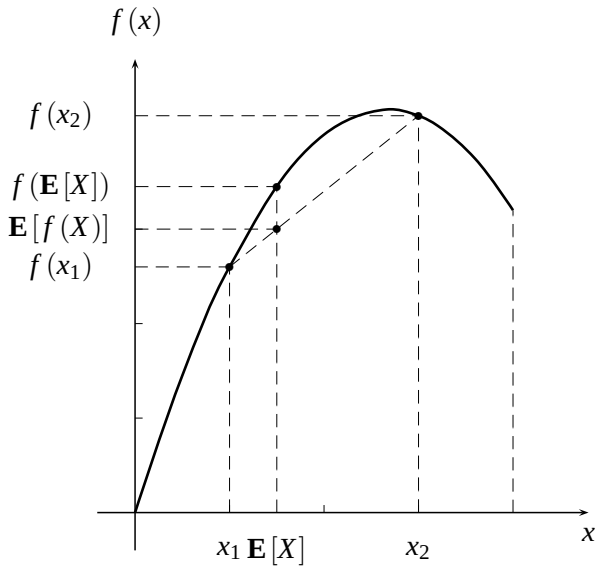
illetve, ha az $f(x)$ függvény konkáv, akkor

$$\mathbf{E}[f(X)] \geq f(\mathbf{E}[X]). \tag{6.108}$$

A Jensen-egyenlőtlenséget az 6.7. ábrán illusztráljuk konvex $f(x)$ függvény és bináris X valószínűségi változó esetén, ahol $\Pr(X = x_1) = p$ és $\Pr(X = x_2) = 1 - p$.

Alkalmazzuk a Jensen-egyenlőtlenséget az egyszerű hatványfüggvény esetében, ahol

$$f(x) = x^{\rho}. \tag{6.109}$$



6.7. ábra. A Jensen-egyenlőtlenség illusztrációja konvex függvény esetén ($p = 0,25$)

Tudjuk, hogy ez a függvény konvex az $x \geq 0$, $0 \leq \rho \leq 1$ tartományban, mivel ilyenkor a függvény második deriváltja

$$f''(x) = \rho(\rho - 1) x^{\rho - 2} \leq 0, \tag{6.110}$$

ezért a feltételes blokkhibavalószínűség átlagos értékének a kifejezésében szereplő

$$\mathbf{E}\left[\left\{\sum_{\substack{j=1\\ j\neq i}}^{M} \left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)\right)^{\frac{1}{1+\rho}}\right\}^{\rho} \mid \mathbf{X}_i = \mathbf{x}_i'\right] \leq \left\{\sum_{\substack{j=1\\ j\neq i}}^{M} \mathbf{E}\left[\left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)\right)^{\frac{1}{1+\rho}} \mid \mathbf{X}_i = \mathbf{x}_i'\right]\right\}^{\rho}. \tag{6.111}$$

A fenti eredmény felhasználásával a feltételes blokkhibavalószínűség átlagos értékére a

$$\mathbf{E}\left[P_{B|i} \mid \mathbf{X}_i = \mathbf{x}_i'\right] \leq \sum_{\mathbf{y}} \left(P_{\mathbf{Y}|\mathbf{X}}\left(\mathbf{y} \mid \mathbf{x}_i'\right)\right)^{\frac{1}{1+\rho}} \left\{\sum_{\substack{j=1\\ j\neq i}}^{M} \mathbf{E}\left[\left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)\right)^{\frac{1}{1+\rho}} \mid \mathbf{X}_i = \mathbf{x}_i'\right]\right\}^{\rho} \tag{6.112}$$

kifejezést kapjuk.

Ha a kódszavak páronként függetlenek, akkor

$$\mathbf{E}\left[\left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)\right)^{\frac{1}{1+\rho}} \mid \mathbf{X}_i = \mathbf{x}_i'\right] = \mathbf{E}\left[\left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}_j)\right)^{\frac{1}{1+\rho}}\right] = \sum_{\mathbf{x}} \left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x})\right)^{\frac{1}{1+\rho}} Q_{\mathbf{X}}(\mathbf{x}), \tag{6.113}$$

ezért

$$\mathbf{E}\left[P_{B|i} \mid \mathbf{X}_i = \mathbf{x}_i'\right] \leq \sum_{\mathbf{y}} \left(P_{\mathbf{Y}|\mathbf{X}}\left(\mathbf{y} \mid \mathbf{x}_i'\right)\right)^{\frac{1}{1+\rho}} (M-1)^{\rho} \left(\sum_{\mathbf{x}} \left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x})\right)^{\frac{1}{1+\rho}} Q_{\mathbf{X}}(\mathbf{x})\right)^{\rho}, \tag{6.114}$$

és

$$\mathbf{E}\left[P_{B|i}\right] \leq \sum_{\mathbf{x}_i'} \mathbf{E}\left[P_{B|i} \mid \mathbf{X}_i = \mathbf{x}_i'\right] Q_{\mathbf{X}}\left(\mathbf{x}_i'\right), \tag{6.115}$$

amiből

$$\mathbf{E}\left[P_{B|i}\right] \leq \sum_{\mathbf{y}} \sum_{\mathbf{x}_i'} \left(P_{\mathbf{Y}|\mathbf{X}}\left(\mathbf{y} \mid \mathbf{x}_i'\right)\right)^{\frac{1}{1+\rho}} Q_{\mathbf{X}}\left(\mathbf{x}_i'\right) (M-1)^{\rho} \left(\sum_{\mathbf{x}} \left(P_{\mathbf{Y}|\mathbf{X}}\left(\mathbf{y} \mid \mathbf{x}\right)\right)^{\frac{1}{1+\rho}} Q_{\mathbf{X}}\left(\mathbf{x}\right)\right)^{\rho} =$$

$$= (M-1)^{\rho} \sum_{\mathbf{y}} \left[\sum_{\mathbf{x}} \left(P_{\mathbf{Y}|\mathbf{X}}\left(\mathbf{y} \mid \mathbf{x}\right)\right)^{\frac{1}{1+\rho}} Q_{\mathbf{X}}\left(\mathbf{x}\right)\right]^{1+\rho}. \tag{6.116}$$

A kifejezések alapján megállapítható, hogy az így kiszámolt felső korlát csak a csatorna paramétereitől, a sorsolási (kódválasztási) statisztikától és a kódszavak számától függ. A felső korlátot diszkrét memóriamentes csatorna esetén a

$$\mathbf{E}\left[P_{B|i}\right] \leq (M-1)^{\rho} \left[\sum_{y} \left[\sum_{x} \left(P_{Y|X}\left(y \mid x\right)\right)^{\frac{1}{1+\rho}} Q_X\left(x\right)\right]^{1+\rho}\right]^{N} \tag{6.117}$$

alakra írhatjuk át, ahol $P_{Y|X}\left(y \mid x\right)$ a csatorna egy kódbetűre vonatkozó feltételes valószínűségi eloszlása, N a blokk kód hossza, $Q_X\left(x\right)$ pedig az egy kódbetű sorsolási valószínűségi eloszlása.

A fentiek alapján definiálhatjuk az $E_0\left(\rho, Q\right)$ úgynevezett Gallager-függvényt:

$$E_0\left(\rho, Q\right) = -\log_2 \sum_{y} \left[\sum_{x} \left(P_{Y|X}\left(y \mid x\right)\right)^{\frac{1}{1+\rho}} Q_X\left(x\right)\right]^{1+\rho}, \tag{6.118}$$

amit felhasználva a felső korlát a

$$\mathbf{E}\left[P_{B|i}\right] \leq (M-1)^{\rho}\, 2^{-NE_0(\rho,Q)}, \quad 0 \leq \rho \leq 1 \tag{6.119}$$

egyszerű formában adható meg. Kihasználva, hogy

$$(M-1)^{\rho} \leq M^{\rho} = 2^{\rho NR}, \tag{6.120}$$

a felső korlátra a

$$\mathbf{E}\left[P_{B|i}\right] \leq 2^{-N(E_0(\rho,Q)-\rho R)}, \quad 0 \leq \rho \leq 1 \tag{6.121}$$

végső formulát kapjuk.

Véletlen blokk kódok Gallager-korlátja

Ha adott egy diszkrét memóriamentes csatorna, melyben N hosszúságú véletlen blokk kóddal viszünk át $M = 2^{NR}$ számú üzenetet oly módon, hogy a kódszavakat páronként függetlenül választjuk, és a kódszavak egyes betűit egy adott $Q_X\left(x\right)$ valószínűségi eloszlás szerint egymástól függetlenül sorsoljuk, akkor az összes lehetséges M elemű kódok halmaza felett értelmezett P_B blokkhibavalószínűség átlagos értékének felső korlátja

$$\mathbf{E}\left[P_B\right] \leq 2^{-NE_G(R)}, \quad 0 \leq \rho \leq 1 \tag{6.122}$$

értékű, függetlenül a $P_Z\left(z\right)$ forráseloszlástól. A kifejezésben

$$E_G\left(R\right) = \max_{Q} E_R\left(R, Q\right) = \max_{Q} \max_{0 \leq \rho \leq 1} \left[E_0\left(\rho, Q\right) - \rho R\right], \tag{6.123}$$

az úgynevezett Gallager-exponens, ahol

$$E_G\left(R, Q\right) = \max_{0 \leq \rho \leq 1} \left[E_0\left(\rho, Q\right) - \rho R\right]. \tag{6.124}$$

A Gallager-függvény és a Gallager-exponens tulajdonságai

A további vizsgálatok előtt adjuk meg a Gallager-függvény és a Gallager-exponens tulajdonságait (lásd a Függelék 8.1. fejezetét).

- A korábbiakból tudjuk, hogy $\rho = 1$ esetén a Gallager-korlát azonos a Bhattacharyya-korláttal, ezért a Gallager-függvény
$$\max_{Q} E_0(\rho, Q)\big|_{\rho=1} = R_0\,, \tag{6.125}$$
így a ρ szerinti maximumkeresés után biztosan igaz, hogy
$$E_G(R) \geq E_B(R) = R_0 - R, \tag{6.126}$$
ahol R_0 a csatorna határsebessége, $E_B(R)$ pedig a korábban megismert Bhattacharyya-exponens.

- A Gallager-függvény $\rho = 0$-nál nulla, a $0 \leq \rho \leq 1$ tartományban nem negatív és ρ-val monoton nő, azaz
$$E_0(\rho, Q) \geq E_0(0, Q) = 0, \quad 0 \leq \rho \leq 1, \tag{6.127}$$
és
$$\frac{\partial E_0(\rho, Q)}{\partial \rho} > 0, \quad 0 \leq \rho \leq 1. \tag{6.128}$$

- A függvény a $0 \leq \rho \leq 1$ tartományban konvex, azaz
$$\frac{\partial^2 E_0(\rho, Q)}{\partial^2 \rho} \leq 0, \quad 0 \leq \rho \leq 1. \tag{6.129}$$

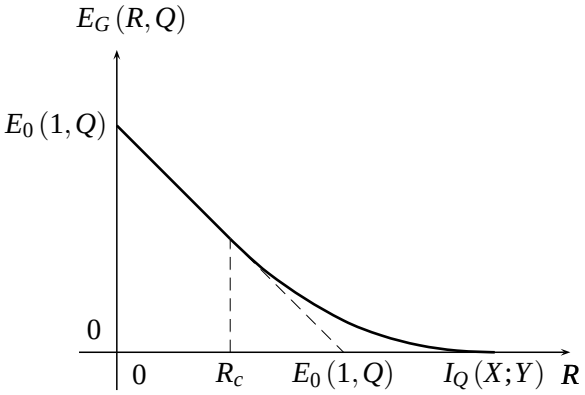
- A függvény kezdeti deriváltja a $\rho = 0$-nál egyenlő a csatorna bemeneti és kimeneti jelei közötti
$$I(X;Y) = H(Y) - H(Y \mid X) \tag{6.130}$$
kölcsönös információval.

- Az $E_G(R, Q)$ exponens az $R = 0$ helyen azonos a Gallager-függvény $\rho = 1$ helyen felvett értékével, mivel
$$E_G(0, Q) = \max_{0 \leq \rho \leq 1} [E_0(\rho, Q) - \rho R]\,|_{R=0} = \max_{0 \leq \rho \leq 1} [E_0(\rho, Q)] = E_0(1, Q)\,, \tag{6.131}$$
mivel $E_0(\rho, Q)$ a $\{0 \leq \rho \leq 1\}$ tartományban ρ-val monoton nő.

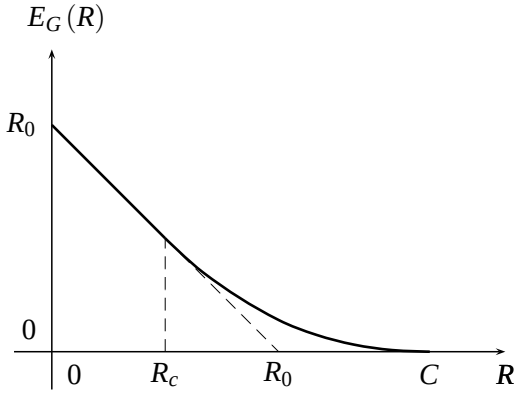
- Az $E_G(R, Q)$ függvény a $\{0 \leq R \leq R_c(Q)\}$ tartományban -1 meredekségű az R függvényében, ahol
$$R_c(Q) = \frac{\partial E_0(\rho, Q)}{\partial \rho}\Big|_{\rho=1}\,. \tag{6.132}$$

- Az $E_G(R, Q)$ függvény az $0 \leq R \leq I_Q(X;Y)$ tartományban pozitív és konkáv (felülről homorú), ahol
$$I_Q(X;Y) = I(X;Y)\big|_{P_X(x)=Q_X(x)}\,. \tag{6.133}$$

Az $E_G(R, Q)$ függvény tulajdonságait a 6.8. ábrán adtuk meg.
Ha ezután végrehajtjuk az $E_G(R, Q)$ függvény optimalizálását a $Q_X(x)$ szerint, akkor az
$$E_G(R) = \max_{Q_X(x)} E_G(R, Q)\,, \tag{6.134}$$
Gallager-exponens értékét kapjuk, melyet a 6.9. ábrán illusztrálunk. Az ábra alapján megállapíthatjuk, hogy az $E_G(R)$ Gallager-exponens a csatorna kapacitása alatt nem negatív értékű, vagyis a korábban meghatározott átlagos blokkhibavalószínűség felső korlátja
$$\mathbf{E}[P_B] \leq 2^{-NE_G(R)}, \quad 0 \leq \rho \leq 1 \tag{6.135}$$
az N növelésével aszimptotikusan nullához tart. Ez azt jelenti, hogy a kapacitásig a csatornában aszimptotikusan hibamentesen lehet kommunikálni, ugyanakkor a fenti egyenlőtlenség segítségével az átlagos blokkhibavalószínűség felső korlátját is meg lehet határozni.



6.8. ábra. Az $E_G(R,Q)$ Gallager-exponens a csatorna átviteli sebességének a függvényében



6.9. ábra. Az $E_G(R)$ Gallager-exponens a csatorna átviteli sebességének a függvényében

6.9. A véletlen kódolási korlátok értelmezése

A korábbi fejezetekben blokk kódolás esetén meghatároztuk a blokkhibavalószínűség felső korlátját véletlen kódválasztást feltételezve. Sajnos ez a korlát első közelítésben a konkrét rendszerekről nem mond semmit, hiszen, abból a tényből, hogy az összes lehetséges blokk kód feletti $\mathbf{E}(P_B)$ átlagos blokkhibavalószínűség felső korlátja elegendően kicsi, még nem következik, hogy létezik olyan kód, amely az összes lehetséges P_Z forráseloszlás mellett elegendően jó $P_{B|i}$ értéket ad ($P_{B|i}$ az i-dik üzenethez tartozó feltételes blokkhibavalószínűség).

Legyen a forrás eloszlása egyenletes, azaz $P_Z(i) = 1/M$, és jelöljük P_B-vel az egyes üzenetekhez tartozó feltételes hibavalószínűségek egyszerű aritmetikai átlagát:

$$P_B = \frac{1}{M}\sum_{i=1}^{M} P_{B|i}. \tag{6.136}$$

Ezután tételezzük fel, hogy M páros, tehát $M = 2M'$, és vegyük ki a halmazból azt az M' kódszót, amelyeknél a $P_{B|i}$ a legnagyobb. A megmaradó M' számú kódszó esetére biztosan igaz, hogy minden $P_{B|i}$ feltételes blokkhibavalószínűség (lásd a Függelék 8.2. fejezetét)

$$P_{B|i} \leq 2P_B. \tag{6.137}$$

Tekintsük ezután a megmaradt M' számú kódszót egy új kódnak, amire maximum likelihood dekódolási szabály alkalmazása mellett igaz, hogy

$$P'_{B|i} \leq \left(P'_{B|i}\right)_{wc} \leq 2P_B \tag{6.138}$$

Felhasználva az úniós Bhattacharyya-korlátot

$$\mathbf{E}\left[\left(P'_B\right)_{wc}\right] \leq 2\mathbf{E}\left[P_B\right] < 2\times 2^{-N(R_0-R)}, \tag{6.139}$$

ahol R az eredeti kód átviteli sebessége, és

$$R' = \frac{1}{N}\log_2 M' = R - \frac{1}{N} \tag{6.140}$$

az új kód átviteli sebessége. Ezekkel a jelölésekkel igaz, hogy

$$\mathbf{E}\left[\left(P'_B\right)_{wc}\right] < 4\times 2^{-N(R_0-R')}. \tag{6.141}$$

Ez az egyenlet azt mondja ki, hogy léteznie kell legalább egy R' átviteli sebességű kódnak, amelynek minden blokkhibavalószínűsége nem rosszabb, mint ez az átlag.

Az egyenletesen jó kód létezése

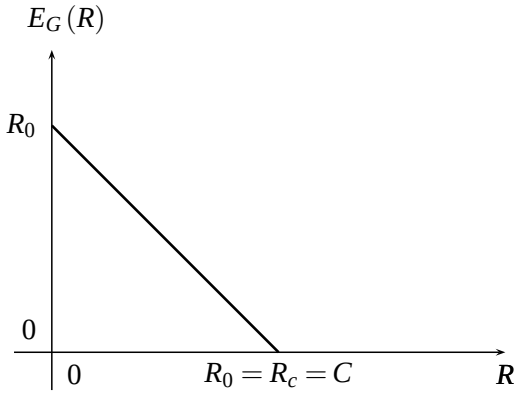
Létezik legalább egy $M = 2^{NR}$ méretű, N hosszúságú kódszavakból álló blokk kód, amelynek a legrosszabb esetben számolt blokkhibavalószínűsége diszkrét memóriamentes csatornában (DMC) maximum likelihood (ML) dekódolási szabályt alkalmazva teljesíti az alábbi egyenlőtlenségeket:

$$(P_B)_{wc} < 4\times 2^{-N(R_0-R)}, \tag{6.142}$$

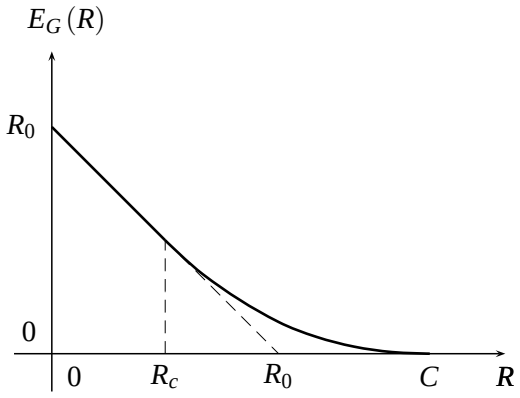
Bhattacharyya-korlát, illetve

$$(P_B)_{wc} < 4\times 2^{-NE_G(R)} \tag{6.143}$$

Gallager-korlát esetén. Az $E_G(R)$ Gallager-exponens jellegét a 6.10. és 6.11. ábrán illusztráljuk az $R_0 = C$ és az $R_0 < C$ esetekben.



6.10. ábra. Az $E_G(R)$ Gallager-exponens jellege az $R_0 = C$ esetén



6.11. ábra. Az $E_G(R)$ Gallager-exponens jellege az $R_0 < C$ esetén

7. fejezet

Fa és trellis kódolás

Ebben a fejezetben a blokk kódolás technikájával szemben a csatornakódolás két másik területét a fa, illetve trellis kódolást elemezzük. Ezek a kódolási módszerek sok alkalmazási területen felülmúlják a hagyományos blokk kódolás minőségi paramétereit, ezért a mindennapi gyakorlat szempontjából is igen jelentősek. A korszerű vezetéknélküli kommunikációs rendszerek szinte mindegyike használja őket.

A kódolási módszer elméleti vizsgálata előtt az alapok jobb megérttetése érdekében egy egyszerű, de ténylegesen alkalmazható megoldás részletes vizsgálatával foglalkozunk, és ezen a példán illusztráljuk a témával kapcsolatos legfontosabb fogalmakat.

Egy elvi példa vizsgálata

A kódolási rendszer pontos definíciójának megadása és az általános analízis előtt elemezzük a 7.1. ábrán megadott egyszerű bináris konvolúciós kódoló működését.

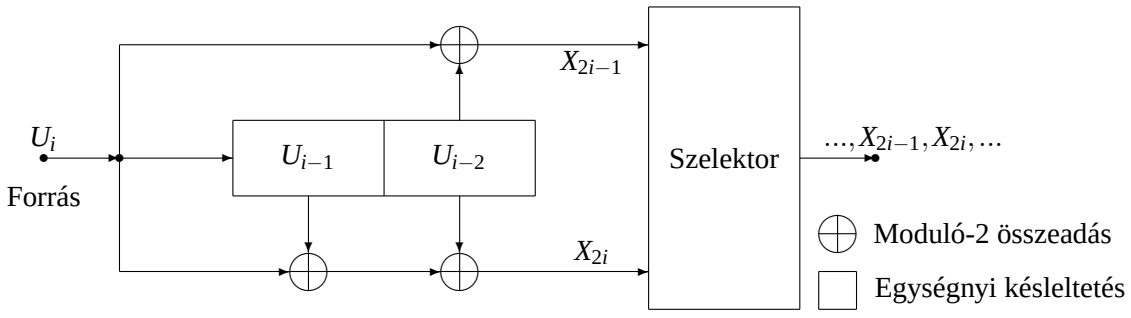
Az ábrán $\{U_i\}$ a bináris forrásszimbólumok sorozata, $\{X_i\}$ a kódolt bináris szimbólumok sorozata.

A rendszer a következőképpen működik:

- A forrás szimbólumai egy két elemből álló shift regiszter bemenetére kerülnek, és egy egyszerű, moduló-2 összeadókat tartalmazó logika az U_i aktuális forrásszimbólum és az U_{i-1}, U_{i-2} korábbi forrásszimbólumok felhasználásával előállítja az X_{2i-1} és X_{2i} kódolt jeleket. A kódoló tehát memóriával rendelkezik, vagyis az aktuális kimeneti jelei nem csak az aktuális bemeneti szimbólumoktól, hanem a korábbi értékektől is függenek.

- A szelektor az X_{2i-1} és X_{2i} szimbólumokat sorszám szerint rendezi. Mivel egy forrásszimbólumhoz két kódszimbólum tartozik, a kódolási arány

$$R_t = \frac{1}{2}. \tag{7.1}$$



7.1. ábra. A példaként vizsgált egyszerű bináris konvolúciós kódoló felépítése

A kódoló kimenetén az alábbi jelek jelennek meg:

$$X_{2i-1} = U_i \oplus U_{i-2} \qquad i = 1,2,... \tag{7.2}$$

$$X_{2i} = U_i \oplus U_{i-1} \oplus U_{i-2} \quad i = 1,2,... \tag{7.3}$$

A fenti eredmény felfogható úgy is, mint a bemeneti sorozat és az $1,0,1,0,0,...$, illetve az $1,1,1,0,0,...$ sorozat ("súlyfüggvény") konvolúciója. Innen ered a konvolúciós kódolás elnevezés.

Más szemmel nézve ez a rendszer egy véges állapotú szekvenciális logikai hálózat, amelyben a kimeneti jelek a bemeneti jelektől és a rendszer állapotváltozóitól, a memóriák tartalmától függenek. Ugyanakkor a rendszer következő állapota is a bemeneti jelek és az aktuális állapot függvénye. A kódoló aktuális σ_i állapota nem más, mint a shift regiszter celláinak a tartalma:

$$\sigma_i = [U_{i-1}, U_{i-2}]\,. \tag{7.4}$$

A szekvenciális logikai hálózatok kimenetét a bemeneti sorozat és a

$$\sigma_1 = [0,0]\,, \tag{7.5}$$

vagy az ezzel egyenértékű

$$U_0 = U_{-1} = 0 \tag{7.6}$$

kezdeti állapotból egyértelműen meg lehet határozni. Megjegyzendő, hogy ennek a rendszernek két szabadsági foka, vagy két független kezdeti feltétele van.

Fa típusú kódok

Ha elhatározzuk, hogy a 7.1. ábrán bemutatott kódolót L_t számú információs bit kódolására használjuk, majd ezt követően éppen T számú 0 értékű bitet adunk a kódoló bemenetére, azaz az

$$U_1, U_2, U_3, ..., U_{L_t}, U_{L_t+1} = 0, U_{L_t+2} = 0, ..., U_{L_t+T} = 0 \tag{7.7}$$

bitsorozatot kódoljuk, akkor a kódoló kimenetén az

$$\mathbf{X} = [X_1, X_2, X_3, ..., X_N] \quad N = 2\,(L_t + T) \tag{7.8}$$

N hosszúságú kódszó jelenik meg (ahol T a kódolóban lévő shift regiszter hossza).

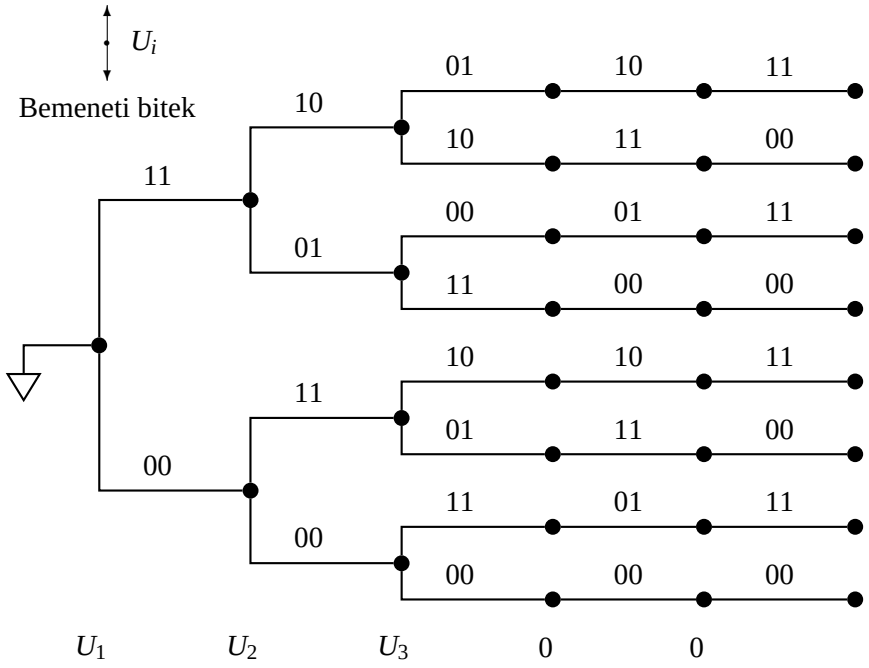
A kódoló ebben az esetben egy L_t hosszúságú bitsorozathoz N hosszúságú kódszót rendel, azaz úgy viselkedik, mint egy

$$R = \frac{L_t}{L_t + T} R_t = \frac{K}{N} \tag{7.9}$$

kódolási arányú blokk kódoló. A kódszavak ilyenkor egy gyökeres fa terminális csomópontjaihoz rendelhetők, ezért az ilyen elven működő kódokat fa típusú kódoknak nevezzük. A 7.2. ábrán ezt a fát ábrázoltuk $L_t = K = 3$ és $T = 2$ esetén. Az ábrán az egyes belső csomópontokban elágazások vannak, és az elágazás iránya az aktuális bemeneti bit értékétől függ. Ha az aktuális bemeneti bit logikai 1 értéket vesz fel, akkor a fa felfelé ágazik el, ha a bit értéke logikai 0, akkor pedig lefelé. Az fa egyes ágait a kódoló által előállított X_{2i-1} és X_{2i} kimeneti bitekkel címkéztük fel. Példánkban a három értékes bithez tartozó nyolc különböző $N = 10$ hosszúságú kódszó a fa gyökerétől az egyes terminális csomópontokhoz tartozó utak mentén olvasható le.

Trellis kódok

A mintarendszerünk működését más megközelítésben is vizsgálhatjuk. $U_{-1} = U_0 = U_4 = U_5 = 0$ feltételek mellett tetszőleges értékes $[U_1, U_2, U_3]$ bemeneti sorozat kódolása esetén ábrázolni tudunk egy olyan fát is, amelynek minden elágazásában feltüntetjük a kódoló aktuális állapotát, a shift regiszter tartalmát is. Ezt a fát adtunk meg a 7.3. ábrán. A fa egyes belső csomópontjaiban ismét elágazások vannak, és az elágazás iránya az aktuális bemeneti bit értékétől függ. Ha az aktuális bemeneti bit



7.2. ábra. A bináris fa típusú kód ábrázolása

logikai 1 értéket vesz fel, akkor a fa felfelé ágazik el, ha a bit értéke logikai 0, akkor pedig lefelé. Az fa egyes ágait most is a kódoló által előállított X_{2i-1} és X_{2i} kimeneti bitekkel címkéztük fel.

A gyökérnél a kódoló kezdeti állapota $\sigma_i = [U_{i-1}, U_{i-2}] = [0,0]$, mivel $U_{-1} = U_0 = 0$. Innen indulva az állapotok, az elágazások iránya és kódoló által előállított kimeneti bitek a bemeneti bitek értékétől függenek. Mindez azt jelenti, hogy ez a fa az általunk korábban említett sorrendi hálózat teljes működését leírja, mivel egyszerre jellemzi

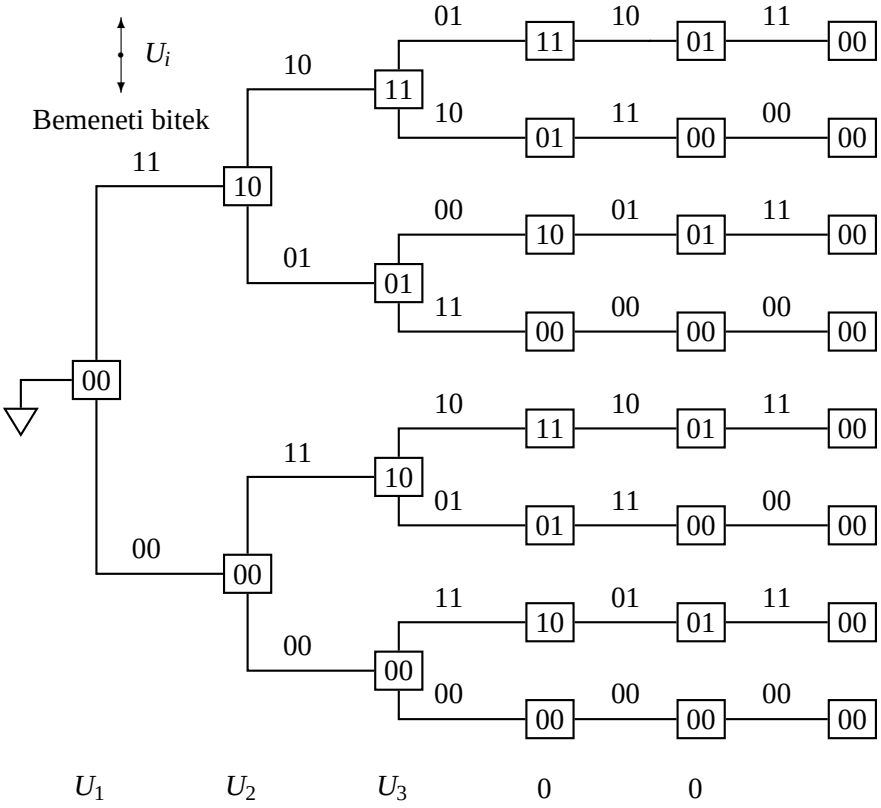
- a kódoló belső állapotának a függését a bemeneti jelektől és a rendszer aktuális állapotától,
- és a rendszer kimeneti jeleinek a függését a a bemeneti jelektől és a rendszer aktuális állapotától.

Ez a két függvény pedig nem más, mint egy dinamikus rendszer állapotváltozós leírása.

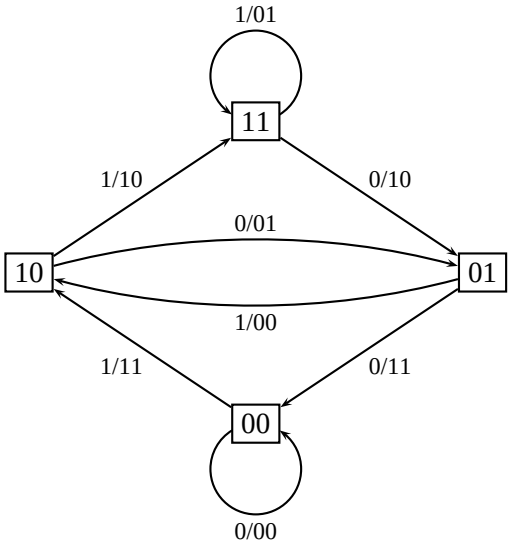
A dinamikus rendszerek működését más kanonikus leírási módszerekkel is tudjuk jellemezni. Ilyen a 7.4. ábrán megadott úgynevezett állapotátmenet diagram, ahol a rendszer állapotaihoz csomópontokat rendelünk, és a csomópontok közötti átmeneteket a $U_i/X_{2i-1}, X_{2i}$ adatokkal, tehát az aktuális bemeneti és a kimeneti bitekkel címkéztük fel. A 7.3. és a 7.4. ábra között az a lényeges különbség, hogy az előbbi a rendszer működését egy kijelölt időintervallumban, az idő függvényében írja le, míg az állapotátmenet diagram a rendszert az időtől függetlenül jellemzi.

A 7.5. ábrán látható trellis a 7.3. ábrán megadott fa és az állapotátmenet diagram tulajdonságait egyesíti azáltal, hogy az állapotok közötti átmeneteket időben írja le. A trellis-en a függőleges tengely irányában az rendszer különböző állapotait tüntettjük fel, az állapotok közötti átmenetek a trellis alatt feltüntetett bemeneti U_i bitektől függenek. Ha az aktuális bemeneti bit logikai 1 értéket vesz fel, akkor a trellis felfelé ágazik el, ha a bit értéke logikai 0, akkor pedig lefelé. A trellis egyes átmeneteit a kódoló által előállított X_{2i-1} és X_{2i} kimeneti bitekkel címkéztük fel.

Az ábráról most is egyértelműen leolvashatók az $[U_{-1} = 0, U_0 = 0, U_1, U_2, U_3, U_4 = 0, U_5 = 0]$ bemeneti sorozathoz tartozó $N = 10$ hosszúságú kódszavak. Ehhez nem kell mást tenni, mint a trellis ágairól leolvasni a bemeneti bitek által meghatározott elágazási irányok szerint a kódoló által előállított X_{2i-1} és X_{2i} kimeneti biteket a trellis kezdő és végpontja között. Érdemes megjegyezni, hogy ha



7.3. ábra. A kódoló működésének a leírsa a belső állapotok feltüntetésével



7.4. ábra. A négy belső állapotú konvolúciós kódoló állapotátmeneti diagramja

a kódoló kezdeti feltétele $\sigma_1 = [0,0]$ és bemeneti bitsorozat utolsó T számú bitje (esetünkben $T = 2$) logikai 0 értéket vesz fel, akkor a folyamat végén a kódoló belső állapota $\sigma_{L_t+T+1} = [0,0]$ lesz, azaz a rendszer visszatér az eredeti kezdeti állapotába.

Mivel a kódoló működésének leírására a trellis igen alkalmas, az ilyen kódolóval generált kódokat **trellis kódnak**, illetve az ilyen kódolót **trellis kódolónak** nevezzük. Emellett fontos megjegyezni, hogy a trellis struktúra speciális tulajdonságait a dekódolásnál komolyan ki lehet használni.

Azt az N_t számot ami meghatározza, hogy egy bemeneti szimbólumtól hány kimeneti szimbólum függ a kódoló **kényszertávolságának** nevezzük. Ez esetünkben az $N_t = (T+1)/R_t = 6$ értékkel egyenlő.

7.1. A Viterbi féle maximum likelihood dekódolási algoritmus

A következőkben egy olyan, gyakorlatban igen fontos algoritmussal ismerkedünk meg, amely lehetővé teszi a konvolúciós kódok maximum likelihood értelemben vett optimális dekódolását zajos csatornák esetén.

Az algoritmus általános definíciója helyett most is a 7.1. ábrán megadott egyszerű bináris konvolúciós kódoló példájával illusztráljuk a működést, ráadásul feltételezzük, hogy a kódolt jeleket bináris szimmetrikus csatornán (BSC) továbbítjuk. Az algoritmust tehát igen egyszerű feltételek mellett mutatjuk be, ugyanakkor törekszünk arra, hogy a működéssel kapcsolatos általános fogalmakat maradéktalanul megismertessük.

Tételezzük fel, hogy a bináris szimmetrikus csatorna hibaparamétere benne van a $0 < \varepsilon < 0.5$ tartományban, és legyen a dekódolás maximum likelihood típusú. A korábbiakból ismert, hogy a diszkrét memóriamentes csatorna $\mathbf{X}$ bemeneti és $\mathbf{Y}$ kimeneti vektorai között értelmezett feltételes valószínűségi eloszlásfüggvény szorzat alakban írható fel, azaz

$$P(\mathbf{y} \mid \mathbf{x}) = \prod_{n=1}^{N} P(y_n \mid x_n) = \prod_{n=1}^{N} \left[(1-\varepsilon) I(y_i = x_i) + \varepsilon I(y_i \neq x_i)\right], \tag{7.10}$$

ahol $I(A)$ az A esemény indikátora:

$$I(A) = \begin{cases} 1, & \texttt{ha } A = \texttt{igaz} \\ 0, & \texttt{ha } A = \texttt{hamis} \end{cases}. \tag{7.11}$$

Ennek alapján ismert $\mathbf{y}$ és $\mathbf{x}$ esetén

$$P(\mathbf{y} \mid \mathbf{x}) = (1-\varepsilon)^{N-d((\mathbf{x},\mathbf{y}))} \varepsilon^{d((\mathbf{x},\mathbf{y}))} = (1-\varepsilon)^N \left(\frac{\varepsilon}{1-\varepsilon}\right)^{d(\mathbf{x},\mathbf{y})}, \tag{7.12}$$

ahol $d(\mathbf{x},\mathbf{y})$ az $\mathbf{x}$ és $\mathbf{y}$ vektorok Hamming-távolsága (azon pozíciók száma, ahol az $\mathbf{x}$ bemeneti és $\mathbf{y}$ kimeneti N hosszúságú vektorok azonos sorszámú elemei különböznek egymástól).

Mivel tudjuk, hogy

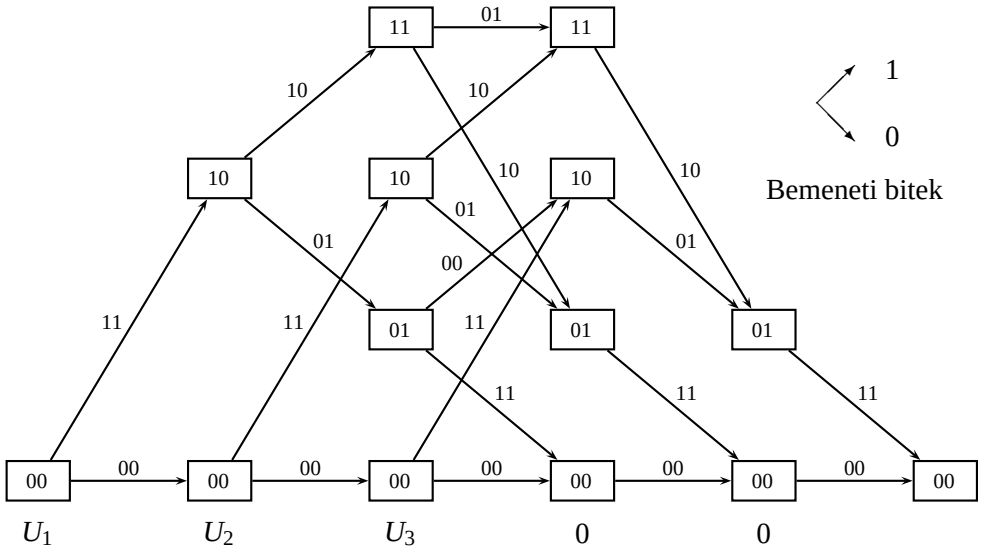
$$0 < \varepsilon < \frac{1}{2} \tag{7.13}$$

ebből nyilvánvaló, hogy

$$0 < \frac{\varepsilon}{1-\varepsilon} < 1, \tag{7.14}$$

ezért a maximum likelihood dekódolási szabály szerint adott $\mathbf{y}$ vektorhoz azt az $\mathbf{x}^*$ vektort kell választani, ahol $P(\mathbf{y} \mid \mathbf{x}^*)$ maximális, amihez esetünkben a $d(\mathbf{x},\mathbf{y})$ Hamming-távolság minimumához, vagy az $(N - d(\mathbf{x},\mathbf{y}))$ Hamming-egybeesés maximumához tartozó $\mathbf{x}^*$ értéket kell megkeresni.

Példa



7.5. ábra. A trellis felépítése a példaként vizsgált bináris kódoló esetén

Határozzuk meg ezután az maximum likelihood detektor által demodulált $\left[\widehat{U}_1, \widehat{U}_2\widehat{U}_3\right]$ sorozat értékét, ha a vevő bemenetére az

$$\mathbf{Y} = \mathbf{y} = [y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}] = [0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 1] \tag{7.15}$$

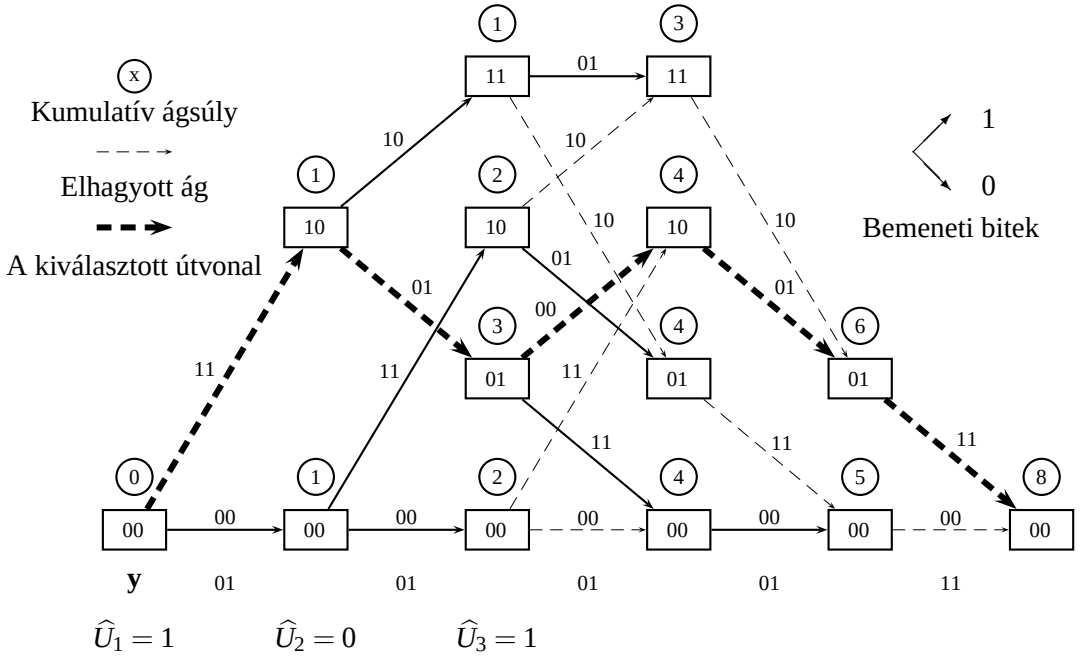
sorozat érkezik. Ehhez használjuk fel a 7.6. ábrán látható trellis-t oly módon, hogy a trellis minden időrésében számítsuk ki a Hamming-egybeesés értékét. A dekódoláskor alkalmazott **metrika**, azaz a trellis elejétől a végéig értelmezett utak "jóságának" a mérőszáma ugyanis a vett **y** vektor és az adott úthoz tartozó $\mathbf{x}_i$ kódszó Hamming-egybeeséseinek a száma.

A kitűzött feladatot az alábbi lépésekben végezhetjük el:

- A trellis minden időrésében kiszámítjuk az úgynevezett ágsúlyokat, a vett y_{2i-1}, y_{2i} szimbólumok és a trellis összes ágához rendelt x_{2i-1}, x_{2i} kódelemek Hamming-egybeesésének a számát. Ez például a második időrésben azt jelenti, hogy kiszámítjuk a bemeneti 01 szimbólumok és rendre az 00, 11, 01 és 10 kódszimbólumok közötti Hamming-egybeesés értékét, az 1, 1, 2 és 0 ágsúlyokat.

- A trellis minden állapotához hozzárendelünk egy memóriacellát, amelyben gyűjtjük a kumulatív ágsúlyokat, és ezzel az összeggel felcímkézzük az egyes állapotokat. Ez az első két időrésben annyit jelent, hogy az adott állapothoz egyszerűen hozzárendeljük a bemenettől az adott állapotig vezető ágak ágsúlyainak az összegét, ugyanis az első két időrésben a bemenettől minden állapothoz csak egyetlen úton lehet eljutni.

- A harmadik időrésben a trellis már teljes, mivel minden állapotból két másik állapotba lehet eljutni a kódoló szabályainak megfelelően. Ennek az a következménye, hogy az időrés végén minden állapotba az időrés elején lévő állapotokból két ág vezet. Nyilvánvaló, hogy ilyenkor a kumulatív ágsúlyok kiszámítása nem triviális, hiszen felvetődik a kérdés, hogy az adott időréshez tartozó ágsúlyok közül melyiket kell figyelembe venni az időrés végén a kumulatív ágsúlyok meghatározásánál. A kérdés a következőképpen válaszolható meg. A dekódolás során azt az utat kell kiválasztani, amely mentén a kumulatív ágsúlyok (a kumulatív Hamming-egybeesések) értéke maximális. Ebből következik, hogy az adott időrés végén a kumulatív ágsúlyok meghatározásánál



7.6. ábra. A Viterbi-algoritmus illusztrálása a példaként vizsgált bináris kódoló esetén bináris szimmetrikus csatornában, ha a vett jelsorozat $\mathbf{y} = \{0,1,0,1,0,1,0,1,1,1\}$

csak azt az ágat kell figyelembe venni, amely mentén a kumulatív ágsúly nagyobb, és a másik ág elhagyható. Példánkban ezt tettük akkor, amikor az [11] állapothoz tartozó kumulatív ágsúly meghatározásánál megnéztük, hogy mekkora az időrés elején a [11] állapothoz tartozó kumulatív ágsúly (ennek az értéke 1) és a két [11] állapot közötti ág súlya (ennek az értéke 2), tehát ezen a úton haladva az [11] állapot kumulatív ágsúlya az időrés végén 3, és ezt összehasonlítottuk azzal az esettel, amikor az időrés végén lévő [11] állapotba az [10] állapotból jutunk el. Ez utóbbi esetben az időrés elején lévő [10] állapothoz tartozó kumulatív ágsúly 2 értékű, az [10]-[11] átmenethez tartozó ágsúly pedig 0 értékű, ezért, ha ezen az úton jutnánk el az időrés végén az [11] állapotba, akkor az [11] állapothoz rendelt kumulatív ágsúly csak 2 értékű lenne. Ebből az következik, hogy az [10]-[11] átmenet a további vizsgálatból kizárható, mivel nem létezhet olyan optimális út, amely ezt az ágat tartalmazza. A fentiekből az következik, hogy ezt a lépést folytatva elérhető, hogy az időrések végén minden állapothoz csak egyetlen megmaradó ág vezessen. Az ábrán az elhagyott ágakat vékony szaggatott, a megmaradt ágakat pedig folytonos vonal jelöli.

- Ha a fentiekben leírt eljárást a teljes trellis-re végrehajtjuk, akkor a dekódolás igen egyszerű. Nem kell mást tenni, mint a kimenettől visszafelé haladva meg kell keresni az egyetlen megmaradó utat, és le kell olvasni azt, hogy ehhez az úthoz milyen bemeneti szimbólumok tartoznak. Az így kiválasztott utat vastag szaggatott vonallal ábrázoltuk, és tudjuk, hogy ehhez az úthoz az $\left[\widehat{U}_1 = 1, \widehat{U}_2 = 0, \widehat{U}_3 = 1\right]$ demodulált sorozat tartozik. Az ábrán a kiválasztott utat vastag szaggatott vonal jelöli.

A Viterbi dekódolás metrikájának a megválasztása általános esetben

A fentiekben vizsgált algoritmus akkor működik helyesen, ha olyan metrikát tudunk bevezetni, amely diszkrét memóriamentes csatornát feltételezve az alábbi tulajdonságokkal rendelkezik:

- A trellis egyes ágaihoz egymástól függetlenül rendelhető ágsúly, és a teljes út eredő metrikája az úthoz tartozó egyes ágak metrikájának az összege. A metrika tehát additív.

- A maximum likelihood szabály szerint kiválasztandó úthoz tartozik a legnagyobb kumulatív

metrika. Diszkrét memóriamentes csatornában (DMC) a csatorna kimenetén és bemenetén megjelenő bármely $\mathbf{y} = [y_1, y_2, ..., y_N]$ és $\mathbf{x} = [x_1, x_2, ..., x_N]$ szimbólumsorozat esetén

$$P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}) = \prod_{n=1}^{N} P(y_n \mid x_n), \tag{7.16}$$

illetve

$$\log\left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x})\right) = \sum_{n=1}^{N} \log\left(P_{Y|X}(y_n \mid x_n)\right), \tag{7.17}$$

ezért az additivitást akkor lehet biztosítani, ha az ágsúlyokat a $\log(P(y_n \mid x_n))$ értékhez kötjük, ugyanakkor ezzel az a feltétel is teljesül, hogy a maximális metrikájú úthoz tartozik a ML dekódolási szabály szerinti optimális $\left[\widehat{U}_1, \widehat{U}_2, \widehat{U}_3\right]$ dekódolt szimbólumsorozat, hiszen ehhez tartozik a

$$P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x}) \tag{7.18}$$

feltételes valószínűségi eloszlás $\mathbf{x}$ szerinti maximuma.

- Az ágsúly, azaz a metrika célszerűen nem negatív értékű.
- Egy időrésben, egy adott y_n vett szimbólum esetén, a legkisebb ágsúly célszerűen 0 értékű, hogy a detektorban a működés során a kumulatív ágsúlyok értéke a lehető legkisebb legyen.

A felsorolt feltételeket teljesíteni tudjuk akkor, ha a dekódolás során az alábbi metrikát maximalizáljuk:

$$\alpha \log\left(P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y} \mid \mathbf{x})\right) + \alpha \sum_{n=1}^{N} f(y_n) = \alpha \sum_{n=1}^{N} \left[\log\left(P_{Y|X}(y_n \mid x_n)\right) + f(y_n)\right]; \quad \alpha > 0, \tag{7.19}$$

ahol célszerűen

$$f(y) = -\log\left[\min_x P_{Y|X}(y \mid x)\right], \tag{7.20}$$

ezért a minimális ágsúly 0 értékű.

A fenti meggondolások alapján diszkrét memóriamentes csatornában a Viterbi-metrikát a következőképpen kell meghatározni:

Bármely vett $\mathbf{y} = [y_1, y_2, ..., y_N]$ sorozat esetén a trellis minden ágában egy x_n, y_n párhoz hozzá kell rendelni a $\mu_n(x_n, y_n)$ ágsúlyt, ahol

$$\mu_n(x_n, y_n) = \alpha\left[\log\left(P_{Y|X}(y_n \mid x_n)\right) + f(y_n)\right], \tag{7.21}$$

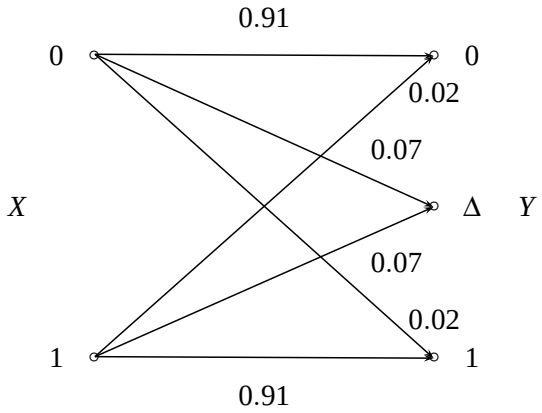
és

$$f(y) = -\log\left[\min_x P_{Y|X}(y \mid x)\right], \tag{7.22}$$

és a dekódolás során azt az utat kell kiválasztani a trellis-ben, amelyhez a maximális kumulatív metrika tartozik.

A Viterbi féle dekódolási algoritmus lépései

- Adott $\mathbf{y} = [y_1, y_2, ..., y_N]$ sorozat esetén a trellis minden időrésében $\mu_n(x_n, y_n)$ ágsúlyok meghatározása.
- A trellis állapotaihoz rendelt kumulatív ágsúlyok kiszámítása, és azok tárolása az állapotokhoz rendelt memóriákban. A kumulatív ágsúlyok kiszámításánál az elhagyható ágak kijelölése, és minden időrésben az adott állapothoz tartozó, egyetlen "versenyben maradt" ág megőrzése.
- A trellis végére érve annak az egyetlen útnak a kijelölése, amely a trellis bemenete és kimenete között megmaradt, és az ehhez az úthoz tartozó optimális dekódolt $\left[\widehat{U}_1 = 1, \widehat{U}_2 = 0, \widehat{U}_3 = 1\right]$ sorozat meghatározása.



7.7. ábra. A példában szereplő bináris szimmetrikus törléses csatorna (BSEC)

Példa

Alkalmazzuk a fentebb ismertetett Viterbi-algoritmust a 7.7. ábrán megadott diszkrét bináris szimmetrikus törléses csatorna esetén.

A dekódolási szabály alkalmazásához először meg kell határozni a $\mu_n(x_n, y_n)$ ágsúly függvényt. A csatorna paramétereinek az ismeretében:

$$-\log_2\left[\min_x P_{Y|X}(0 \mid x)\right] = -\log_2\left[\min_x P_{Y|X}(1 \mid x)\right] = -\log_2(0.02) = 5.64, \tag{7.23}$$

$$-\log_2\left[\min_x P_{Y|X}(\Delta \mid x)\right] = -\log_2(0.07) = 3.84, \tag{7.24}$$

ezért

$$f(\Delta) = -\log_2\left[\min_x P_{Y|X}(\Delta \mid x)\right] = 3.84$$

$$f(0) = f(1) = -\log_2\left[\min_x P_{Y|X}(0 \mid x)\right] = -\log_2(0.02) = 5.64, \tag{7.25}$$

és

$$-\log_2 P_{Y|X}(0 \mid 0) = -\log_2 P_{Y|X}(1 \mid 1) = -\log_2(0.91) = 0.14 \tag{7.26}$$

aminek az alapján a

$$\log_2 P_{Y|X}(y \mid x) + f(y) \tag{7.27}$$

függvény értékeit különböző x és y esetében ki tudjuk számolni. A függvény értékeit a 7.8. ábra táblázata tartalmazza. Jól látható, hogy a táblázat minden sorában van legalább egy 0 érték, vagyis az ágsúlyok minimális értéke bármely y esetén biztosan 0.

Válasszunk ezután egy tetszőleges $\alpha > 0$ normalizáló paramétert, ami legyen $\alpha = (5.5)^{-1}$, ekkor a Viterbi-metrika $\mu_n(x,y)$ ágsúly függvénye a

$$\mu_n(x,y) = \alpha\left[\log_2 P_{Y|X}(y \mid x) + f(y)\right] \tag{7.28}$$

összefüggés alapján számítható. A függvény értékeit a 7.9. ábra táblázatában tüntettük fel. Érdekes megfigyelni, hogy a metrika "véletlenül" most is a Hamming-egybeesések számával egyenlő. Fontos azonban tudni, hogy általános esetben a metrika nincsen kapcsolatban a Hamming-távolsággal.

Rajzoljuk fel ezután a kódoló trellis-ét (lásd a a 7.10. ábrát), és alkalmazzuk a Viterbi-algoritmust akkor, ha a vett jelek sorozata

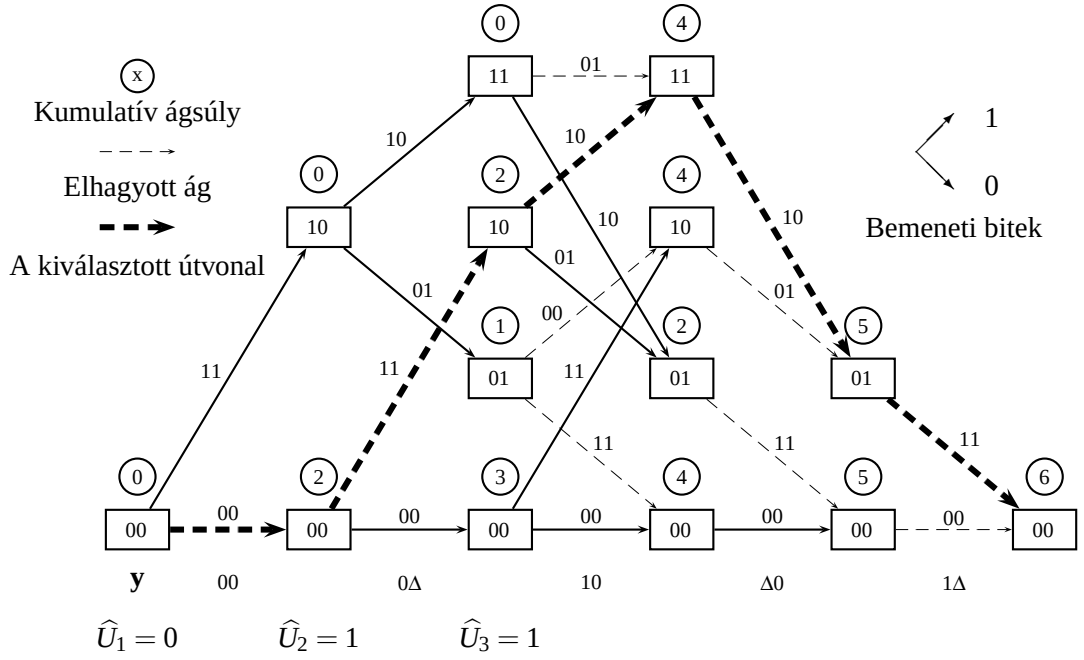
$$\mathbf{y} = [y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}] = [0\ 0\ 0\ \Delta\ 1\ 0\ \Delta\ 0\ 1\ \Delta]. \tag{7.29}$$

y \ x	0	1
0	5.5	0
Δ	0	0
1	0	5.5

7.8. ábra. A példabeli bináris szimmetrikus törléses csatorna Viterbi-metrikája normalizálás előtt

y \ x	0	1
0	1	0
Δ	0	0
1	0	1

7.9. ábra. A példabeli bináris szimmetrikus törléses csatorna Viterbi-metrikája normalizálás után



7.10. ábra. A Viterbi-algoritmus illusztrálása a példaként vizsgált bináris kódoló esetén törléses szimmetrikus csatornában, ha a vett jelsorozat $\mathbf{y} = \{0,0,0,\Delta,1,0,\Delta,0,1,\Delta\}$

A kumulatív metrika értékeinek a kiszámítása és az elhagyott ágak megjelölése után a trellis végétől a megmaradó ágakon visszafelé haladva ismét kijelölhető az az út, amelyhez a maximális kumulatív metrika, azaz az optimális dekódolt sorozat tartozik. Ennek alapján az $\left[\widehat{U}_1 = 0, \widehat{U}_2 = 1, \widehat{U}_3 = 1\right]$ optimális dekódolt sorozatot kapjuk. Az ábrán az elhagyott ágakat vékony, a kiválasztott utat vastag szaggatott vonal, a megmaradt ágakat pedig folytonos vonal jelöli.

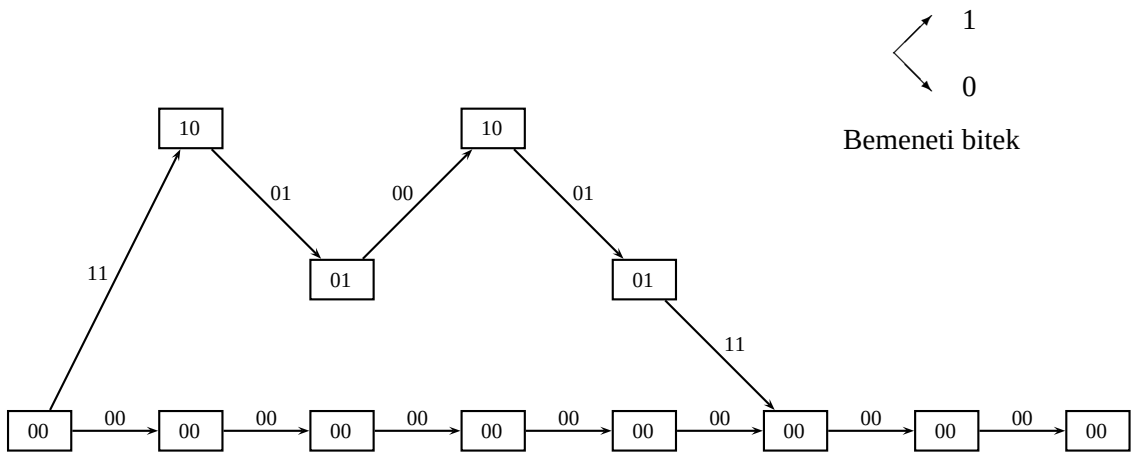
A trellis részletes vizsgálatából megállapítható, hogy a harmadik időrés végén lévő $[01]$ állapot kumulatív metrikája 2 értékű, de ugyanezt az értéket kapjuk akkor is, ha a 0 kumulatív metrikájú $[11]$ állapotból a 2 ágsúlyú $[11]-[01]$ ágon keresztül, vagy a 2 kumulatív metrikájú $[10]$ állapotból a 0 ágsúlyú $[10]-[01]$ ágon keresztül jutunk el a $[01]$ állapotba. Ilyenkor mindkét utat meg kell tartani, és ha dekódoláskor a megmaradó utak a harmadik időrés végén érintenék a $[01]$ állapotot, akkor a megmaradó utak közül sorsolással kellene az optimális utat kiválasztani. A mi konkrét feladatunknál a trellis végétől visszafelé haladva a megmaradó utak elkerülik a hermadik időrés végén lévő $[01]$ állapotot, ezért ezzel a kérdéssel nem kellett foglalkoznunk.

7.2. A Viterbi-dekóder hibavizsgálata, a kitérők számának meghatározása

A Viterbi féle dekódolási algoritmus ismertetése után ebben a fejezetben az a célunk, hogy szoros felső becslést adjunk a rendszer bithibaarányára. A vizsgálatot ismét a példaképpen választott konvolúciós kódoló esetében végezzük el, és feltételezzük, hogy a csatorna diszkrét és memóriamentes. A hibabecslés kulcskérdése az úgynevezett kitérők fogalmának a bevezetése és a kitérők számának a meghatározása.

Tételezzük fel, hogy a vizsgált bináris $R_t = 1/2$ kódolási arányú konvolúciós kódoló bemenetére csupa 0 értékű üzenet érkezik, azaz $U_1 = 0, U_2 = 0, ..., U_i = 0, ...$ Ekkor nyilvánvaló, hogy a kódoló mindig a $\sigma = [0,0]$ állapotban marad, és a kódoló kimenetén is csupa nulla kódolt információ jelenik meg. Mindez azt jelenti, hogy hibamentes átvitel esetén a dekódolóban is a csupa nulla értékekhez tartozó útvonalon kell haladni a trellis bemenetétől a kimenetéig.

Ha a csatornában hiba lép fel, akkor a dekódoló - optimális döntési algoritmus esetén is - a helyes



7.11. ábra. A kitérők szerkezete $d = 6$ és $i = 2$ esetén

útvonal helyett hibás utat választhat, azaz az eredeti csupa nulla kódolt csatornabitet tartalmazó útvonal helyett egy "kitérőre" tér, és a kitérőhöz természetesen hibásan dekódolt $\widehat{U}_1, \widehat{U}_2, ..., \widehat{U}_i, ...$ információs bitek tartoznak. Minden kitérő a $\sigma = [0,0]$ állapotból indul, és oda tér vissza, tehát egy kitérő a trellis egy adott időrésében indul, és egy másik későbbi időrésben végződik (lásd a 7.11. ábrát). Emellett minden kitérőhöz két jellemző paraméter rendelhető:

- d a kitérő mentén mérhető nullától különböző csatornabitek, dekódolt bináris csatornaszimbólumok száma, és
- i a kitérő mentén mérhető nullától különböző információs bitek, dekódolt bináris üzenetszimbólumok száma.

Ábránkon egy olyan lehetséges kitérőt ábrázoltunk, amelynél $d = 6$ és $i = 2$.

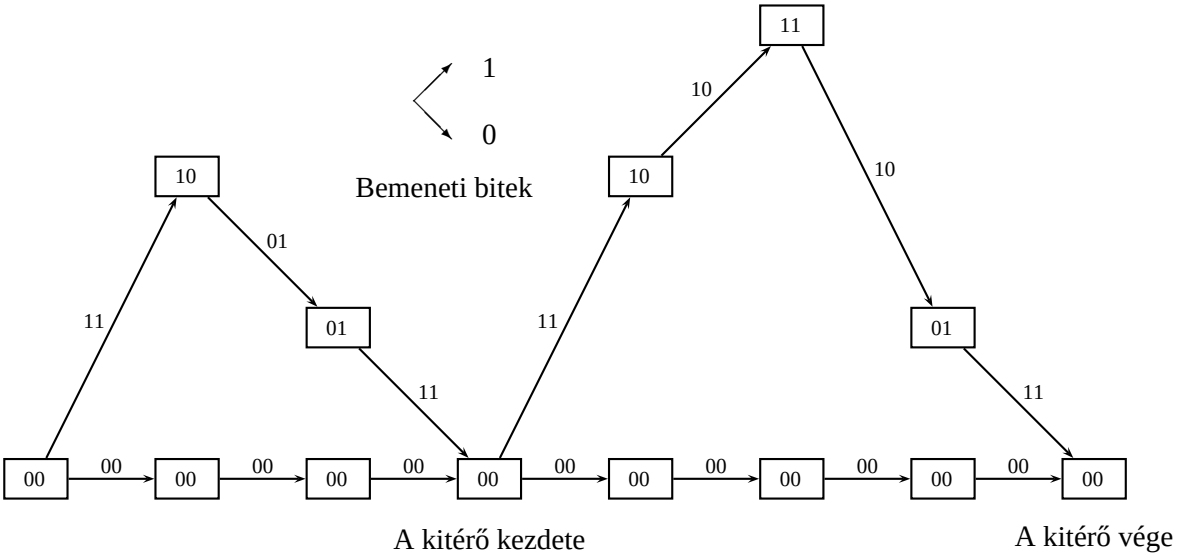
Természetesen a kitérők - az indulási pont és az érkezési pont függvényében - különbözőek lehetnek, sőt az is lehetséges, hogy két különböző kitétőnek azonosak a d, i paraméterei. Ezt illusztráltuk a 7.12. ábrán, ahol egy $d = 5, i = 1$, és egy - a 7.11 ábrán bemutatottól eltérő - $d = 6, i = 2$ paraméterű kitérőt ábrázoltunk.

A következőkben azt tűzzük ki célul, hogy meghatározzuk az adott d, i paraméterekkel rendelkező kitérők számát, vagyis megadjuk azt a $a(d,i)$ mennyiséget, amely azt határozza meg, hogy hány olyan - tetszőleges hosszúságú - kitérő van, amelynek mindegyike a trellis egy adott j-dik időrésében indul, és éppen d számú csatornabitben, valamint i számú információs bitben különbözik a csupa nullákat tartalmazó eredeti helyes úttól.

Mielőtt ezt a számolást elkezdenénk megjegyezzük, hogy eddig referenciakódnak a csupa nulla kódot választottuk, amiből valaki jogosan arra következtethet, hogy eredményeink csak erre az egyedi esetre lesznek érvényesek. Ez konvolúciós kódolók esetében szerencsére nem áll fent, ami azt jelenti, hogy vizsgálatunk bármilyen bemeneti információs bitsorozat esetén azonos eredményre vezetne. A konvolúciós kódolók "linearitása" miatt ugyanis a kitérők száma a bemeneti információs bitek tényleges értékeitől független. A konvolúciós kódolók linearitásának a kérdésére a későbbiekben még visszatérünk.

Adjuk meg eztán a $a(d,i)$ függvény pontos definícióját.

Definíció



7.12. ábra. A kitérők szerkezete $d = 5$, $i = 1$, és $d = 6$, $i = 2$ esetén

Az $a(d,i)$ függvény megadja azoknak a d,i paraméterű kitérőknek a számát, amelyek az első időrésben indulnak, és a helyes úttól éppen d számú csatornabitben és i számú információs bitben különböznek abban az esetben, ha a konvolúciós kódoló bemenetén lévő információs bitek száma $L_t \to \infty$, azaz a kódoló folyamatosan működik.

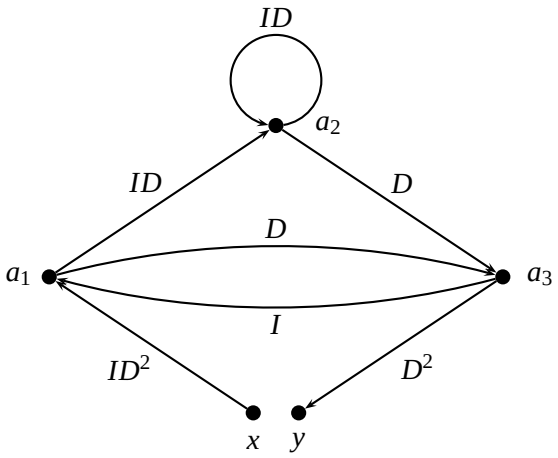
A $a(d,i)$ függvény kiszámításához alkalmazzunk egy egyszerű, de igen hatásos "trükköt". Térjük vissza a 7.4. ábrán megadott állapotátmenet diagramhoz, és képzeljük el a következőket:

- Vágjuk fel az állapotátmenet diagramot a $\sigma = [0,0]$ állapotnál, és hozzunk létre egy virtuális be- és kimenetet (lásd a 7.13. ábrát). A gondolat lényege az, hogy minden kitérő ebből az állapotból indul, és biztosan ebbe az állapotba tér vissza, tehát, ha tudunk valamit a bemenet és kimenet között értelmezett "átviteli függvényről", akkor módunkban áll ismereteket szerezni a kitérők számáról. Ehhez az ágakhoz rendelt "átviteli függvényt" ügyesen kell megválasztani.

- Az "átviteli függvény" megválasztásához példaképpen induljunk ki a $\sigma = [0,0]$ állapotból, mivel minden kitérő ebből az állapotból indul, és lépjünk át a $\sigma = [1,0]$ állapotba. Számoljuk meg az ehhez az ághoz tartozó nullától különböző csatornaszimbólumok és információs szimbólumok számát. Rendeljünk ehhez az átmenethez egy speciális kétváltozós "átviteli függvényt", amelynek a független változóit D-vel és I-vel jelöljük, és amelynél az adott ághoz tartozó nullától különböző csatornaszimbólumok számát a D kitevőjében, az adott ághoz tartozó nullától különböző információs szimbólumok számát pedig az I kitevőjében helyezzük el. A szimbólumok számának a kitevőbe helyezése azért praktikus, mert tudjuk, hogy a "sorba kapcsolt" ágak "átviteli függvényei" összeszorzódnak, így a kitevőben lévő szimbólumok száma összeadódik, számunkra pedig az ágmetrikák összege adja a kiválasztott út eredő metrikáját, ami szerint a trellis-ben az optimális utat ki kell választani.

- Rendeljünk ezután az állapotátmenet diagram minden csomópontjához egy "jelet" (az ábrán az a_1, a_2 és a_3 értékeket), és jelöljük a "felvágott" állapotátmenet diagram bemenő jelét x-szel, a kimenő jelét pedig y-nal.

- Határozzuk meg ezután az x és y változók közötti $T(D,I)$ átviteli függvényt a klasszikus lineáris hálózati leíró módszerek segítségével.



7.13. ábra. A négy belső állapotú konvolúciós kódoló kitérőinek a folyamatgráfja

A fenti műveletek az alábbi lineáris egyenletrendszerhez vezetnek:

$$\begin{aligned} a_1 &= xID^2 + a_3 I, \\ a_2 &= a_1 ID + a_2 ID, \\ a_3 &= a_2 D + a_1 D \\ y &= a_3 D^2 \end{aligned} \quad . \tag{7.30}$$

Egyszerű átalakítások után a fenti egyenletrendszer megoldásával a

$$T(D,I) = \frac{ID^5}{1-2ID} \tag{7.31}$$

átviteli függvényhez jutunk.

A kitérők számának meghatározásához állítsuk elő a $T(D,I)$ átviteli függvény kétdimenziós Taylor-sorát

$$T(D,I) = \sum_{i=1}^{\infty} \sum_{d=1}^{\infty} a(d,i) D^d I^i, \tag{7.32}$$

ami esetünkben a

$$T(D,I) = ID^5(1 + 2ID + 4I^2D^2 + ... + 2^k I^k D^k + ...) \tag{7.33}$$

alakban írható fel, amiből

$$a(i,d) = \begin{cases} 2^{i-1}, & d = i+4, \;\; i = 1,2,3,... \\ 0, & \texttt{egyébként} \end{cases} \quad . \tag{7.34}$$

Ez eredmény igen érdekes, mivel jól látható, hogy a konvolúciós kódoló kötött kódolási szabályai miatt csak olyan kitérőket lehet választani, amelyekben a hibás csatornaszimbólumok száma éppen 4-gyel nagyobb a hibás információs bitek számánál, és a d és i paraméterekkel rendelkező különböző kitérők száma $a(i,d) = 2^{i-1}$.

Térjünk vissza ezután arra a kérdésre, hogy a kitérők száma, $a(i,d)$ nem függ az aktuálisan átvitt információs szimbólumok értékétől. Ehhez azt kell bizonyítani, hogy a kódoló "lineáris". A bizonyításhoz jelöljük a bemeneti szimbólumsorozatot **u**-val, és a hozzá tartozó kódolt jeleket a $g(\mathbf{u})$ függvénnyel. A konvolúciós kódolóban lévő moduló-2 összeadók miatt egyszerűen belátható, hogy

$$g(\mathbf{u} \oplus \mathbf{u}') = g(\mathbf{u}) \oplus g(\mathbf{u}'), \tag{7.35}$$

azaz a két bemeneti bitsorozat moduló-2 összegéhez tartozó kód azonos a két bemeneti bitsorozathoz tartozó kódok moduló-2 összegével. Ebből egyenesen következik, hogy $g(\mathbf{u}) \oplus g(\mathbf{u}')$ maga is kódszó, mivel $\mathbf{u} \oplus \mathbf{u}'$ egy lehetséges bemeneti bitsorozat.

Emellett azt is tudjuk, hogy két tetszőleges $\mathbf{x}$ és $\mathbf{y}$ bináris sorozat Hamming-távolsága $d(\mathbf{x},\mathbf{y})$ nem változik akkor, ha a sorozatokhoz egy harmadik $\mathbf{z}$ bináris sorozatot moduló-2 hozzáadunk, azaz

$$d(\mathbf{x},\mathbf{y}) = d(\mathbf{x} \oplus \mathbf{z}, \mathbf{y} \oplus \mathbf{z}). \tag{7.36}$$

Ebből nyilvánvaló, hogy

$$d(g(\mathbf{u}), g(\mathbf{u}')) = d(g(\mathbf{u}) \oplus g(\mathbf{u}), g(\mathbf{u}') \oplus g(\mathbf{u})) = d(\mathbf{0}, g(\mathbf{u} \oplus \mathbf{u}')), \tag{7.37}$$

vagyis a $g(\mathbf{u})$ és $g(\mathbf{u}')$ kódszavak Hamming-távolsága ugyanolyan, mint a $g(\mathbf{u} \oplus \mathbf{u}')$ kódszó Hamming-távolsága a $\mathbf{0}$ kódszótól. Ebből az következik, hogy bármely bemeneti információs sorozatot választhatjuk referenciasorozatnak, a kódszavak Hamming-távolságától függő $a(i,d)$ függvény ettől a választástól független lesz.

7.3. A Viterbi-dekóder hibavizsgálata, a bithibaarány felső korlátjának meghatározása

Ebben a fejezetben az a célunk, hogy a Viterbi-dekóder hibaarányára szoros felső korlátot adjunk a Bhattacharyya-korlát felhasználásával. A korábbi fejezetekből tudjuk, hogy diszkrét memóriamentes csatornában a blokkhibaarány felső korlátja legrosszabb esetben a

$$(P_B)_{wc} \leq \prod_{n=1}^{N} \sum_{y} \sqrt{P_{Y|X}(y \mid x_{1n}) P_{Y|X}(y \mid x_{2n})} \tag{7.38}$$

kifejezéssel határozható meg.

Emellett a kifejezés jobb oldalán lévő összeg

$$\sum_{y} \sqrt{P_{Y|X}(y \mid x_{1n}) P_{Y|X}(y \mid x_{2n})} = \begin{cases} 1, & \texttt{ha } x_{1n} = x_{2n} \\ 2^{-D_B}, & \texttt{ha } x_{1n} \neq x_{2n} \end{cases}, \tag{7.39}$$

ahol D_B a csatorna Bhattacharyya-távolsága.

A fenti egyenletből következik, hogy a blokkhibaarány felső korlátja legrosszabb esetben a

$$(P_B)_{wc} \leq \left(2^{-D_B}\right)^{d(\mathbf{x}_1, \mathbf{x}_2)} \tag{7.40}$$

kifejezés alapján az $\mathbf{x}_1$ és $\mathbf{x}_2$ kódsorozatok Hamming-távolságától függ.

Az átlagos bithibaarány egy K információs bitből álló bemeneti információsorozat esetén a

$$P_b = \frac{1}{K} \sum_{i=1}^{K} P_{e,i} \tag{7.41}$$

egyenlőség alapján határozható meg, ahol $P_{e,i}$ annak a valószínűsége, hogy a K elemű sorozat i-dik bitje meghibásodik. Jelöljük V_i-vel ennek az eseménynek az indikátor valószínűségi változóját, azaz

$$V_i = \begin{cases} 1, & \texttt{ha az } i\texttt{-dik bit meghibásodik} \\ 0, & \texttt{ha az } i\texttt{-dik bit nem hibásodik meg} \end{cases}, \tag{7.42}$$

vagyis

$$\begin{aligned} &\Pr(V_i = 1) = P_{e,i} && \texttt{és} \\ &\mathbf{E}[V_i] = 1 \times P_{e,i} + 0 \times (1 - P_{e,i}) = P_{e,i}. \end{aligned} \tag{7.43}$$

Ezt felhasználva az átlagos bithibaarány a

$$P_b = \frac{1}{K}\sum_{i=1}^{K}\mathbf{E}[V_i] = \mathbf{E}\left[\frac{\sum_{i=1}^{K}V_i}{K}\right] \tag{7.44}$$

egyenlőség alapján határozható meg, ahol $\sum_{i=1}^{K}V_i$ kódsorozat átvitele során keletkező információs bithibák számával azonos valószínűségi változó.

Jelöljük ezután W_j-vel az L_t+T hosszúságú trellis j-dik időrésében induló kitérőhöz tartozó információs bithibák számát, amiből az átlagos bithibaarány a

$$P_b \leq \mathbf{E}\left[\frac{\sum_{j=1}^{L_t}W_j}{k_0 L_t}\right] \tag{7.45}$$

képlet segítségével határozható meg, ahol k_0 az információs bitek száma a trellis egy időrésében (illusztratív példánkbam ez az érték 1). A kifejezés csak azt mondja ki, hogy a trellis különböző időréseiben induló kitérőkhöz tartozó összes bithiba relatív gyakoriságának a várható értéke azonos a hibavalószínűséggel, ami a nagy számok gyenge törvényéből egyenesen következik. A felső korlát abból adódik, hogy a különböző időrésekben induló kitérők átfedésben lehetnek egymással, ezért a keletkező hibákat többszörösen vehetjük figyelembe.

Ezután egyetlen feladatunk maradt: meg kell határoznunk a $\mathbf{E}[W_j]$ értékét, illetve erre az értékre szoros felső becslést kell adnunk. Ehhez vezessük be a B_{kj} esemény fogalmát. A B_{kj} esemény akkor következik be, ha a dekódolás során a dekóder a j időrésben induló kitérők közül éppen a k-dikat választja, ahol k a kitérők egyszerű sorszáma. Ha a k-dik kitérőhöz éppen a d_k és i_k paraméterek tartoznak, akkor a B_{kj} esemény valószínűsége a korábbi eredmények felhasználásával a

$$\Pr(B_{kj}) \leq \left(2^{-D_B}\right)^{d_k} \tag{7.46}$$

kifejezéssel felülről becsülhető.

Mivel i_k a k-dik kitérőhöz tartozó információs bithibák száma, ezért

$$W_j = \begin{cases} i_k & \texttt{ha } B_{kj} \texttt{ bekövetkezik,} \\ 0, & \texttt{ha } B_{kj} \texttt{ nem kövekezik be} \end{cases}. \tag{7.47}$$

A fenti összefüggések alapján a felső becslés a

$$\mathbf{E}[W_j] = \sum_k i_k \Pr(B_{kj}) \leq \sum_k i_k \left(2^{-D_B}\right)^{d_k} = \sum_i \sum_d i a_j(d,i)\left(2^{-D_B}\right)^d \tag{7.48}$$

kifejezés segítségével határozható meg, mivel az összegzés argumentuma csak az i és d paraméterektől függ. Érdemes felhívni a figyelmet arra, hogy ez a felső korlát függ a j értékétől is, vagyis attól, hogy a vizsgált kitérők a trellis melyik időrésében indulnak el. Nyilvánvaló azonban, hogy folytonos működés esetén, amikor L_t tart a végtelenhez, tehát a trellis hossza minden határon túl növekszik, a kitérők struktúrája már függetlenné válik az indulás helyétől, továbbá az is igaz, hogy végtelen hosszúságú trellis esetén a kitérők száma biztosan nagyobb mint véges trellis esetén, azaz

$$a_j(d,i) \leq a(d,i), \tag{7.49}$$

ahol $a(d,i)$ a d,i paraméterű kitérők száma a végtelen hosszúságú trellis-ben.

Ennek alapján az átlagos bithibaarány felső korlátja a

$$P_b \leq \frac{1}{k_0}\sum_i \sum_d i a(d,i)\left(2^{-D_B}\right)^d \tag{7.50}$$

kifejezéssel adható meg. A korábbi egyenlőtlenségben szereplő j szerinti összegzés és az L_t-vel való osztás azért tűnt el, mert a W_j várható értékének a felső korlátja végtelen trellis-t feltételezve függetlenné vált j-től, a kitérők indulási pozíciójától. Ily módon a felső korlát számításakor ugyanazt a mennyiséget L_t-szer össze kellett adni, és ezután ezt az összeget L_t-vel kellett osztani.

Felhasználva a korábban definiált $T(D,I)$ "átviteli függvényt", egyszerűen belátható, hogy

$$\frac{\partial T(D,I)}{\partial I} = \sum_i \sum_d i a(d,i) I^{i-1} D^d, \tag{7.51}$$

ezért a bithibaarány felső korlátja a

$$P_b \leq \frac{1}{k_0} \frac{\partial T(D,I)}{\partial I} \Big|_{I=1, D=2^{-D_B}} . \tag{7.52}$$

kifejezés segítségével határozható meg.

Példa

Számítsuk ki az eddig vizsgált konvolúciós kódoló bithibaarányának felső korlátját abban az esetben, ha a rendszer bináris törléses csatornában működik, és a dekódolást a Viterbi-algoritmussal végezzük el. Esetünkben a kódoló állapotátmenet diagramjához rendelt "átviteli függvény"

$$T(D,I) = \frac{ID^5}{1-2ID}, \tag{7.53}$$

amiből az "átviteli függvény" I szerinti parciális deriváltja

$$\frac{\partial T(D,I)}{\partial I} = \frac{D^5}{(1-2ID)^2}. \tag{7.54}$$

Korábbi példákból ismert, hogy a bináris törléses csatorna Bhattacharyya-távolsága

$$D_B = -\log_2 \delta, \tag{7.55}$$

ezért

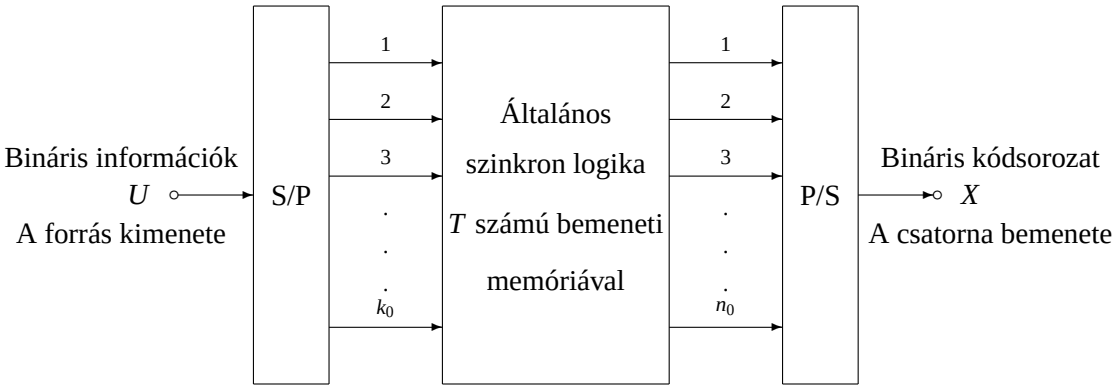
$$2^{-D_B} = \delta. \tag{7.56}$$

Ezt az értéket behelyettesítve a P_b felső korlátjának a kifejezésébe a

$$P_b \leq \frac{\delta^5}{(1-2\delta)^2} \tag{7.57}$$

végeredményhez jutunk. Ha például $\delta = 0.1$, akkor a bithibaarány felső korlátja $P_b \leq 1.56 \times 10^{-5}$, vagyis a konvolúciós kódoló jelentős hibajavító képességgel rendelkezik.

Fontos megjegyezni azt, hogy a Viterbi-algoritmus végrehajtásakor a trellis úgynevezett megmaradó ágait meg kell őrizni az optimális dekódolás érdekében. Éppen ezért kritikus kérdés az, hogy az ágakat tároló memóriának milyen kapacitásúnak kell lenni, vagyis milyen mennyiségű adatot kell egy tényleges megvalósítás esetén tárolni. Szimulációs eredmények igazolták, hogy a P_b átlagos hibaarány már lényegesen nem csökken akkor, ha az úgynevezett döntési késleltetés eléri a kényszertávolság ötszörösét. Ez azt jelenti, hogy az aktuális időrésből ilyen távolságra visszatekintve már majdnem biztos, hogy a megmaradó utak ugyanarra az ágra mutatnak a korábbi időrésben, ezért az algoritmust viszonylag egyszerű eszközökkel hatékonyan meg lehet valósítani.



7.14. ábra. A konvolúciós kódolók általános felépítése

7.4. Véletlen kódolás trellis kód esetén, a Viterbi-exponens számítása

Ebben a fejezetben az a célunk, hogy kiterjesszük a véletlen kódolás elméletét a konvolúciós kódolók esetére is, és megmutassuk, hogy a konvolúciós kódolók minőségi paraméterei lényegesen felülmúlják a hagyományos blokk kódolókét.

A konvolúciós kódolók általános felépítése a 7.14. ábrán látható. A forrás bináris információsorozata egy soros-párhuzamos átalakítóra kerül, amely időrésenként egy-egy k_0 bites szimbólumot juttat a kódoló bemenetére. A konvolúciós kódoló ezekből a szimbólumokból T számút tárol a memóriájában, és lineáris műveletekkel (bináris esetben modoló-2 összeadásokkal) minden időrésben egy-egy n_0 bites kimeneti szimbólumot állít elő, amely egy párhuzamos-soros átalakítóra kerül, ami előállítja a csatorna bemenetére jutó bináris kódsorozatot.

A további vizsgálatok előtt vezessük be az alábbi jelöléseket. Legyen:

- k_0 az egy időrésben található bemeneti információs bitek száma,
- n_0 az egy időrésben előállított csatornabitek (kódbitek) száma,
- $\mathbf{U}_i = [U_{(i-1)k_0+1}, U_{(i-1)k_0+2}, ..., U_{ik_0}]$ a kódoló i-dik bemeneti k_0 bites szimbóluma,
- $\mathbf{X}_i = [X_{(i-1)n_0+1}, X_{(i-1)n_0+2}, ..., X_{in_0}]$ a kódoló i-dik kimeneti n_0 bites szimbóluma,
- $\mathbf{X}_i = f_i(\mathbf{U}_i, \mathbf{U}_{i-1}, ..., \mathbf{U}_{i-T})$ a kódolási függvény, ami megadja a kódgenerálás szabályát, vagyis a kódoló kimeneti sorozatának a függését az aktuális bemeneti $\mathbf{U}_i$ szimbólumtól, és a memóriában tárolt $\mathbf{U}_{i-1}, ..., \mathbf{U}_{i-T}$ korábbi szimbólumoktól,
- $\sigma_i = [\mathbf{U}_{i-1}, ..., \mathbf{U}_{i-T}]$ a kódoló állapota, amit felhasználva

$$\mathbf{X}_i = f_i(\mathbf{U}_i, \sigma_i). \tag{7.58}$$

A korábbi reprezentatív példa alapján meghatározhatjuk az általános konvolúciós kódoló legfontosabb paramétereit, ha feltételezzük, hogy a bemeneti sorozat L_t értékes szimbólumból és T számú $\mathbf{0}$ szimbólumból áll, azaz a bemenetre az $\mathbf{U}_1, \mathbf{U}_2, ..., \mathbf{U}_{L_t}, \mathbf{0}_{(1)}, \mathbf{0}_{(2)}, ..., \mathbf{0}_{(T)}$ sorozat érkezik:

- A konvolúciós kódoló kódolási aránya $R_t = k_0/n_0$ $\left[\frac{\texttt{bit}}{\texttt{csatornaigénybevétel}}\right]$,
- A kódoló állapotainak a száma $2^{k_0 T}$,

- Az $(L_t,\ T,\ k_0,\ n_0)$ paraméterekkel rendelkező konvolúciós kódoló kódszavainak a száma $M = 2^{k_0 L_t} = 2^{n_0 R_t L_t}$,
- A kódoló által előállított kódszavak hossza $N = (L_t + T)n_0$,
- A blokk kódoló kódolási aránya $R = \frac{L_t}{L_t+T} R_t$,
- A kódoló kezdeti σ_1 és végső σ_{L_t+T+1} állapota nulla értékű.

A kódoló trellis-én a bemenet és a kimenet között pontosan M különböző út található, és a dekódolás során a Viterbi-algoritmus segítségével ezek közül az utak közül kell az optimális metrikájú utat kiválasztani. A trellis felépítése csak az $(L_t,\ T,\ k_0)$ paraméterektől függ, tehát független n_0-tól.

Segédtétel

Az $(L_t,\ T,\ k_0)$ paraméterekkel rendelkező trellis-en a j-dik időrésben induló, és a $j+l$-dik időrésben végződő kitérők száma, $b(j,l)$ független a referencia út megválasztásától, azaz az L_t számú értékes üzenetszimbólum értékétől, és a kitérők számát a

$$b(j,l) \begin{cases} = 0, & \texttt{ha } l \le T \\ \le (2^{k_0}-1)2^{k_0(l-T-1)}, & \texttt{ha } l > T \end{cases} \tag{7.59}$$

kifejezés adja meg.

Bizonyítás

A segédtétel az alábbi lépésekkel igazolható:

- A trellis minden állapotából 2^{k_0} számú ág indul el, mivel a kódoló bemenetére érkező k_0 bites $\mathbf{U}$ szimbólumok ennyi különböző értéket vehetnek fel. Éppen ezért a j-dik időrésben, a kitérő indulási helyén a lehetséges elágazások száma $(2^{k_0}-1)$, mivel az összes elágazások közül az egyik a helyes úthoz tartozik.
- A $j+l$-dik időrésben minden kitérő visszajut a helyes útra, ami azt jelenti, hogy a kódoló σ_{j+l} állapota a helyes úthoz tartozó állapottal lesz azonos. Ezt az állapotot a $j+l$-dik időrés előtti T számú $[\mathbf{U}_{j+l-1}, \mathbf{U}_{j+l-2}, ..., \mathbf{U}_{j+l-T}]$ bemeneti szimbólum határozza meg, ami azt jelenti, hogy a j-dik időrésben induló összes kitérőben az utolsó T szimbólumnak azonosnak kell lenni. Így az összes kitérő utolsó T időrésében minden állapotból csak egyetlen - minden kitérőben azonos szimbólumoz tartozó - elágazás indulhat el. Ebből a meggondolásból egyenesen következik, hogy olyan kitérő nem lehet, amelyben $l \le T$.
- A fentiek alapján az első időrésben az elágazások száma $(2^{k_0}-1)$, és az azt követő $l-T-1$ időrésben pedig időrésenként 2^{k_0}, mivel ezeket az elágazásokat az $[\mathbf{U}_{j+1}, \mathbf{U}_{j+2}, ..., \mathbf{U}_{j+l-T-1}]$ bemeneti szimbólumok határozzák meg. A lehetséges kitérők száma így maximálisan $(2^{k_0}-1)2^{k_0(l-T-1)}$ lehet. Azért maximálisan, mert a fenti számítás csak akkor érvényes, ha a trellis hossza nagyobb, mint $j+l$. Ha ez nem áll fent, akkor a kitérők száma ennél az értéknél kisebb.

Ezzel a segédtételt bebizonyítottuk.

Ezután foglalkozzunk az $\mathbf{X}_i = f_i(\mathbf{U}_i, \sigma_i)$ kódolási függvénnyel, ami nem jelent mást, mint azt, hogy a konvolúciós kódoló szabályainak megfelelően el kell helyezni az $(L_t,\ T,\ k_0)$ paraméterű trellis egyes ágain n_0 csatornabitet (kódbitet).

A véletlen kódolás most is annyit jelent, hogy trellis bármely adott útján az $\mathbf{X}$ kódszó azonos sorsolási valószínűséggel jelenik meg, és

$$Q_{\mathbf{X}}(x_1, x_2, ..., x_N) = \prod_{n=1}^{N} Q_X(x_n), \quad N = (L_t + T)n_0. \tag{7.60}$$

A kódok páronként függetlenek egymástól abban az értelemben, hogy bármilyen helyes út és bármilyen a j időrésben induló és a $j+l$, $l>T$ időrésben végződő kitérő esetén a kitérőhöz, és az érintett időrésben a helyes úthoz tartozó kódszavak azonos statisztikájúak és függetlenek, mivel minden szimbólumukat egymástól függetlenül választottuk meg a $Q_X(x)$ sorsolási valószínűségi eloszlás szerint.

A bithibavalószínűség felső korlátjának a számítása

Célunk az, hogy meghatározzuk az $\mathbf{E}[P_b]$ átlagos bithibavalószínűség felső korlátját trellis kód és Viterbi-dekódolás esetén.

Jelöljük E_{jl}-lel azt az eseményt, hogy a maximum likelihood dekóder a trellis-ben a helyes út helyett éppen a egyik j-dik időrésben induló és $j+l$-dik $(l>T)$ időrésben végződő kitérőt választotta, azaz biztosan hibát követett el. Ez annyit jelent, hogy egyet kiválasztott a $b(j,l)$ számú ilyen kitérő közül.

Felhasználva a 6.119. egyenletben megadott Gallager-korlátot ki tudjuk számolni az E_{jl} esemény valószínűségének felső korlátját az alábbi kifejezéssel

$$\mathbf{E}[\Pr(E_{jl})] \le (M^*-1)^{\rho} 2^{-N^* E_0(\rho,Q)}; \quad 0 \le \rho \le 1, \tag{7.61}$$

ahol (M^*-1) a lehetséges hibás "üzenetek" száma, vagyis a j-dik időrésben induló és a $j+l$-dik $(j>T)$ időrésben végződő összes lehetséges kitérők száma, N^* az ehhez a szakaszhoz tartozó "kódszavak hossza", $E_0(\rho,Q)$ a 6.118. egyenletben megadott Gallager-függvény és Q a kódszimbólumok sorsolási valószínűségi eloszlása.

Mivel a korábbiakból tudjuk, hogy $(M^*-1)=b(j,l)$ és $N^*=ln_0$, a kifejezés a

$$\mathbf{E}[\Pr(E_{jl})] \le (b(j,l))^{\rho} 2^{-ln_0 E_0(\rho,Q)}; \quad 0 \le \rho \le 1. \tag{7.62}$$

alakba írható át.

Felhasználva ezután a 7.59. egyenletből $b(j,l)$ értékét behelyettesítés után a

$$\mathbf{E}[\Pr(E_{jl})] \le (2^{k_0}-1)^{\rho} 2^{\rho k_0(l-T-1)} 2^{-ln_0 E_0(\rho,Q)} \tag{7.63}$$

kifejezést kapjuk.

Korábban már definiáltuk az N_t úgynevezett kényszertávolságot, ami azoknak a csatornabiteknek (kódbiteknek) a száma, amelyeket egy bemeneti információs bit befolyásol. Esetünkben a kényszertávolság értéke

$$N_t = (T+1)n_0. \tag{7.64}$$

Ezt az értéket felhasználva újraírhatjuk a 7.63. egyenletet, miszerint

$$\mathbf{E}[\Pr(E_{jl})] \le (2^{k_0}-1)^{\rho} 2^{-[n_0 E_0(\rho,Q)-\rho k_0](l-T-1)} 2^{-N_t E_0(\rho,Q)}; \;\; 0 \le \rho \le 1; \;\; l>T, \tag{7.65}$$

és felhasználva a $\left(2^{k_0}-1\right)^{\rho} < 2^{k_0}$ triviális egyenlőtlenséget a

$$\mathbf{E}[\Pr(E_{jl})] < 2^{k_0} 2^{-n_0[E_0(\rho,Q)-\rho R_t](l-T-1)} 2^{-N_t E_0(\rho,Q)}; \;\; 0 \le \rho \le 1; \;\; l>T \tag{7.66}$$

felső korlátot kapjuk.

Határozzuk meg ezután az információs bithibák értékét a maximum likelihood dekóder által kiválasztott kitérő mentén. Jelöljük ezt az értéket W_j-vel, ami egyszerű megfontolásokkal a

$$W_j \begin{cases} \le k_0(l-T), & \texttt{ha az } E_{jl} \texttt{ esemény bekövetkezik, } j>T \\ = 0, & \texttt{ha az } E_{jl} \texttt{ esemény nem következik be} \end{cases}. \tag{7.67}$$

egyenlettel határozható meg.

A következő lépésben megjegyezzük, hogy a 7.67. egyenlet következtében az információs bithibák várható értékének a felső korlátja az összes lehetséges kódot figyelembe véve a

$$\mathbf{E}^*[W_j] = \sum_{l=T+1}^{L_t+T+1-j} \mathbf{E}^*[W_j \mid E_{jl}] \Pr(E_{jl}) \leq \sum_{l=T+1}^{L_t+T+1-j} k_0(l-T) \Pr(E_{jl}) \tag{7.68}$$

egyenlet alapján határozható meg, és a várható érték az összes trellis kódot figyelembe véve a

$$\mathbf{E}[W_j] \leq \sum_{l=T+1}^{L_t+T+1-j} k_0(l-T)\mathbf{E}[\Pr(E_{jl})] \tag{7.69}$$

kifejezéssel számítható.

Felhasználva a 7.66. egyenletet a felső korlátra a

$$\mathbf{E}[W_j] < k_0 2^{k_0} 2^{-N_t E_0(\rho,Q)} \sum_{l=T+1}^{L_t+T+1-j} (l-T) 2^{-n_0[E_0(\rho,Q)-\rho R_t](l-T-1)} =$$

$$= k_0 2^{k_0} 2^{-N_t E_0(\rho,Q)} \sum_{i=0}^{L_t+1-j} i \left\{ 2^{-n_0[E_0(\rho,Q)-\rho R_t]} \right\}^{i-1} \leq$$

$$\leq k_0 2^{k_0} 2^{-N_t E_0(\rho,Q)} \frac{1}{\left(1-2^{-n_0[E_0(\rho,Q)-\rho R_t]}\right)^2}; \quad R_t < \frac{E_0(\rho,Q)}{\rho} \tag{7.70}$$

kifejezés adódik (lásd a Függelék 8.3. fejezetét).

A további számítások egyszerűsítése érdekében vezessük be a

$$c(R_t,\rho,Q) = \frac{2^{k_0}}{\left(1-2^{-n_0[E_0(\rho,Q)-\rho R_t]}\right)^2}; \quad R_t < \frac{E_0(\rho,Q)}{\rho}, \tag{7.71}$$

jelölést, amit felhasználva a felső korlátra a

$$\mathbf{E}[W_j] < k_0 c(R_t,\rho,Q) 2^{-N_t E_0(\rho,Q)}; \quad R_t < \frac{E_0(\rho,Q)}{\rho} \tag{7.72}$$

kifejezést kapjuk.

Természetesen a trellis mentén minden időrésben indulhatnak kitérők, így a 7.45. egyenlethez hasonlóan az átlagos bithibavalószínűséget az

$$\mathbf{E}[P_b] = \frac{1}{k_0 L_t} \sum_{j=1}^{L_t} \mathbf{E}[W_j] \tag{7.73}$$

egyenlőség alapján határozhatjuk meg. Ha a konvolúciós kódoló és a Viterbi-dekóder folyamatosan működik, akkor most is igaz, hogy a kitérők struktúrája nem függ j-től, a kitérők indulási pozíciójától, ezért $\mathbf{E}[W_j] \leq \mathbf{E}[W]$, így

$$\mathbf{E}[P_b] = \frac{1}{k_0 L_t} \sum_{j=1}^{L_t} \mathbf{E}[W_j] \leq \frac{1}{k_0 L_t} \sum_{j=1}^{L_t} \mathbf{E}[W] = \frac{L_t}{k_0 L_t} \mathbf{E}[W] = \frac{1}{k_0} \mathbf{E}[W]. \tag{7.74}$$

7.5. A trellis kódok Viterbi féle véletlen kódolási korlátja

Az előző fejezet vizsgálatai alapján megadhatjuk véletlen kódolás esetére az átlagos bithibaarány Viterbi féle felső korlátját, akkor, ha diszkrét memóriamentes csatornában trellis vagy konvolúciós kódolót és maximum likelihood dekódolót használunk. A korábbi eredmények szerint az átlagos bithibaarány felső korlátja

$$\mathbf{E}[P_b] < c(R_t,\rho,Q)2^{-N_t E_0(\rho,Q)}; \quad 0 \le \rho \le 1, \tag{7.75}$$

és

$$R_t < \frac{E_0(\rho,Q)}{\rho}, \tag{7.76}$$

ahol $E_0(\rho,Q)$ az 6.118. egyenletben definiált Gallager-függvény. Ezen egyenlet alapján a bithibaarány N_t növekedésével exponenciálisan csökken mindaddig, amíg a megadott feltételt figyelembe véve az $E_0(\rho,Q)$ függvény ρ és Q szerinti optimuma pozitív.

Célunk a továbbiakban az, hogy a 7.75. egyenletben ρ és Q szerinti optimalizálás után megtaláljuk adott R_t mellett a legjobb exponenst, és ez alapján összevessük egymással a konvolúciós és a blokk kódolás minőségi paramétereit.

A Függelékben (lásd 8.1. fejezet) részletesen analizáltuk a Gallager-függvény tulajdonságait, és ebből tudjuk, hogy az $E_0(\rho,Q)$ függvény ρ szerint monoton növekszik (lásd a 8.1. ábrát). Ezért adott R_t esetén az optimalizáláskor mindig a lehető legnagyobb ρ értéket kell választani. Ez természetesen a $\rho = 1$ vagy a

$$R_t = \frac{E_0(\rho,Q)}{\rho} \tag{7.77}$$

egyenletet kielégítő érték lehet. Nyilvánvaló, hogy kis R_t esetén az optimális érték mindig $\rho = 1$ lesz, mivel ilyenkor a 7.76. egyenlet biztosan teljesül. Nagyobb R_t-k esetén azonban a 7.77. egyenlet adja meg az exponens optimumához tartozó ρ értékét. Sajnos az $R_t = E_0(\rho,Q)/\rho$ egyenlethez tartozó ρ nem választható, mivel ekkor a 7.70. egyenletben szereplő mértani sor már nem lenne konvergens, vagyis a $c(R_t,\rho,Q)$ függvény minden határon túl növekedne (lásd a Függelék 8.3. fejezetét).

Ezt a problémát a következő ötlettel tudjuk elkerülni. Válasszunk egy tetszőlegesen kicsi ε pozitív számot, és adjunk szigorúbb előírást a 7.77. egyenletnél az alábbiak szerint:

$$R_t \le \frac{E_0(\rho,Q)-\varepsilon}{\rho}; \quad E_0(\rho,Q) - \rho R_t \ge \varepsilon. \tag{7.78}$$

Felhasználva ezt a szigorúbb feltételt

$$c(R_t,\rho,Q) \le \frac{2^{k_0}}{\left(1-2^{-\varepsilon n_0}\right)^2}, \tag{7.79}$$

ami már nem függ ρ-tól és Q-tól. A Gallager-függvény $\rho = 1$-nél veszi fel a maximumát (lásd a 8.1. ábrát), ezért a maximum a 6.125. egyenlet szerint

$$\max_{\rho,Q} E_0(\rho,Q) = \max_{Q} E_0(1,Q) = R_0, \tag{7.80}$$

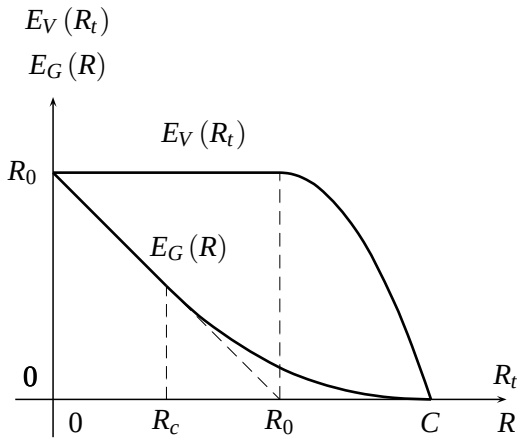
ahol R_0 a csatorna határsebessége. Figyelembe véve a 7.78. egyenletet a legjobb exponens

$$E_t(R_t,\varepsilon) = R_0 \tag{7.81}$$

a teljes $0 \le R_t \le R_0 - \varepsilon$ tartományban.

Ennél nagyobb R_t értékek esetén az $E_t(R_t,\varepsilon)$ értékét az

$$E_t(R_t,\varepsilon) = \max_{Q} E_0(\rho^*,Q), \tag{7.82}$$



7.15. ábra. Az $E_V(R_t)$ Viterbi-exponens és az $E_G(R)$ Gallager-exponens a csatorna átviteli sebességének a függvényében

kifejezés adja meg az $R_0 - \varepsilon < R_t < C - \varepsilon$ tartományban, ahol ρ^* értékét az

$$R_t = \frac{E_0(\rho^*, Q) - \varepsilon}{\rho^*} \tag{7.83}$$

megoldása szolgáltatja, és

$$C = \lim_{\rho \to 0} \frac{E_0(\rho)}{\rho}, \tag{7.84}$$

ahogy ezt korábban megismertük. Emlékeztetőül megjegyezzük, hogy $E_0(\rho, Q)$ kezdeti deriváltja a $\rho = 0$-nál azonos az $I_Q(X;Y)$ kölcsönös információval, aminek a Q szerinti optimuma a csatorna kapacitásával egyenlő (lásd a 8.1. Függeléket).

A trellis kódok Viterbi féle kódolási tétele

Mindezek alapján kimondhatjuk a trellis kódok Viterbi féle kódolási tételét. Ha adott egy tetszőleges $R_t = k_0/n_0$ kódolási arányú és $N_t = (T+1)n_0$ kényszertávolságú trellis kód, amelyet diszkrét memóriamentes csatornában maximum likelihood dekóderrel használunk, és az értékes információs szimbólumok száma, L_t tetszőleges (beleértve az $L_t \to \infty$ esetet is), akkor egy tetszőlegesen kicsi ε pozitív szám mellett és a bemeneti bitek bármilyen valószínűségi eloszlása esetén a rendszer átlagos bithibaaránya kielégíti a

$$\mathbf{E}[P_b] < c_v(\varepsilon) 2^{-N_t E_t(R_t, \varepsilon)} \tag{7.85}$$

egyenlőtlenséget, ahol $E_t(R_t, \varepsilon)$ pozitív az $R_t \leq C - \varepsilon$ tartományban, és

$$c_v(\varepsilon) = 2^{k_0}(1 - 2^{-\varepsilon n_0})^2. \tag{7.86}$$

Mivel a kifejezésben ε tetszőlegesen kicsire választható, a legjobb Viterbi-exponens az

$$E_v(R_t) = \lim_{\varepsilon \to 0} E_t(R_t, \varepsilon) \tag{7.87}$$

határátmenettel számítható.

A Viterbi-exponenst az R_t függvényében a 7.15. ábrán adjuk meg, összehasonlítva azt a Gallager-exponessel. Az ábra alapján kimondhatjuk, hogy a konvolúciós kódok minőségi paraméterei lényegesen felülmúlják a hagyományos blokk kódokét.

8. fejezet

Függelék

8.1. A Gallager-függvény és a Gallager-exponens tulajdonságai

- A korábbiakból tudjuk, hogy $\rho = 1$ esetén a Gallager-korlát azonos a Bhattacharyya-korláttal, ezért, ha az $E_0(\rho, Q)$ Gallager-függvénybe $\rho = 1$-et helyettesítünk, akkor

$$\max_Q E_0(1,Q) = \max_Q \left(-\log_2 \sum_y \left[\sum_x \left(P_{Y|X}(y \mid x) \right)^{\frac{1}{1+\rho}} Q_X(x) \right]^{1+\rho} \Big|_{\rho=1} \right) =$$

$$= \max_Q \left(-\log_2 \sum_y \left[\sum_x \sqrt{P_{Y|X}(y \mid x)} Q_X(x) \right]^2 \right) = R_0, \tag{8.1}$$

tehát

$$\max_Q E_0(\rho, Q) \big|_{\rho=1} = R_0 \,, \tag{8.2}$$

így a ρ szerinti maximumkeresés után biztosan igaz, hogy

$$E_G(R) = \max_Q E_R(R,Q) = \max_Q \max_{0 \le \rho \le 1} [E_0(\rho, Q) - \rho R] \ge R_0 - R = E_B(R), \tag{8.3}$$

ahol $E_B(R)$ a korábban megismert Bhattacharyya-exponens.

- Ebben a pontban megmutatjuk, hogy az $E_0(\rho, Q)$ Gallager-függvény minden pozitív kapacitású csatornában ρ növekedésével a $0 \le \rho \le 1$ tartományban monoton nő.

  Ismert, hogy tetszőleges $P_i,\ \{i = 1, 2, ..., K\}$ diszkrét valószínűségi eloszlás és $a_i \ge 0$ esetén

$$\left[\sum_{i=1}^K a_i^r P_i \right]^{\frac{1}{r}} \le \left[\sum_{i=1}^K a_i^s P_i \right]^{\frac{1}{s}}, \tag{8.4}$$

  ha $\{0 < r < s\}$, és az egyenlőség akkor és csak akkor áll fent, ha a_i konstans. Ha ez nem áll fent, akkor az

$$\left[\sum_{i=1}^K a_i^r P_i \right]^{\frac{1}{r}} \tag{8.5}$$

  függvény az $\{0 < r\}$ tartományban r-rel monoton nő.

  Az

$$\begin{array}{l} a_i \Rightarrow P_{Y|X}(y \mid x) \\ r \Rightarrow \frac{1}{1+\rho_1} \\ s \Rightarrow \frac{1}{1+\rho_2} \\ P_i \Rightarrow Q_X(x) \end{array} \tag{8.6}$$

helyettesítések után a

$$\left[\sum_x P_{Y|X}(y\mid x)^{\frac{1}{1+\rho_1}} Q_X(x)\right]^{1+\rho_1} \geq \left[\sum_x P_{Y|X}(y\mid x)^{\frac{1}{1+\rho_2}} Q_X(x)\right]^{1+\rho_2}, \tag{8.7}$$

ha $\{-1<\rho_1<\rho_2\}$, és az egyenőség akkor és csak akkor áll fent, ha $P_{Y|X}(y\mid x)$ nem függ x-től. Ez utóbbi esetben a csatorna kimenete független a csatorna bemenetétől, azaz a csatorna kapacitása nulla. Tehát, ha a csatorna kapacitása nem nulla, akkor a függvény a $\{-1<\rho\}$ tartományban ρ-val monoton csökken.

A Gallager-függvény definíciója szerint minket csak a $0\leq\rho\leq 1$ tartománybeli viselkedés érdekel, amelyben az

$$\left[\sum_x P_{Y|X}(y\mid x)^{\frac{1}{1+\rho}} Q_X(x)\right]^{1+\rho} \tag{8.8}$$

függvény a $\rho=0$ helyen veszi fel a maximum értékét, és az a

$$\left[\sum_x P_{Y|X}(y\mid x)^{\frac{1}{1+\rho}} Q_X(x)\right]^{1+\rho}\Big|_{\rho=0} = \sum_x P_{Y|X}(y\mid x)\,Q_X(x) = \sum_x P_{Y,X}(y,x) = P_Y(y) \tag{8.9}$$

kifejezéssel egyenlő.

Ezek alapján az

$$E_0(\rho,Q) = -\log_2 \sum_y \left[\sum_x \left(P_{Y|X}(y\mid x)\right)^{\frac{1}{1+\rho}} Q_X(x)\right]^{1+\rho}, \quad 0\leq\rho\leq 1 \tag{8.10}$$

Gallager-függvény minimumát a $\{0\leq\rho\leq 1\}$ tartományban a $\rho=0$ helyen veszi fel:

$$E_0(0,Q) = -\log_2 \sum_y \left[\sum_x \left(P_{Y|X}(y\mid x)\right)^{\frac{1}{1+\rho}} Q_X(x)\right]^{1+\rho}\Big|_{\rho=0} = -\log_2 \sum_y P_Y(y) = 0, \tag{8.11}$$

tehát a függvény nem negatív és ρ-val monoton nő, azaz

$$\frac{\partial E_0(\rho,Q)}{\partial\rho} > 0, \quad 0\leq\rho\leq 1. \tag{8.12}$$

A függvény viselkedését a 8.1. ábrán illusztráljuk.

- Ebben a pontban megmutatjuk, hogy az $E_0(\rho,Q)$ Gallager-függvény a $0\leq\rho\leq 1$ tartományban konvex.

  Legyen λ, ρ_1 és ρ_2 tetszőleges számok a $[0,1]$ tartományban, és jelöljük ρ_λ-val a

$$\rho_\lambda = \lambda\rho_1 + (1-\lambda)\rho_2 = \lambda\rho_1 + \overline{\lambda}\rho_2 \tag{8.13}$$

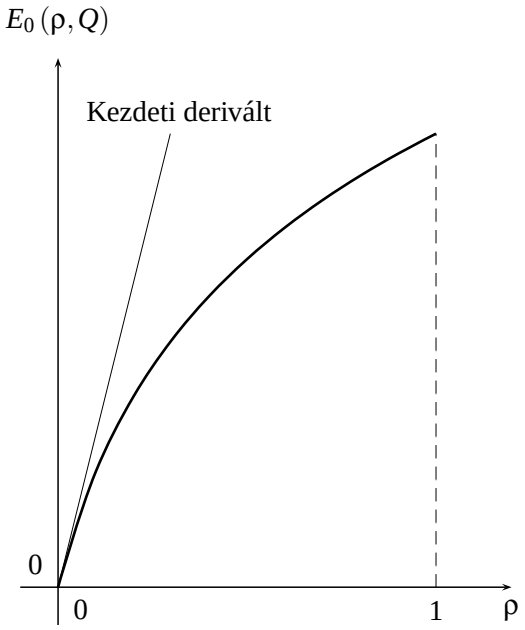
  értéket, ahol $\overline{\lambda}=(1-\lambda)$. Ha az $E_0(\rho,Q)$ Gallager-függvény ρ-ban konvex, akkor fent kell állnia az

$$E_0(\rho_\lambda,Q) \geq \lambda E_0(\rho_1,Q) + \overline{\lambda}E_0(\rho_2,Q) \tag{8.14}$$

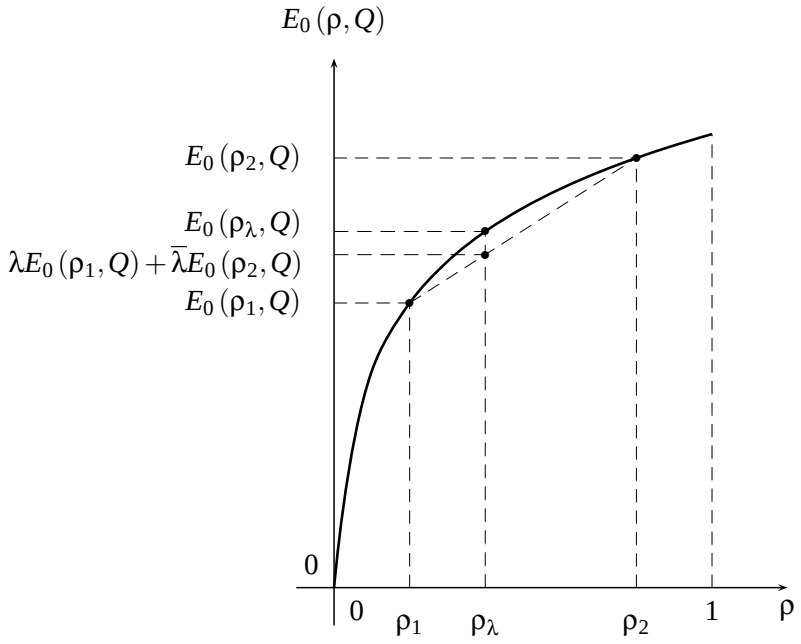
  egyenlőtlenségnek, amit a 8.2. ábrán illusztrálunk.

  Ismert, hogy tetszőleges $P_i,\ \{i=1,2,...,K\}$ diszkrét valószínűségi eloszlás és $a_i\geq 0$ esetén

$$\left[\sum_{i=1}^K P_i a_i^{\frac{1}{\lambda s+\overline{\lambda}r}}\right]^{\lambda s+\overline{\lambda}r} \leq \left[\sum_{i=1}^K P_i a_i^{\frac{1}{s}}\right]^{\lambda s} \left[\sum_{i=1}^K P_i a_i^{\frac{1}{r}}\right]^{\overline{\lambda}r}, \tag{8.15}$$



8.1. ábra. Az $E_0(\rho, Q)$ jellegének illusztrálása a ρ függvényében



8.2. ábra. Az $E_0(\rho, Q)$ konvex jellegének az illusztrálása a ρ függvényében

és az egyenlőség akkor és csak akkor áll fent, ha $ca_i^{1/s} = a_i^{1/r}$ minden i-re.

Az

$$\begin{aligned} a_i &\Rightarrow P_{Y|X}(y \mid x) \\ r &\Rightarrow (1+\rho_1) \\ s &\Rightarrow (1+\rho_2) \\ P_i &\Rightarrow Q_X(x) \end{aligned} \tag{8.16}$$

helyettesítések után

$$\lambda s + (1-\lambda) r = \lambda(1+\rho_1) + (1-\lambda)(1+\rho_2) = \lambda\rho_1 + (1-\lambda)\rho_2 + 1 = 1 + \rho_\lambda, \tag{8.17}$$

ezért

$$\left[\sum_x \left(P_{Y|X}(y \mid x)\right)^{\frac{1}{1+\rho_\lambda}} Q_X(x)\right]^{1+\rho_\lambda} \leq$$

$$\leq \left[\sum_x \left(P_{Y|X}(y \mid x)\right)^{\frac{1}{1+\rho_1}} Q_X(x)\right]^{\lambda(1+\rho_1)} \left[\sum_x \left(P_{Y|X}(y \mid x)\right)^{\frac{1}{1+\rho_2}} Q_X(x)\right]^{\bar{\lambda}(1+\rho_2)}. \tag{8.18}$$

Alkalmazzuk ezután a

$$\sum_{i=1}^K a_i b_i \leq \left(\sum_{i=1}^K a_i^{\frac{1}{\lambda}}\right)^{\lambda} \left(\sum_{i=1}^K b_i^{\frac{1}{1-\lambda}}\right)^{1-\lambda} \tag{8.19}$$

Hölder-egyenlőtlenséget, amely minden $\lambda \in [0,1]$, $a_i \geq 0$ és $b_i \geq 0$ számhalmazra igaz, és amelynél az egyenlőség akkor és csak akkor áll fent, ha $a_i^{1-\lambda} = b_i^{\lambda}$, és vizsgáljuk meg az $E_0(\rho, Q)$ függvényben szereplő

$$\sum_y \left[\sum_x \left(P_{Y|X}(y \mid x)\right)^{\frac{1}{1+\rho_\lambda}} Q_X(x)\right]^{1+\rho_\lambda} \leq$$

$$\leq \sum_y \left[\sum_x \left(P_{Y|X}(y \mid x)\right)^{\frac{1}{1+\rho_1}} Q_X(x)\right]^{\lambda(1+\rho_1)} \left[\sum_x \left(P_{Y|X}(y \mid x)\right)^{\frac{1}{1+\rho_2}} Q_X(x)\right]^{\bar{\lambda}(1+\rho_2)} \tag{8.20}$$

kifejezés jobb oldalát, és vegyük észre, hogy a

$$a_i \Rightarrow \left[\sum_x \left(P_{Y|X}(y \mid x)\right)^{\frac{1}{1+\rho_1}} Q_X(x)\right]^{\lambda(1+\rho_1)} \tag{8.21}$$

és a

$$b_i \Rightarrow \left[\sum_x \left(P_{Y|X}(y \mid x)\right)^{\frac{1}{1+\rho_2}} Q_X(x)\right]^{\bar{\lambda}(1+\rho_2)} \tag{8.22}$$

helyettesítés után a

$$\sum_y \left[\sum_x \left(P_{Y|X}(y \mid x)\right)^{\frac{1}{1+\rho_1}} Q_X(x)\right]^{\lambda(1+\rho_1)} \left[\sum_x \left(P_{Y|X}(y \mid x)\right)^{\frac{1}{1+\rho_2}} Q_X(x)\right]^{(1-\lambda)(1+\rho_2)} \leq$$

$$\leq \left(\sum_y \left[\sum_x \left(P_{Y|X}(y \mid x)\right)^{\frac{1}{1+\rho_1}} Q_X(x)\right]^{(1+\rho_1)}\right)^{\lambda} \left(\sum_y \left[\sum_x \left(P_{Y|X}(y \mid x)\right)^{\frac{1}{1+\rho_2}} Q_X(x)\right]^{(1+\rho_2)}\right)^{1-\lambda}. \tag{8.23}$$

Ezután igaz, hogy

$$\sum_y \left[\sum_x \left(P_{Y|X}(y \mid x)\right)^{\frac{1}{1+\rho_\lambda}} Q_X(x)\right]^{1+\rho_\lambda} \leq$$

$$\leq \left(\sum_y \left[\sum_x \left(P_{Y|X}(y \mid x) \right)^{\frac{1}{1+\rho_1}} Q_X(x) \right]^{(1+\rho_1)} \right)^{\lambda} \left(\sum_y \left[\sum_x \left(P_{Y|X}(y \mid x) \right)^{\frac{1}{1+\rho_2}} Q_X(x) \right]^{(1+\rho_2)} \right)^{1-\lambda}, \tag{8.24}$$

és képezve a két oldal kettes alapú logaritmusának a minusz egyszeresét

$$-\log_2 \sum_y \left[\sum_x \left(P_{Y|X}(y \mid x) \right)^{\frac{1}{1+\rho_\lambda}} Q_X(x) \right]^{1+\rho_\lambda} \geq$$

$$\geq -\lambda \log_2 \sum_y \left[\sum_x \left(P_{Y|X}(y \mid x) \right)^{\frac{1}{1+\rho_1}} Q_X(x) \right]^{(1+\rho_1)} - (1-\lambda) \log_2 \sum_y \left[\sum_x \left(P_{Y|X}(y \mid x) \right)^{\frac{1}{1+\rho_2}} Q_X(x) \right]^{(1+\rho_2)}, \tag{8.25}$$

ezért igaz, hogy

$$E_0(\rho_\lambda, Q) \geq \lambda E_0(\rho_1, Q) + \bar{\lambda} E_0(\rho_2, Q), \tag{8.26}$$

vagyis az $E_0(\rho, Q)$ Gallager-függvény a vizsgált tartományban konvex, azaz

$$\frac{\partial^2 E_0(\rho, Q)}{\partial \rho^2} \leq 0, \tag{8.27}$$

amivel az állítást bebizonyítottuk.

- Ebben a pontban a Gallager-függvény $\rho = 0$ helyen felvett kezdeti deriváltját határozzuk meg a ρ szerint (lásd a 8.1. ábrát).

  Az eredeti függvény a korábbiaknak megfelelően az

$$E_0(\rho, Q) = -\log_2 \sum_y \left[\sum_x \left(P_{Y|X}(y \mid x) \right)^{\frac{1}{1+\rho}} Q_X(x) \right]^{1+\rho} \tag{8.28}$$

  formában írható fel.

  A formális és hosszadalmas deriválási műveletek elvégzése helyett állítsuk elő a logaritmus argumentumában lévő

$$\sum_y \left[\sum_x \left(P_{Y|X}(y \mid x) \right)^{\frac{1}{1+\rho}} Q_X(x) \right]^{1+\rho} \tag{8.29}$$

  függvény Taylor-sorának első két tagját az

$$a^{\frac{1}{1+\rho}} \cong a - \rho a \ln a + \ldots \tag{8.30}$$

  és a

$$b^{1+\rho} \cong b + \rho b \ln b + \ldots \tag{8.31}$$

  Taylor-sorok segítségével. Ennek alapján a

$$b = \sum_x \left(P_{Y|X}(y \mid x) \right)^{\frac{1}{1+\rho}} Q_X(x) = \sum_x \left(P(y \mid x) \right)^{\frac{1}{1+\rho}} Q(x) \tag{8.32}$$

  és az

$$a = P_{Y|X}(y \mid x) = P(y \mid x) \tag{8.33}$$

  helyettesítések után a

$$\sum_y \left[\sum_x \left(P(y \mid x) \right)^{\frac{1}{1+\rho}} Q(x) \right]^{1+\rho} \cong$$

$$\cong \sum_y \left\{ \sum_x \left(P(y \mid x)\right)^{\frac{1}{1+\rho}} Q(x) + \rho \left[\sum_x \left(P(y \mid x)\right)^{\frac{1}{1+\rho}} Q(x) \right] \ln \left[\sum_x \left(P(y \mid x)\right)^{\frac{1}{1+\rho}} Q(x) \right] \right\} \cong$$

$$\cong \sum_y \sum_x P(y \mid x) \left(1 - \rho \ln \left(P(y \mid x)\right)\right) Q(x) +$$

$$+\rho \sum_y \left[\sum_x P(y \mid x) \left(1 - \rho \ln \left(P(y \mid x)\right)\right) Q(x) \right] \ln \left[\sum_x P(y \mid x) \left(1 - \rho \ln \left(P(y \mid x)\right)\right) Q(x) \right] \cong$$

$$\cong \sum_y \sum_x P(y \mid x) Q(x) - \rho \sum_y \sum_x P(y \mid x) Q(x) \ln \left(P(y \mid x)\right) +$$

$$+\rho \sum_y \sum_x P(y \mid x) Q(x) \ln \left[\sum_x P(y \mid x) Q(x) \right] =$$

$$= \sum_y \sum_x P(x,y) - \rho \sum_y \sum_x P(x,y) \ln \left(P(y \mid x)\right) + \rho \sum_y \sum_x P(y,x) \ln \left(P(y)\right) =$$

$$= 1 - \rho \sum_y \sum_x P(x,y) \ln \left(P(y \mid x)\right) + \rho \sum_y \sum_x P(x,y) \ln \left(P(y)\right). \tag{8.34}$$

Felhasználva a fenti egyenletet, és a

$$\log_2 (1 + cx) = \frac{\ln (1 + cx)}{\ln 2} \cong x \frac{c}{\ln 2} \ldots \tag{8.35}$$

Taylor-sort, az $E_0(\rho, Q)$ függvény Talor-sorának első két tagja a $\rho = 0$-ban az alábbi alakban írható fel:

$$E_0(\rho, Q) \cong -\log_2 \left\{ 1 - \rho \sum_y \sum_x P(x,y) \ln \left(P(y \mid x)\right) + \rho \sum_y \sum_x P(x,y) \ln \left(P(y)\right) \right\} =$$

$$= -\log_2 \left\{ 1 + \rho \left(-\sum_y \sum_x P(x,y) \ln \left(P(y \mid x)\right) + \sum_y \sum_x P(x,y) \ln \left(P(y)\right) \right) \right\} \cong$$

$$\cong -\frac{\rho}{\ln 2} \left(-\sum_y \sum_x P(x,y) \ln \left(P(y \mid x)\right) + \sum_y \sum_x P(x,y) \ln \left(P(y)\right) \right) =$$

$$= \rho \left(\sum_y \sum_x P(x,y) \log_2 \left(P(y \mid x)\right) - \sum_y \sum_x P(x,y) \log_2 \left(P(y)\right) \right) =$$

$$= \rho \left(H(Y) - H(Y \mid X)\right) = \rho I(X;Y), \tag{8.36}$$

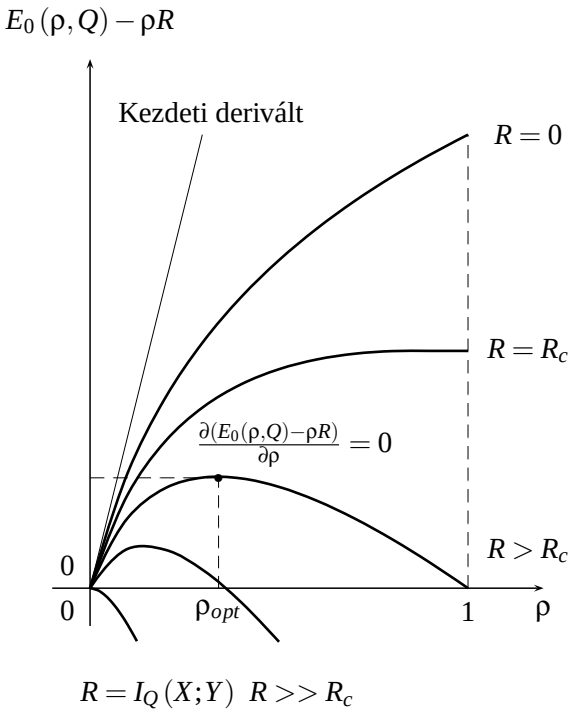
azaz az $E_0(\rho, Q)$ meredeksége a $\rho = 0$ helyen azonos a csatorna bemeneti és kimeneti jele közötti kölcsönös információval, tehát

$$\frac{\partial E_0(\rho, Q)}{\partial \rho} \Big|_{\rho=0} = I(X;Y). \tag{8.37}$$

- Vizsgáljuk meg ezután az

$$E_G(R, Q) = \max_{0 \le \rho \le 1} \left[E_0(\rho, Q) - \rho R \right] \tag{8.38}$$

exponens viselkedését az R átviteli sebesség függvényében. Ehhez meg kell keresni a $0 \le \rho \le 1$ tartományban az $E_0(\rho, Q) - \rho R$ függvény ρ szerinti maximumát. A feladat megoldása előtt célszerű ábrázolni az $E_0(\rho, Q) - \rho R$ függvényt, hogy a ρ szerinti maximumról képet tudjunk alkotni (lásd a 8.2. ábrát). Az ábrából jól látható, hogy



8.3. ábra. Az $E_0(\rho,Q)-\rho R$ jellegének illusztrálása a ρ függvényében

– Kis R értékeknél a függvény a $0 \leq \rho \leq 1$-ban a tartomány szélén a $\rho = 1$ helyen veszi fel a maximális értékét. Ezen a maximum helyen

$$E_G(R,Q) = E_0(1,Q) - R, \tag{8.39}$$

azaz ebben a tartományban az exponens az átviteli sebesség növekedésével lineárisan csökken, és a csökkenés meredeksége egy. Emellett tudjuk, hogy

$$E_0(1,Q) - R = E_B(Q), \tag{8.40}$$

ahol $E_B(Q)$ nem más, mint a Q szerinti maximalizálás előtti Bhattacharyya-exponens.

– Ez a helyzet addig az R_c értékig tart, amíkor az $E_0(\rho,Q)-\rho R$ függvény ρ szerinti deriváltja a $\rho = 1$ helyen éppen nulla értékű, azaz

$$\frac{\partial\left(E_0(\rho,Q)-\rho R_c\right)}{\partial\rho}\Big|_{\rho=1} = 0, \tag{8.41}$$

amiből

$$\frac{\partial E_0(\rho,Q)}{\partial\rho}\Big|_{\rho=1} - R_c = 0, \tag{8.42}$$

illetve

$$R_c = \frac{\partial E_0(\rho,Q)}{\partial\rho}\Big|_{\rho=1}. \tag{8.43}$$

Látható, hogy R_c-nél nagyobb adatsebességeknél az $E_0(\rho,Q)-\rho R$ maximumához tartozó ρ érték kisebb egynél.

– Ha R jóval nagyobb, mint R_c, akkor az $E_0(\rho,Q)-\rho R$ maximumához tartozó ρ érték monoton csökken, és amikor R eléri az $E_0(\rho,Q)$ kezdeti deriváltját, az

$$R=\frac{\partial E_0(\rho,Q)}{\partial\rho}\Big|_{\rho=0}=I_Q(X;Y), \tag{8.44}$$

értéket, akkor az $E_0(\rho,Q)-\rho R$ maximumához tartozó ρ érték nulla lesz, és az $E_G(R,Q)$ Gallager-exponens a $0\le\rho\le 1$ tartományban nem lehet nullánál nagyobb, mivel

$$\lim_{\rho\to 0}E_G(R,Q)=\lim_{\rho\to 0}\left(E_0(\rho,Q)-\rho R\right)=\rho\left(I_Q(X;Y)-R\right), \tag{8.45}$$

ami biztosan nem pozitív, ha $I_Q(Y;X)\le R$. Ebből megállapítható, hogy a Gallager-exponens optimális ρ választása esetén az $I_Q(Y;X)>R$ tartományban pozitív értéket vesz fel.

– A fentiekből a Q_X szerinti maximumkeresés után igaz, hogy

$$E_G(R)=\max_{Q_X}E_G(Q,R)\ge 0 \tag{8.46}$$

az

$$R\le\max_{Q_X}I_Q(X;Y)=C \tag{8.47}$$

tartományban, azaz a kapacitásnál kisebb átviteli sebességek mellett a korábban megismert

$$\mathbf{E}[P_B]\le 2^{-N(E_0(\rho,Q)-\rho R)}=2^{-NE_G(R)},\quad 0\le\rho\le 1 \tag{8.48}$$

kifejezés alapján aszimptotikusan (ha a N minden határon túl nő) hibamentesen lehet kommunikálni, és egyúttal véletlen kódolásnál felső korlátot lehet adni az átlagos blokkhibavalószínűségre.

8.2. Az átlagokra vonatkozó egyenlőtlenség igazolása

Legyen $\{x_i\}$ $(i=1,2,\ldots,M)$ pozitív valós számok halmaza, és jelöljük $\bar{x}$-sal a számok számtani átlagát. Legyen $M=2M'$ páros, és vegyük ki a halmazból az M' számú legnagyobb értéket. Ebben az esetben igaz, hogy a megmaradó számok mindegyike:

$$x_i\le 2\bar{x}. \tag{8.49}$$

Az állítás egyszerűen belátható, ha feltételezzük, hogy az eredeti M számot növekvő sorrendbe állítjuk $x_1\le x_2\le\ldots\le x_{M'}\le x_{M'+1}\le\ldots\le x_M$, és kiszámítjuk $\bar{x}$ értékét

$$\bar{x}=\frac{1}{M}\left[\sum_{i=1}^{M'}x_i+\sum_{i=M'+1}^{2M'}x_i\right]. \tag{8.50}$$

Ha az állítás nem volna igaz, akkor az első M' sorszámú x_i között kellene lenni legalább egy $2\bar{x}$-nál nagyobb értékű elemnek, azaz minden M'-nél nagyobb sorszámú x_i-nek nagyobbnak kellene lenni $2\bar{x}$-nál. Ha ez igaz lenne, akkor az egyenlőség jobb oldalát nem növelnénk, ha minden ilyen tagot $2\bar{x}$-vel helyettesítenénk:

$$\bar{x}=\frac{1}{M}\left[\sum_{i=1}^{M'}x_i+\sum_{i=M'+1}^{2M'}x_i\right]\ge\frac{1}{M}\left[\sum_{i=1}^{M'}x_i+2M'\bar{x}\right]=\frac{1}{M}\sum_{i=1}^{M'}x_i+\bar{x}, \tag{8.51}$$

amiből nyilvánvaló, hogy ekkor az első M' sorszámú tag értéke biztosan nem lehet nullánál nagyobb, ami ellentmond a kiindulási feltételnek. Eszerint az első M' sorszámú tag értéke biztosan kisebb, vagy legfeljebb egyenlő $2\bar{x}$-sal.

8.3. Az $\mathbf{E}[W_j]$ felső korlátjának származtatása trellis kódoló és véletlen kódolás esetén

A 7.70. egyenletben az információs bithibák várható értékének, $\mathbf{E}[W_j]$-nek a felső korlátját kívántuk meghatározni. Az ottani megfontolások alapján és felhasználva a 7.66. egyenletet a felső korlátra a

$$\mathbf{E}[W_j] < k_0 2^{k_0} 2^{-N_t E_0(\rho,Q)} \sum_{l=T+1}^{L_t+T+1-j} (l-T) 2^{-n_0[E_0(\rho,Q)-\rho R_t](l-T-1)} \tag{8.52}$$

kifejezés adódott. A szummázás határainak formális átalakításával, azaz $i = l - T$ választással az egyenlet a

$$\mathbf{E}[W_j] < k_0 2^{k_0} 2^{-N_t E_0(\rho,Q)} \sum_{i=1}^{L_t+1-j} i \left\{ 2^{-n_0[E_0(\rho,Q)-\rho R_t]} \right\}^{i-1} =$$

$$= k_0 2^{k_0} 2^{-N_t E_0(\rho,Q)} \sum_{i=0}^{L_t+1-j} i \left\{ 2^{-n_0[E_0(\rho,Q)-\rho R_t]} \right\}^{i-1} \tag{8.53}$$

formába alakítható át.

Általában ismert, hogy minden $0 \le a < 1$ esetén a

$$\sum_{i=0}^{L_t+1-j} i a^{i-1} \le \sum_{i=0}^{\infty} i a^{i-1} = \frac{\partial}{\partial a} \sum_{i=0}^{\infty} a^i = \frac{\partial}{\partial a} \left[\frac{1}{1-a} \right] = \frac{1}{(1-a)^2}, \tag{8.54}$$

ezért a $\mathbf{E}[W_j]$ kifejezés felső korlátját az $a = 2^{-n_0[E_0(\rho,Q)-\rho R_t]}$ választás után a

$$\mathbf{E}[W_j] < k_0 2^{k_0} 2^{-N_t E_0(\rho,Q)} \frac{1}{\left(1 - 2^{-n_0[E_0(\rho,Q)-\rho R_t]}\right)^2}; \quad R_t < \frac{E_0(\rho,Q)}{\rho} \tag{8.55}$$

formában írhatjuk fel.