7

AZ INFORMÁCIÓELMÉLET ALAPJAI

Részletek

Ebben a fejezetben néhány alapvető tételt ismerünk meg a hírközlés információelméleti alapjaiból. Definiálni fogjuk az **információt**, amit eddig csak az üzenetek szinonimájaként használtunk.

FORRÁSKÓDOLÁS

Egy kézenfekvő ötlet a forrás üzeneteinek tömörítésére olyan változó hosszúságú kódszavakat használni, amelyek kielégítik a következő egyenlőtlenség-láncot:

$$\log_2 \frac{1}{p_i} \le l_i < \log_2 \frac{1}{p_i} + 1$$

tehát vagy éppen annyi bináris számjegyet használni, mint a szimbólum reciprok-valószínűségének ("meglepetési tényezőjének") logaritmusa - amennyiben ez egész szám - vagy pedig az ezt követő egész számot.

Ez az ötlet azért gyümölcsöző, mert kiszámítva a lánc egyes tagjainak az átlagát (várhatóértékét), a következőt kapjuk:

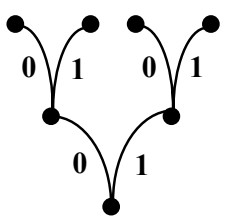
$$\sum_{i=1}^{m} p_i \cdot \log_2 \frac{1}{p_i} \le \sum_{i=1}^{m} p_i \cdot l_i < \sum_{i=1}^{m} p_i \cdot \log_2 \frac{1}{p_i} + 1$$

Az összefüggés baloldalán lévő átlagot entrópiának hívjuk és $H(\mathcal{P})$-vel jelöljük, a középső tag az átlagos kódszóhosszúság és a jele legyen $L(\mathcal{P})$, míg a jobboldalon nyilván $H(\mathcal{P})+1$ áll. Ilymódon megkaptuk a forráskódolás Shannon által kimondott első tételét, csak sajnos még azt nem tudjuk, hogy a fenti módon választott hosszúságú kódszavak alkothatnak-e egy ú.n. pillanatkódot.

A pillanatkód azt jelenti, hogy egyik kódszó sem eleje, kezdete valamely másik kódszónak. Arra természetesen szükség van, hogy a keletkező kód pillanatkód legyen, hiszen ellenkező esetben a kódszavak határainak jelzésére további szimbólumokat kellene alkalmazni, ami érvénytelenné tenné a fent kiszámított átlagos szóhosszúságot.

Például bináris esetben csak egyetlen egységnyi hosszúságú kódszó lehet, például az 1 mert az összes többinek ekkor a 0-val kell kezdődnie, és több, mint egy bináris számjegyet kell tartalmaznia, ilymódon az 1-es nem lesz a kezdetük.

A legszemléletesebb módszer pillanatkódok szerkesztésére a gyökeres fa használata. A mellékelt ábra mutat egy ilyen bináris fát (csupán két szintben), ahol a közös gyökérből induló ágakat minden elágazásnál (bináris fa ágai mindig kétfelé ágaznak el) megjelöljük a bináris szimbólumokkal. Ha a gyökértől az ágak mentén haladva összeolvassuk a szimbólumokat, akkor az ágvégeken, a leveleknél olyan bináris számokat, kódszavakat kapunk, amelyek pillanatkódok. Persze nem kell feltétlenül valamennyi ág mentén



elmenni a végéig, korábban is megállhatunk és letörhetjük az ág folytatását. Az így kapott kódszavak rövidebbek lesznek, és továbbra sem lesz egyik sem eleje valamely másiknak. Ennek alapján egyszerűen választ adhatunk arra a kérdésre, hogy hány ilyen kódszót helyezhetünk el a fán. Mivel mindegyik szinten duplázódik az ágak száma, ezért amennyiben a fa teljes, akkor nyilván kettőnek a szint-számmal, jelölje *N*, megegyező hatványa lesz a levelek, azaz a kódszavak száma. Ha lemetszünk egy ágat az *i*-edik szinten, akkor az előbbiek szerint ezzel eltávolítunk egy olyan bináris részfát, amelynek *N-i* szinje van. A metszésnél elhelyezhetünk egy levelet, azaz kódszót. Ebben a gondolatmenetben persze lemetszhetjük az ágvégen lévő levelet is, majd ide helyezünk egy kódszót, tehát valójában nem csökkentjük a teljes fát. Végül hány kódszót helyezhetünk el összesen? Nyilván nem többet, mint a teljes fa összes leveleinek a száma, azaz, ha l_i-vel jelöljük a kódszavak hosszát, ami természetesen egyenlő a fa szintjének a sorszámával, ahová a kódszót helyezzük, akkor a következő összefüggést kapjuk:

$$2^N \geq \sum_{i=1}^{m} 2^{N-l_i}$$

Az egyenlőtlenség mindkét oldalát elosztva 2^N-el, a Kraft egyenlőtlenséget kapjuk a bináris esetre:

$$\sum_{i=1}^{m} 2^{-l_i} \leq 1$$

Ez az egyenlőtlenség szükséges és elégséges feltétele annak, hogy egy kód az *m* darab, egyenként l_i hosszúságú kódszóval, pillanatkód legyen. Végül, ha figyelembe vesszük, hogy *r*-áris esetben a fa minden szinten *r* felé ágazik, akkor az egyenlőtlenségben a 2-őt *r*-re kell cserélni.

Az entrópia maximuma

A $H(\mathcal{P}) := \sum_{i=1}^{m} p_i \cdot \log_2 \frac{1}{p_i}$-ként definiált entrópia, mint a memóriátlan forrás által szimbólumonként átlagosan kibocsátott információ a maximális értékét egyenletes eloszlás esetén, azaz $p_i = 1/m$ mellett éri el, és értéke $\log_2 m$. Ennek egyszerű bizonyítását mutatjuk be az alábbiakban. Számítsuk ki a $H(\mathcal{P}) - \log_2 m$ különbséget!

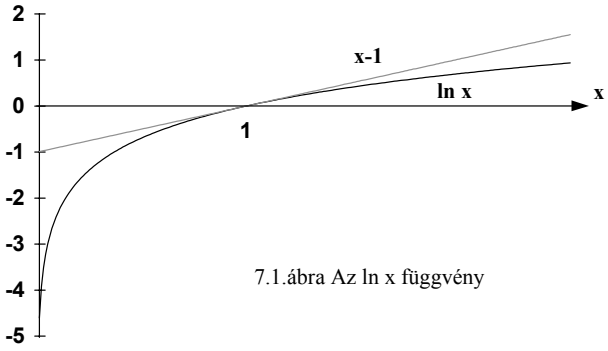
$$H(\mathcal{P}) - \log_2 m = \sum_{i=1}^{m} p_i \cdot \log_2 \frac{1}{p_i} - \log_2 m = \sum_{i=1}^{m} p_i \cdot \log_2 \frac{1}{p_i} - \sum_{i=1}^{m} p_i \cdot \log_2 m$$

ahol a második tagban figyelembe vettük, hogy $\sum_{i=}^{m} p_i = 1$. A két szummát összevonva a következőt kapjuk:

$$H(\mathcal{P}) - \log_2 m = \sum_{i=1}^{m} p_i \cdot \log_2 \frac{1}{m \cdot p_i}$$

Használjuk fel a logaritmus függvénynek egy közismert tulajdonságát, amit a mellékelt ábrán is szemléltettünk:

$\ln x \le x-1$ vagy $\ln\frac{1}{x} \ge 1-x$



7.1.ábra Az ln x függvény

Mivel $\log_2 x = \frac{\ln x}{\ln 2}$, a fenti különbségre kapjuk:

$$H(\mathcal{P}) - \log_2 m = \frac{1}{\ln 2}\sum_{i=1}^{m} p_i \cdot \ln\frac{1}{m \cdot p_i}$$

Illetve alkalmazva az első egyenlőtlenséget:

$$H(\mathcal{P}) - \log_2 m \le \frac{1}{\ln 2}\sum_{i=1}^{m} p_i \cdot \left(\frac{1}{m \cdot p_i} - 1\right) = \frac{1}{\ln 2}\left[\sum_{i=1}^{m}\frac{1}{m} - \sum_{i=1}^{m} p_i\right] = 0$$

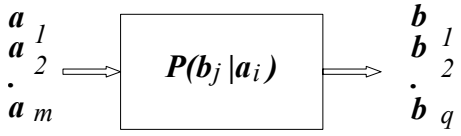
Az entrópia tehát maximum $\log_2 m$ értékű lehet, amely értéket tényleg el is éri, ha $p_i = 1/m$, mert az *ln* függvény és az egyenes felhasznált viszonya szerint *x=1* esetén egyenlőség áll fenn.

CSATORNAKÓDOLÁS

A CSATORNAKAPACITÁS

A forráskódolásnál bevezetett entrópia értelmezésének kiterjesztése alapján konstruáljunk egy kifejezést a csatornán átjutó információ mennyiségére.

Az információs csatornát írjuk le a bemenetén lévő $\mathcal{A} = \{a_i\}$, i=1,2,...,*m;* bemeneti abc-vel, a kimenetén lévő $\mathcal{B} = \{b_i\}$, i=1,2,...,*q*; kimeneti abc-vel, valamint a $P(b_j|a_i) = P_{ij}$ átmenet-valószínűségekkel.



7.2. ábra A csatornamodell

Az átmenet-valószínűségek kényelmesen kezelhetők mátrix elrendezésben:

$$\mathbf{P} = \begin{bmatrix} P_{11} & P_{12} & \dots & P_{1q} \\ P_{21} & P_{22} & \dots & P_{2q} \\ . & . & \dots & . \\ P_{m1} & P_{m2} & \dots & P_{mq} \end{bmatrix}$$

Ha bemeneti szimbólumokat választunk $\mathbf{P}(\mathcal{A}) = \left(\mathrm{P}(a_1), \mathrm{P}(a_2), \dots, \mathrm{P}(a_m)\right)$ valószínűséggel, akkor azok a csatornán átjutva kimeneti szimbólumokat eredményeznek $\mathbf{P}(\mathcal{B}) = \left(\mathrm{P}(b_1), \mathrm{P}(b_2), \dots, \mathrm{P}(b_q)\right)$ valószínűséggel. A kimeneti szimbólumok valószínűségeit egyszerűen meghatározhatjuk a bemeneti szimbólumok valószínűségeivel és az átmenet-valószínűségekkel:

$$\mathbf{P}(\mathcal{B}) = \mathbf{P}(\mathcal{A}) \cdot \mathbf{P} \qquad (7.1)$$

A továbbiakban feltételezzük, hogy a $\mathbf{P}(\mathcal{A})$ a-priori valószínűség-eloszlás és a **P** csatornamátrix adott, tehát a $\mathbf{P}(\mathcal{B})$ kimeneti eloszlás a (7.1) alapján számítható.

A bemeneti eloszlásból és a csatornamátrixból kiszámíthatjuk az **együttes** és az ú.n. **a-posteriori** valószínűségeket:

$$\mathrm{P}(a_i,\, b_j) = \mathrm{P}(b_j |\, a_i)\, \mathrm{P}(a_i) = \mathrm{P}(a_i |\, b_j)\, \mathrm{P}(b_j)\,. \tag{7.2}$$

$$\mathrm{P}(a_i |\, b_j) = \frac{\mathrm{P}(b_j |\, a_i)\, \mathrm{P}(a_i)}{\mathrm{P}(b_j)} = \frac{\mathrm{P}(b_j |\, a_i)\, \mathrm{P}(a_i)}{\sum_{i=1}^{m} \mathrm{P}(b_j |\, a_i)\, \mathrm{P}(a_i)}, \tag{7.3}$$

Az a-posteriori valószínűségekre számíthatunk egy entrópiát, ugyanúgy, amint azt az a-priori valószínűségeknél tettük:

$$\begin{aligned} H(\mathcal{A}) &= \sum_{\mathcal{A}} \mathrm{P}(a) \log_2 \frac{1}{\mathrm{P}(a)}, \\ H(\mathcal{A} |\, b_j) &= \sum_{\mathcal{A}} \mathrm{P}(a |\, b_j) \log_2 \frac{1}{\mathrm{P}(a |\, b_j)}. \end{aligned} \tag{7.4}$$

Amint a (7.4)-es első egyenlete megadja, hogy az $\mathcal{A}$ forrás szimbólumainak leírására átlagosan **hány bit kell**, úgy a második egyenlet azt mondja meg, hogy átlagosan hány bit kell az $\mathcal{A}$ forrás szimbólumainak jellemzésére akkor, ha a csatorna kimenetén a b_j szimbólumot észleltük.

Nyilván igazából arra vagyunk kíváncsiak, hogy **bármelyik** kimeneti szimbólum megfigyelése után átlagosan hány bittel írhatók le a bemeneti szimbólumok. Ehhez szinte önként adódik az ötlet, számítsuk ki az **átlagos a-posteriori entrópiát**:

$$H(\mathcal{A} |\, \mathcal{B}) = \sum_{\mathcal{B}} \mathrm{P}(b)\, H(\mathcal{A} |\, b). \tag{7.5}$$

Ezt a mennyiséget feltételes entrópiának nevezik, az eredeti angol neve pedig *equivocation*. Shannon forráskódolási tételének általánosításával beláthatjuk, hogy a feltételes entrópia megadja a bemeneti szimbólumok meghatározásához átlagosan szükséges bitek számát, amennyiben megfigyelhetjük az általuk létrehozott kimeneti szimbólumokat.

Ilyen módon természetesen hangzik, hogy a kimeneti szimbólumok megfigyelésekor kapott információ előállítható egy különbségként, amelyben a bemeneti szimbólumok információjából le kell vonni a kimeneti szimbólumoknak a bemenetiekre vonatkozó információját, azaz az ú.n. **kölcsönös** információ a következő lesz:

$$I(\mathcal{A};\mathcal{B}) = H(\mathcal{A}) - H(\mathcal{A} |\, \mathcal{B})\,. \tag{7.6}$$

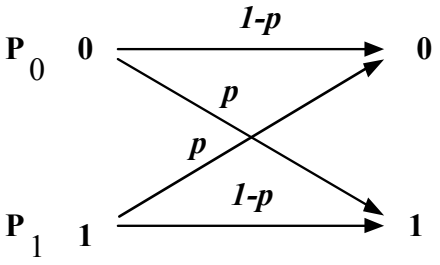
Értelmezzük még egy kicsit tovább ezt a kifejezést! Nézzük a lehetséges szélső határokat! Lássuk be, hogy a kölcsönös információ 0 és $H(\mathcal{A})$ között változhat! Nyilván akkor lesz nulla, ha a feltételes entrópia egyenlő a bemeneten lévő forrás entrópiájával. Mit is jelent ez? Miként már fentebb értelmeztük, ez azt jelenti, hogy a kimeneti szimbólumok megfigyelése után átlagosan még **ugyanannyi** bit kell a bemenő szimbólumok jellemzéséhez, mint ha semmit se tettünk volna. Ez tehát egyenértékű a lehető legrosszabb csatornával, vagy pontosabban megvizsgálva (egyszerű ugyan, de itt most nem tesszük meg) azt jelenti, hogy a kimenő és a bemenő szimbólumok függetlenek. A kölcsönös információ másik szélső értékét pedig akkor

kapjuk, ha semmit sem kell levonni, azaz $H(\mathcal{A}|\mathcal{B})=0$. Ez pedig azt jelenti, hogy a kimeneti szimbólumok megfigyelése után már semmi plusz információra nincs szükségünk ahhoz, hogy jellemezzük a bemeneti szimbólumokat. Ami nyilván egyenértékű azzal, hogy ideálisan jó a csatorna, mert a bemeneten lévő szimbólumokat maradéktalanul jellemzik a kimeneti megfigyeléseink.

A fentiek alapján logikus definíció a csatorna átviteli képességére, pontosabban **kapacitására** a kölcsönös információ lehető legnagyobb értékét venni. Az eddigiekből világos, hogy a kölcsönös információ az a-priori valószínűségeknek és a csatorna átmenet-valószínűségeinek a függvénye. Egészen természetes, hogy a csatorna jellemzését függetlenítsük a bemenetére kapcsolt forrást jellemző a-priori entrópiától, tehát:

$$C = \max_{P(\mathcal{A})} I(\mathcal{A};\mathcal{B}) = \max_{P(\mathcal{A})} [H(\mathcal{A}) - H(\mathcal{A}|\mathcal{B})]. \qquad (7.7)$$

Példaként érdemes megvizsgálni egy igen egyszerű, de nagyjelentőségű esetet, a bináris szimmetrikus csatornát (BSC). Legyen a forrás eloszlása P_0 és $P_1 = 1 - P_0$, a BSC-t jellemző átmenet-valószínűségek pedig p, illetve $1-p$, azaz a téves, illetve a helyes átmenet valószínűsége. Ezt szemléltettük a 7.3. ábrán. Amennyiben a fenti jellemzőket behelyettesítjük a (7.7) összefüggésbe, akkor az derül ki, hogy mind a két tagban szerepelni fognak az a-priori valószínűségek, ami nehézkessé teszi a maximum megkeresését. Szerencsére könnyen ki lehet mutatni, hogy a kölcsönös információ kifejezése igen érdekes és hasznos szimmetria tulajdonságokkal rendelkezik, nevezetesen:



7.3 ábra A BSC

$$I(\mathcal{A};\mathcal{B}) = H(\mathcal{A}) - H(\mathcal{A}|\mathcal{B}) = I(\mathcal{B};\mathcal{A}) = H(\mathcal{B}) - H(\mathcal{B}|\mathcal{A}). \qquad (7.8)$$

Számítsuk ki az utóbbi kifejezésben szereplő két tagot külön-külön:

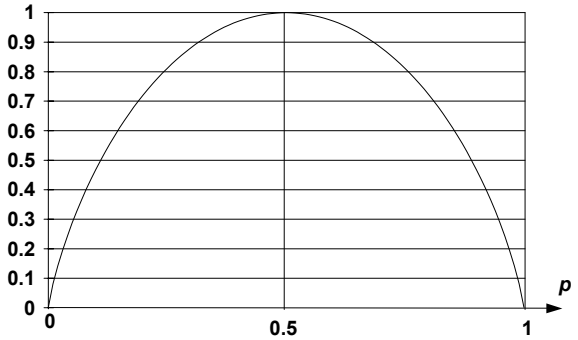
$$H(\mathcal{B}) = P(b=0)\cdot\log_2\frac{1}{P(b=0)} + P(b=1)\cdot\log_2\frac{1}{P(b=1)}$$

$H(\mathcal{B})$ akkor éri el a maximumát, ha a kimenet "egyenletes eloszlású", azaz $P(b=0)=P(b=1)=1/2$:

$$H(\mathcal{B}) = 0{,}5\cdot\log_2\frac{1}{0{,}5} + 0{,}5\cdot\log_2\frac{1}{0{,}5} = 1\,[\text{bit}]$$

Illusztrációként bemutatjuk az entrópia-függvényt bináris esetre a 7.4 ábrán.

7.4 ábra A bináris enrópia-függvény:



Folytatva a BSC kapacitásának kiszámítását, a feltételes entrópia következik, de most $\mathcal{B}|\mathcal{A}$ esetén! Ezt pedig egyszerűen a (7.4) és a (7.5) összefüggések alapján az alábbiak

szerint számíthatunk ki:

$$H(\mathcal{B}\,|\,\mathcal{A}) = \sum_{\mathcal{A}} \mathrm{P}(a)\; H(\mathcal{B}\,|a) = \sum_{i=1}^{m} \mathrm{P}(a_i) \sum_{j=1}^{q} \mathrm{P}(b_j\,|a_i)\, \log_2 \frac{1}{\mathrm{P}(b_j\,|a_i)}$$

A bináris esetre nagyon egyszerű a szummák kiszámítása, hiszen mindegyikben csak két tag szerepel:

$$H(\mathcal{B}\,|\,\mathcal{A}) = P_0\left[P(b=0\,|a=0)\cdot\log_2\frac{1}{P(b=0\,|a=0)} + P(b=1\,|a=0)\cdot\log_2\frac{1}{P(b=1\,|a=0)}\right] +$$
$$+ P_1\left[P(b=0\,|a=1)\cdot\log_2\frac{1}{P(b=0\,|a=1)} + P(b=1\,|a=1)\cdot\log_2\frac{1}{P(b=1\,|a=1)}\right]$$

Az itt részletesen felírt átmenet-valószínűségekre korábban már bevezettünk jeleket:

$$P(b=0\,|a=0) = 1-p;\quad P(b=1\,|a=0) = p$$
$$P(b=0\,|a=1) = p;\quad P(b=1\,|a=1) = 1-p$$

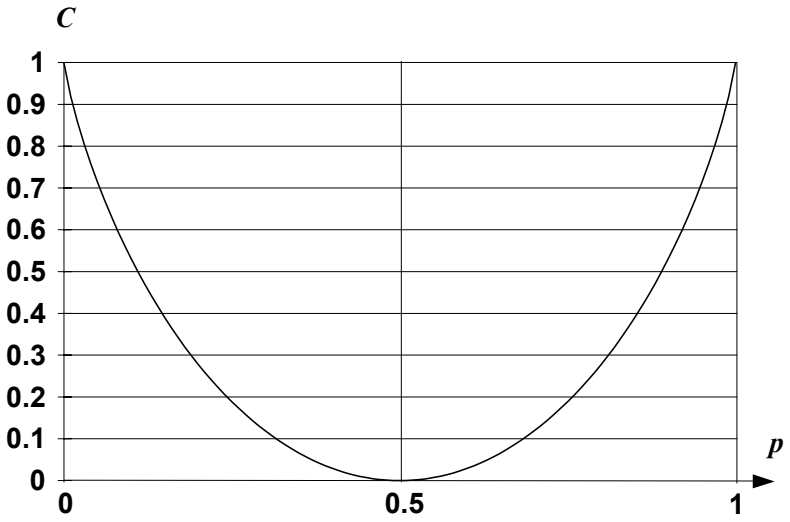
Ezzel a feltételes entrópia:

$$H(\mathcal{B}\,|\,\mathcal{A}) = P_0\left[(1-p)\cdot\log_2\frac{1}{(1-p)} + p\cdot\log_2\frac{1}{p}\right] + P_1\left[p\cdot\log_2\frac{1}{p} + (1-p)\cdot\log_2\frac{1}{(1-p)}\right] =$$
$$= (P_0+P_1)\cdot\left[p\cdot\log_2\frac{1}{p} + (1-p)\cdot\log_2\frac{1}{(1-p)}\right] = p\cdot\log_2\frac{1}{p} + (1-p)\cdot\log_2\frac{1}{(1-p)}$$

ahol világosan látszik, hogy $H(\mathcal{B}|\mathcal{A})$ független a forrás valószínűségeloszlásától, tehát a kölcsönös információra keresett maximum a BSC esetén a következő lesz:

$$C = 1 - p\cdot\log_2\frac{1}{p} - (1-p)\cdot\log_2\frac{1}{(1-p)}$$

A BSC kapacitását ábrázoltuk a p bithibarány függvényében az alábbi ábrán. Természetesen semmi meglepő nincs a görbében, hiszen az eredmény igen szoros kapcsolatban van a bináris entrópia-függvénnyel.



7.5. ábra A Bináris Szimmetrikus Csatorna kapacitása