Hírközléselmélet

(Előadásjegyzet)

Készítette:

Czimer Kristóf

Esetleges hibákat a következő e-mailcímen jelezd/jelezze:

czimer.kristof@gmail.com

1. Sztochasztikus Folyamatok

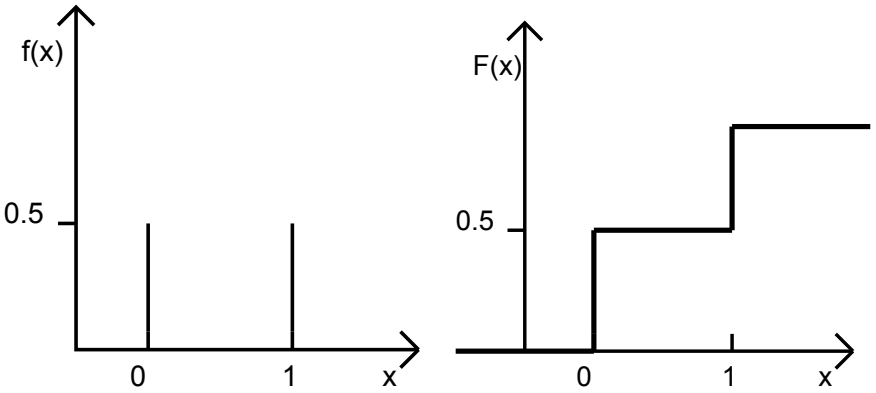
Egy véletlen változót a sűrűségfüggvényével, vagy az eloszlásfüggvényével jellemzünk leggyakrabban. Általános esetben mind az eloszlásfüggvény, mind a sűrűségfüggvény időben változik. A függvények között az alábbi összefüggések állnak fenn.

1.1. Eloszlásfüggvény (Elsőrendű Eloszlásfüggvény)

Az eloszlásfüggvény x pontjának értéke megmutatja, mennyi annak a valószínűsége, hogy a valószínűségi változó értéke a $[-\infty; x]$ intervallumon helyezkedik el.

$$F_{\xi}^{(1)}(x, t_1) = P(x_i < x)$$

$$F_{\xi}^{(1)}(x, t_1) = \int_{-\infty}^{x} f^{(1)}(\xi, t_1) d\xi$$



1.1. ábra. Érmedobás (elsőrendű) sűrűség és eloszlásfüggvénye

1.2. Sűrűségfüggvény (Elsőrendű Sűrűségfüggény)

A sűrűségfüggvény azt mutatja meg, mekkora annak a valószínűsége, hogy a valószínűségi változó értéke az adott értéket veszi fel. Diszkrét eloszlású valószínűségi változóknak szigorú értelemben véve csak általánosított sűsűrésgfüggvénye van (amit a továbbiakban ugyanűgy sűrűségfüggvénynek tekintünk). A sűrűségfüggvény integrálja a teljes tartományon 1.

$$f_{\xi}^{(1)}(x,t_1) = \frac{\partial F_{\xi}^{(1)}(x,t_1)}{\partial x}$$

1.3. Várható érték

Egy véletlen változó folyamat várható értéke:

$$m_{\xi}(t_1) = E_{\xi}\{\xi_{t_1}\} = \int_{-\infty}^{\infty} x \cdot f^{(1)}(x,t_1)dx$$

1. Példa

Ha egy érmét sokszor (végtelenszer) feldobunk, ez egy diszkrét idejű valószínűségi változót ad meg. A fejet, illetve az írást 0-val és 1-gyel jelölve az elsőrendű sűrűségfüggvény, illetve eloszlásfüggvény az alábbi lesz.

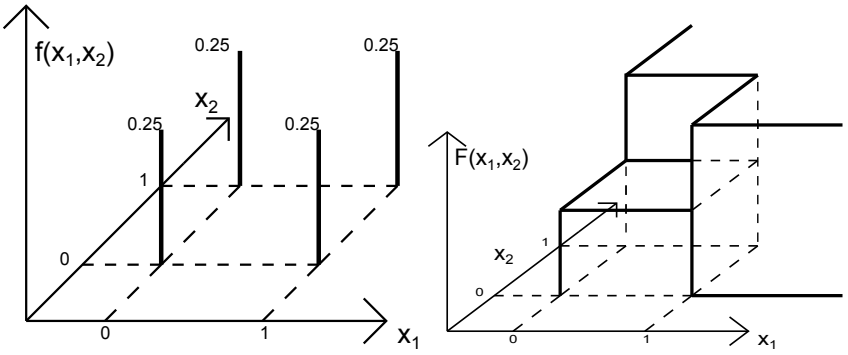
$$f_\xi^{(1)}(x,t_1) = 0.5 \cdot [\delta(x,t_1) + \delta(x-1,t_1)$$

$$F_\xi^{(1)}(x,t_1) = 0.5 \cdot [\epsilon(x,t_1) + \epsilon(x-1,t_1)$$

1.4. Magasabb rendű eloszlásfüggvények és sűrűségfüggvények

A fenti példában a lehetséges kimenetelek száma 2. A pénzérme feldobásával egy kísérletnek két lehetséges kimenetele lehet. Amennyiben a kísérletet kétszer végezzük el, két egymás utáni időpontban, a lehetséges kimenetelek száma 4-re nő (FF,FI,IF,II, azaz 00,01,10,11). Ha ezen kísérletek eloszlását illetve sűrűségfüggvényét ismerjük, többet tudunk a rendszerről, mintha csak egy kísérlet eloszlását illetve sűrűségfüggvényét ismernénk.

Ezen megfontolások alapján $F_\xi^{(n)}(x_1, x_2, ...x_n, t_1, t_2, ...t_n)$ az n-edrendű eloszlásfüggvény, az n-edrendű sűrűségfüggvény $f_\xi^{(n)}(x_1, x_2, ...x_n, t_1, t_2, ...t_n)$, ahol $t_i \in \{T\}$ az időpillanatokat jelöli. A valószínűségi változónkról akkor tudunk a legtöbbet, ha a fenti eloszlás illetve sűrűségfüggvény mindent n-re és minden T-re ismert. Keressük meg a fenti példában szereplő eloszlás másodrendű sűrűségfüggvényét. A lehetséges kimenetelek száma 4 (00,01,10,11), amelyek egyforma valószínűségűek. Ezek alapján a sűrűségfüggvény és az integrálásával kapott eloszlásfüggvény:



1.2. ábra. Érmedobás másodrendű sűrűség és eloszlásfüggvénye

1.5. N-edrendű Stacionaritás

Egy folyamat n-edrendben stacionárius, ha az n-edrendű eloszlásfüggvényére igaz az alábbi összefüggés, azaz ha az minden t_i időpillanatban minden τ-val eltolt pillanatban megegyezik önmagával

$$F_{\xi}^{(n)}(x_1, x_2, ...x_n, t_1, t_2, ...t_n) = F_{\xi}^{(n)}(x_1, x_2, ...x_n, t_1 + \tau, t_2 + \tau, ...t_n + \tau)$$

$$\forall\{T\} - re \text{ és } \forall\tau - ra$$

1.6. Erős Stacionaritás

Egy folyamat erősen stacionárius, ha $\forall n$-re stacionárius. Ez egy meglehetősen erős megkötés, bár az előző példában szereplő pénzfeldobás ilyen[1], általános esetben azonban nem, ezért a gyakorlatban inkább a gyenge stacionaritás fogalmát használják.

1.7. Gyenge Stacionaritás

Egy folyamat gyengén stacionárius, ha a várhatóértéke időfüggetlen és a korrelációs függvénye nem függ az időpontok megválasztásától, csupán az időpillanatok között távolságtól. Például n = 2 esetére:

$$m_{\xi}(t_1) = m_{\xi}$$

$$R(t_1, t_2, \Delta\tau) = R(\Delta\tau)$$

A második egyenletet az eloszlásfüggvényre is megfogalmazhatjuk a következőképpen:

$$F_{\xi}^{(n)}(x_1, x_2, t_1, t_2) = F_{\xi}^{(n)}(x_1, x_2, 0, \Delta t)$$

[1] ha közben az érme tulajdonságai nem változnak

2. Információelmélet

Diszkrét Valószínűségi változók

Az információelmélet alapjait Ralph Hartley és Claude Shannon fektették le. Hartley információról alkotott definíciója a következő volt. Egy olyan rendszerben, amelyben egy D lehetséges értéket felvevő véletlen változó szerepel, a lehetséges állapotok száma D^n.

Hartley úgy gondolta, az információ mértékét úgy kell megválasztani, hogy eggyel növelve a lehetséges értékek számát, a véletlen változó információtartalma szintén 1-gyel növekedjen. Hartley felismerte, hogy ezt logaritmusképzéssel érheti el, hiszen ekkor az exponensben szereplő n szorzótényezőként jelenik meg. A logaritmus alapja tetszőleges a szám lehet. A leggyakrabban alkalmazott logaritmus a *logaritmus dualis (ld)*, azaz a kettes alapú logaritmus. Ezen értelmezés szerint az információ mértékegysége a bit. Az információ definíciója :

$$I = \log_a D^n = n \cdot \log_a D$$
$$[I] = bit$$

Claude Shannon azonban úgy gondolta, a Hartley féle definíció nem tükrözi kellőképpen a valóságot. Például egy zsákban legyen 6 golyó, amelyek közül 3 piros, 3 fehér színű. Egy fehér golyó húzásánál a 1 bit információt nyerünk lévén két lehetség állapot kettes alapú logaritmusa 1. Legyen a 6 golyó közül most 1 piros, 5 pedig fehér. Ha most fehér golyót húzunk nem lepődünk meg, hiszen erre jobban számítottunk, mint a piros színűre. Azaz az események bekövetkezési valószínűsége is információt képvisel, méghozzá minnél kevésbé valószínűbb egy esemény, annál inkább 'meglepődünk' a bekövetkezésénél, azaz annál több információt nyerünk. Ezen megfontolások alapján Shannon az alábbi definíciót vezette be egy diszkrét véletlen változó információtartalmára.

2.1. Információtartalom:

$$I(x_i) = log_2 \frac{1}{p(x_i)}$$

Ahol,

$p(x_i)$ - Az esemény bekövetkezésének valószínűsége.

A gyakorlatban azonban nem is egyetlen esemény információtartalmának, mint inkább az események átlagos információtartalmának, az entrópiának van jelentősége. Az entrópia kifejezése:

2.2. Entrópia:

$$H(X) = \sum_{x_i \in X} p(x_i) \log_2 \frac{1}{p(x_i)}$$

1. Példa

Legyenek 0 és 1 egy forrás által kibocsátandó szimbólumok. A két szimbólum valószínűsége legyen $p_0 = p_1 = 0.5$.

Ekkor a forrás entrópiája:

$$H(X) = 0.5 \cdot \log_2 \frac{1}{0.5} + 0.5 \cdot \log \frac{1}{0.5} = 0.5 + 0.5 = 1$$

2.Példa

Legyen most a $p_0 = 0.25$ és $p_1 = 0.75$. Azaz a forrás most sokkal gyakrabban ad 1-et.

$$H(X) = 0.25 \cdot \log_2 \frac{1}{0.25} + 0.75 \cdot \log \frac{1}{0.75} = 0.8113$$

A forrás entrópiája csökkent. A forrás kevesebb információt tud átlagosan közölni velünk a második esetben, hiszen az 1-esek küldésekor nem 'lepődünk meg', annál inkább a 0-k érkezésekor, ezek azonban ritkábban jönnek.

Az entrópia korlátos függvény. Shannon forráskódolási tétele kimondja, hogy az entrópia mindig pozitív azonban kisebb mint a forrás számossága, azaz a lehetséges kimenetelek száma.

2.3. Az Entrópia korlátossága (Shannon)

$$0 \leq H(X) < log_2 n$$

Ahol,

n - a forrás számossága #X

Bizonyítás

Tegyük fel, hogy

$$H(X) \leq log_2 n$$

átrendezve kapjuk,

$$H(X) - log_2 n \leq 0$$

a második tagot $p(x_i)$-vel súlyozva és összeadva (ezt megtehetjük, mivel a súlyozó együtthatók összege pontosan 1)

$$\sum_{x_i \in X} p(x_i) \log_2 \frac{1}{p(x_i)} - \sum_{x_i \in X} p(x_i) \log_2 n$$

$$\sum_{x_i \in X} p(x_i) \log_2 \frac{1}{p(x_i) \cdot n} \leq 0$$

a logaritmus azonosságait használva,

$$\frac{1}{\ln 2} \sum_{x_i \in X} p(x_i) \ln \frac{1}{p(x_i) \cdot n} \leq 0$$

Az $y = \ln(x)$ függvény az $x = 1$-nél metszi az x tengelyt, és felülről becsülhető az $y = x - 1$ egyenessel. Ezt kihasználva a következő felső becslést adhatunk az a fenti kifejezésre.

$$\frac{1}{\ln 2} \sum_{x_i \in X} p(x_i) \ln \frac{1}{p(x_i) \cdot n} \leq \frac{1}{\ln 2} \sum_{x_i \in X} p(x_i) [\frac{1}{p(x_i) \cdot n} - 1] \leq 0$$

$p(x_i)$-vel egyszerűsítve, az alábbi kifejezést kapjuk. Az első összeadandó tag az összes kimenetelek számának reciproka. Ezt pontosan az esemény kimeneteinek számára kell összegezni, így ez a tag 1-gyel egyenlő. A második tag az egyes események valószínűségeinek összege, ami a teljes halmazon szintén 1-et ad.

$$\frac{1}{\ln 2} [\sum_{x_i \in X} \frac{1}{n} - \sum_{x_i \in X} p(x_i)] = \frac{1}{\ln 2} [1 - 1] = 0 \leq 0$$

q.e.d.

Feltéve, hogy a forrás eloszlása pontosan ismert, az átlagos kódszóhossz bevezetésével Shannon forráskódolási tétele másképpen is megfogalmazható.

2.4. Átlagos kódszóhossz

$$L(x) = \sum_{x_i \in X} p(x_i) \cdot l_i$$

ahol l_i az adott szimbólum kódszóhosszát p_i pedig előfordulási valószínűségét jelöli.

2.5. Shannon forráskódolási tétele

$$H(X) \leq L(x) < H(X) + 1$$

ahol az egyenlőség akkor áll fenn, amennyiben szimbólumok eloszlása 2 hatványai szerinti.

2.6. Kullback Leibler távolság(relatív entrópia)

Ha X egy valószínűségi változó és p(x), q(x) ennek eloszlásfüggvényei a két eloszlásfüggvény relatív entrópiája

$$D(p(x)\|q(x)) = \sum_{x_i \in X} p(x) \log_2 \frac{p(x)}{q(x)}$$

A Kullback Leibler távolság nem kommutativ, azaz

$$D(p(x)\|q(x)) \neq D(q(x)\|p(x))$$

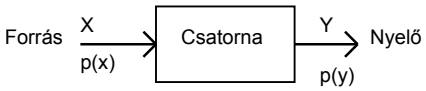
Ha a forrás nem teljesen ismert, akkor forráskódolási tétel a következőképpen írható:

2.7. Shannon forráskódolási tétele becsült forráseloszlásra

$$H(X) + D(p(x)\|q(x)) \leq L(x) < H(X) + D(p(x)\|q(x)) + 1$$

3. Információátvitel

3.1. Átviteli Csatorna



3.3. ábra.

Az információs csatorna fő részei a forrás, a csatorna és a nyelő. A forrás magából $p(x_i)$ eloszlású valószínűségi változót ad ki, a csatorna ebből egy $p(y_i)$ eloszlású véletlen változót generál, amelyek a nyelőre jutnak. A csatorna teremt tehát kapcsolatot az Y és X között. E kapcsolat jellemzőit tárgyalja a következő fejezet.

3.2. Feltételes Entrópia

Y és X kapcsolatát jellemzi a feltételes entrópia

$$H(Y|X) = \sum_{x_i \in X} \sum_{y_i \in Y} p(x_i) p(y_i|x_i) \log_2 \frac{1}{p(y_i|x_i)}$$

Ahol,

$p(x_i)$ - Annak a valószínűsége, hogy a forrás x_i szimbólumot bocsát ki

$p(y_i|x_i)$ - Annak a valószínűsége, hogy a nyelő y_i szimbólumot érzékel feltéve, hogy a forrás x_i szimbólumot bocsátott ki.

Vagy másképpen

$$H(Y|X) = E\{I(y_i|x_i)\}$$

Ahol,

$I(y_i|x_i)$ - A feltételes információ

3.3. Együttes Entrópia

$$H(\chi^n) = \sum_{x_1 \in X_1} \sum_{x_2 \in X_2} ... \sum_{x_n \in X_n} (-p(x_1, x_2...x_n) \cdot \log_2 p(x_1, x_2...x_n))$$

Ahol,

$p(x_1, x_2...x_n)$ - x_i-k együttes bekövetkezési valószínűsége

$\chi^n = \{X_1, X_2...X_n\}$

3.4. Diszkrét Sztochasztikus Folyamat Entrópiája

$$H(\chi) = \lim_{n \to \infty} \frac{1}{n} H(\chi^n)$$

3.5. Kölcsönös Információ

$$I(x_i, y_i) = \log_2 \frac{p(x_i|y_i)}{p(x_i)} = \log_2 \frac{p(y_i|x_i)}{p(y_i)}$$

Érdemes megvizsgálni két speciális esetet. Az első, ha x_i és y_i függetlenek, azaz a forrás független a nyelőtől (teljesen rossz csatorna), akkor $p(y_i|x_i) = p(y_i)$ és így a kölcsönös információ értéke 0. Ha $p(y_i) = p(x_i)$ (tökéletes csatorna), akkor a $p(y_i|x_i) = 1$. A későbbiekben látni fogjuk, hogy a csatornán akkor vihető át a legtöbb információ, ha a forrás entrópiája maximális. Így például $p(x_i) = 0.5$, és $p(y_i) = 0.5$ esetén a kölcsönös információ 1 bit.

3.6. Átlagos Kölcsönös Információ

$$I(X, Y) = \sum_{x_i \in X} \sum_{y_i \in Y} p(x_i, y_i) \cdot I(x_i, y_i)$$

$$I(X,Y) = \sum_{x_i \in X} \sum_{y_i \in Y} p(x_i, y_i) \log_2 \frac{p(x_i, y_i)}{p(x_i) \cdot (y_i)}$$

azaz x,y együttes eloszlásának Kullback-Leibler távolsága a két eloszlás szorzatától

$$I(X,Y) = D(p(x,y) \| p(x) \cdot p(y))$$

Valószínűségszámításból ismert, hogy két eloszlás együttes eloszlása a két eloszlás szorzatát adja, amennyiben a két eloszlás egymástól független. Jelen esetben ez azt jelenti, hogy $p(x,y) = p(x) \cdot p(y)$ ami pedig az Átlagos kölcsönös információt 0-val teszi egyenlővé.

3.7. A Posteriori Entrópia

Az átlagos kölcsönös entrópia kifejezését másképp felírva az indexeket immáron elhagyva a rövidebb jelölés érdekében,

$$I(X,Y) = \sum_{x \in X} \sum_{y \in Y} p(x,y) \log_2 \frac{p(x,y)}{p(x) \cdot (y)} = \sum_{x \in X} \sum_{y \in Y} p(x,y) [\log_2 \frac{1}{p(x)} - \log_2 \frac{1}{p(x|y)}]$$

$$= \sum_{x \in X} \sum_{y \in Y} p(x) \cdot p(y|x) \log_2 \frac{1}{p(x)} - \sum_{x \in X} \sum_{y \in Y} p(x,y) \log_2 \frac{1}{p(x|y)}$$

A különbség első tagja a nem más mint a forrás entrópiája, mivel

$$\sum_{x \in X} \sum_{y \in Y} p(x) \cdot p(y|x) \log_2 \frac{1}{p(x)} = \sum_{x \in X} p(x) \log_2 \frac{1}{p(x)} \sum_{y \in Y} p(y|x)$$

$$= H(X) \cdot 1 = H(X)$$

A különbség második tagja pedig az un. A posteriori entrópia, amely azt fejezi ki, hogy az Y megfigyelésével mekkora a bizonytalanságunk X-ben

$$H(X|Y) = \sum_{x \in X} \sum_{y \in Y} p(x,y) \log_2 \frac{1}{p(x|y)}$$

Így a kölcsönös információ a következőképpen írható fel

$$I(X,Y) = H(X) - H(X|Y)$$

3.8. Csatornakapacitás

A csatornakapacitás definíció szerint nem más mint az átlagos kölcsönös információ maximuma p(x) szerint.

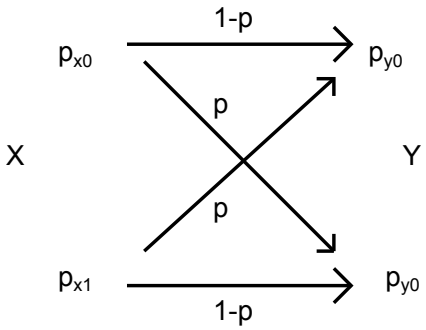
$$C = \max_{p(x)}\{I(X,Y)\}$$

3.9. Shannon II. tétele

Egy H(X) forrás entrópiával, C kapacitással rendelkező csatornára minden P_ϵ hibavalószínűséghez létezik $\Omega_c(x) = x'$ transzformáció (kódolás) $H(X) \leq C$ esetén.

1.Példa

Bináris Szimmetrikus Csatorna (BSC)



3.4. ábra. BSC

A forrás azonos valószjnűséggel ad ki magából 0-t illetve 1-et $p_{x0} = p_{x1} = 0.5$, valamint definiálunk egy hibázási valószjnűséget, amelyet p-vel jelölünk. Ekkor a kimeneten a 0, illettve 1 detekciók valószínűségei:

$$p_{y0} = p_{x0} \cdot (1-p) + p_{x1} \cdot p = 0.5$$

$$p_{y1} = p_{x1} \cdot (1-p) + p_{x0} \cdot p = 0.5$$

Azaz a kimeneten lévő szimbólum detekciók valószjnűsége nem függ a hibázási valószínűségektől. Ez azért van mert ugyanannyival több 1-est érzékelünk 0 helyett, mint fordítva, lévén a csatorna szimmetrikus. A kölcsönös információ kifejezése:

$$I(X,Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$$

$$H(Y) = \sum_{y_i \in Y} p(y_i) \cdot \log_2 \frac{1}{p(y_i)} = p_{y0} \cdot \log_2 \frac{1}{p_{y0}} + p_{y1} \cdot \log_2 \frac{1}{p_{y1}}$$

$$H(Y) = 0.5 + 0.5 = 1$$

$$H(Y|X) = \sum_{x_i} p(x_i) \sum_{y_i} p(y_i|x_i) \log_2 \frac{1}{p(y_i|x_i)}$$

$$= p_{x0}[(1-p)\log_2 \frac{1}{1-p} + p \log_2 \frac{1}{p}] + (1-p_{x0})[(1-p)\log_2 \frac{1}{1-p} + p \log_2 \frac{1}{p}]$$

$$= [(1-p)\log_2 \frac{1}{1-p} + p \log_2 \frac{1}{p}]$$

Shannon első tétele szerint az entrópia korlátos. H(Y) kifejezését megfigyelve határértékszámítással adódik, hogy az entrópia kifejezése $p_y = 0$ és $p_y = 1$ értékeire 0. Ahol p_y jelöli p_{y0}-t (vagy p_{y1}-et) ennek megfelelően $p_{y1} = 1 - p_y$ (vagy $p_{y0} = 1 - p_y$. Az entrópia tehát maximális $p_y = 0.5$-nél, értéke 1. és zérus $p_y = 0$ valamint $p_y = 1$-nél. Ezáltal a bináris szimmetrikus csatorna kapacitása.

$$C = 1 - H(Y|X)$$

Ahol $H(Y|X)$ csak a hibavalószínűségtől függő tag.

3.10. Diszkrét Memóriamentes csatorna (DMC) Additív Gauss Zaj (AWGN)

A diszkrét memóriamentes csatornát a következőkben az additív fehér Gauss zaj esetére fogjuk vizsgálni. A csatorna modellje így egy összeadó, melynek egyik bemenete a jel a másik pedig a zaj mintái. A zaj mintáinak eloszlásfüggvénye Gaussi. A nulla várható értékű sűrűségfüggvényt a 3.1 egyenlet adja meg.

$$f_n(x) = \frac{1}{\sqrt{2\pi\sigma_n^2}} \exp[\frac{-(x)^2}{2\sigma_n^2}] \tag{3.1}$$

Frekvenciatartományban a fehér zaj jelzővel olyan zajt illetünk, melynek spektrális sűrűségfüggvénye egyenletes, azaz minden frekvencián egyforma, Gauss zaj esetében $\frac{N_0}{2}$ értékű ahol $N_0 = k \cdot T_\Sigma$ a Boltzmann állandó és az összesített redukált zajhőmérséklet szorzata. A sztochasztikus jelek elméletéből az is ismert, hogy a Zaj teljesítménye megegyezik szórásnégyzetével. $P_z = \sigma^2$

3.11. Differenciális Entrópia (folytonos eloszlásra)

$$H(X) = -\int_x f_x(x) \log_2 f_x(x) dx \tag{3.2}$$

1.Példa

GWN entrópiája

$$H(X)_{gauss} = \frac{1}{2} \log_2(2\pi e\sigma^2) \tag{3.3}$$

2.Példa

$\frac{x}{2}$ hosszú impulzus entrópiája

$$H(X)_{imp} = -1 \tag{3.4}$$

A fentiekből látható, hogy a definíció miatt az entrópia lehet negatív is.

3.12. Az AWGN csatorna kapacitása

Az előző fejezetekben láttuk, hogy a csatorna kapacitása az átlagos kölcsönös információ maximuma, amely felírható a feltételes entrópiával is. Ha figyelembe vesszük, hogy additív fehér gauss zaj esetén, $H(Y) = H(X + N)$ és $H(Y|X) = H(N)$ ahol H(N) a zaj, míg H(X+N) a jel és a zaj együttes entrópiája, akkor Gaussi jelet feltételezve a csatorna kapacitása a 3.8 egyenlet szerinti kifejezés lesz.

$$C_{max} = \max_{p(x)}\{H(Y) - H(Y|X)\} \tag{3.5}$$

$$C_{max} = \max_{p(x)}\{H(X + N) - H(N)\} \tag{3.6}$$

$$C_{max} = \frac{1}{2}\log_2(2\pi e(\sigma_n^2 + \sigma_j^2) - \frac{1}{2}\log_2(2\pi e(\sigma_n^2) \tag{3.7}$$

$$C_{max} = \frac{1}{2}\log_2(2\pi e(1 + \frac{\sigma_j^2}{\sigma_n^2}) \tag{3.8}$$

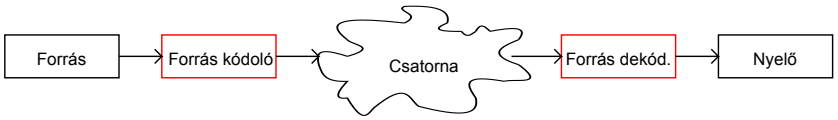
A logaritmusban megjelenő kifejezés, a $\frac{\sigma_j^2}{\sigma_n^2}$ az un. jel zaj viszony. A fenti levezetés azt feltételezi, hogy végtelen sávszélesség áll rendelkezésre. A valóságban azonban adott sávszélességgel áll rendelkezésre, ekkor a 3.9 egyenlet szerinti kifejezés érvényes.

$$C_{max} = B\log_2(1 + \frac{P}{B \cdot N_0}) \tag{3.9}$$

4. Forráskódolás

4.1. A forráskódolás feladata

A forráskódolás feladata a p(x) eloszlással rendelkező x_i forrásszimbólumok l_i kódszimbólumokhoz való kölcsönösen egyértelmű hozzárendelése. A forráskódolás csökkenteni igyekszik az átvitt információ költségét. A nagy valószínűséggel adott szimbólumokhoz rövidebb kódokat rendel, így csökkenti az átlagos kódszóhosszt.



4.5. ábra. Információ átvitele

4.2. Átlagos kódszóhossz

$$L_x = \sum_x p(x) l_i \tag{4.10}$$

Az átlagos kódszóhossz korlátos, méghozzá nagyobb a forrás entrópiájánál, de legfeljebb a forrás entrópiája + 1.

$$H(X) \leq L_x < H(X) + 1 \tag{4.11}$$

4.3. Pillanatkód

A pillanatkód olyan kód, amely a vétel pillanatában dekódolható. Például ilyen kód a Prefix kód

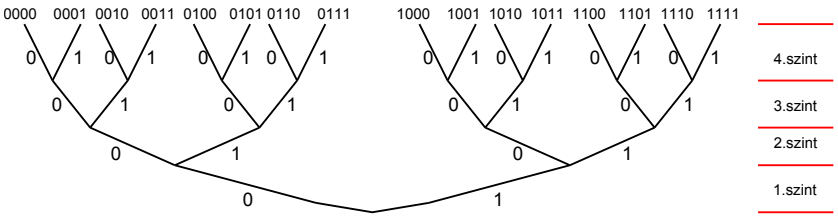
4.4. Prefix és Postfix kódok

Az egyik gyakori pillanatkód a prefix kód. Ebben a kódban egyik kódszó sem kezdődik ugyanúgy, mint egy másik. Legyen például a = 0; b = 10; c

= 11. Ekkor a 01110101... kódsorozat egyféleképpen dekódolható, méghozzá a,c,b,b,a,... az a után jövő egyes lehet egy b vagy egy c. Bár ezt a kódszót még nem tudjuk, az összes előtte lévőt igen. A postfix kód nem pillanatkód. Ebben a kódban egyik kódszó sem végződik úgy, mint egy másik. Legyen például a = 1; b = 10; c = 00. Ekkor a következő kódsorozat 111000 csak egyféleképpen dekódolható, méghozzá a,a,b,c. Ha azonban még egy bit érkezik nevezetesen egy 0, Akkor a dekódolt szimbólumok megváltoznak, tehát 1110000-hoz a,a,a,c,c tartozik. A postfix kódnál az utolsó bitet tudni kell, hiszen a kódolásnál hátulról indulunk. A kód tehát kölcsönösen egyértelmű, de nem pillanatkód.

4.5. Kódkonstrukció Bináris fával

A bináris fával történő kódkonstrukciónál minden elágazásnál egy további bitet adunk az eddigiekhez. Az ágak jelölik a bitek értékét a levelek (végelemek) pedig a kódok. Az így konstruált kód pillanatkód lesz, hiszen az elágazások miatt semelyik kód nem kezdődhet úgy mint egy másik. A lehetséges kódok száma ezzel a módszerrel L bit esetén éppen 2^L. Ez a kód azonban nem ad optimális kódszóhosszat, mivel minden kód ugyanolyan hosszú. Az optimális kód megtalálásához csökkenteni kell azon kódszavak hosszát, amelyek gyakrabban fordulnak elő.



4.6. ábra. Bináris fa

4.6. A Kraft egyenlőtlenség

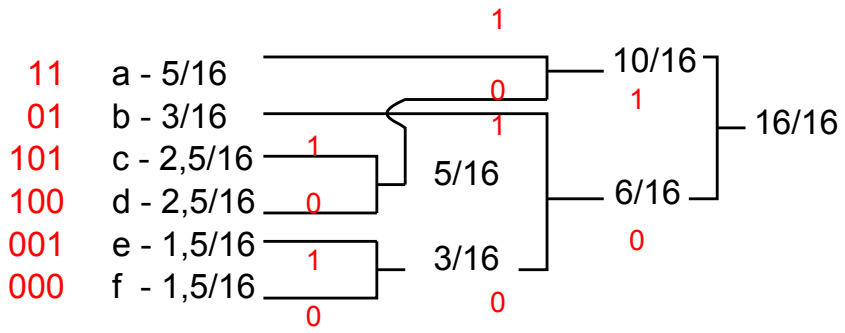
A bináris fát szintekre oszthatjuk minden elágazásnál. Ha az i. szinten elvágunk egy ágat, akkor rövidebb kódot kapunk, melynek hossza éppen i. Ekkor az elvágott ággal egy olyan bináris részfát távolítottunk el, melynek 2^{L-i} szintje van. A metszés persze történhet a levélelemeknél is, ilyenkor

nem csökkentjük a teljes fát. Ebből tehát az látszik, hogy a fán elhelyezhető kódszavak maximális száma 2^L. Ez az un. Kraft egyenlőtlenség bináris fára.

$$2^L \geq \sum_{i=1}^{m} 2^{L-i} \tag{4.12}$$

4.7. Huffman kódolás

A Huffman kódolásnál a forrás eloszlásában a két aktuálisan legkisebb valószínűségű szimbólumot összevonjuk egy kompozit szimbólumba. A végén az összevonásokkal egy bináris fát kapunk. A kódokat az előző fejezetben ismertetett eljárással jelöljük ki, Az alábbi példában felfelé 1-es lefelé 0 kódot alkalmaztunk. Az irányhoz a kód hozzárendelése bináris esetben azonban tetszőleges, akár szintenként más módszert is alkalmazhatunk, azaz a fa "megcsavarható".



4.7. ábra. Huffman kódolás

4.8. Kódhatékonyság

Egy kód hatékonyságát az entrópiához viszonyítjuk. A kód hatékonysága nem más, mint a forrás entrópiájának és az átlagos kódszóhossz hányadosa. A kód hatékonysága 100%, ha a forrásszimbólumok A-priori eloszlása 2 negatív hatványai szerinti.

$$h = \frac{H(X)}{L_x} \tag{4.13}$$

1.Példa

Számoljuk ki 4.7 ábrán megadott eloszlás és a hozzá tartozó kód hatékonyságát.

Az átlagos kódszóhossz:

$L_x = 2 \cdot (\frac{5}{16} + \frac{3}{16}) + 3 \cdot (\frac{2,5}{16} + \frac{2,5}{16} + \frac{1,5}{16} + \frac{1,5}{16} = 2,5$

Az eloszlás entrópiája

$H(X) = \frac{5}{16} \cdot \log_2 \frac{5}{16} + \frac{3}{16} \cdot \log_2 \frac{3}{16} + \frac{5}{16} \cdot \log_2 \frac{2,5}{16} + \frac{3}{16} \cdot \log_2 \frac{1,5}{16} = 2,45$

A kód hatékonysága tehát

$h = \frac{H(X)}{L_x} = 2,45/2,5 = 98,2\%$

2.Példa

Legyen a - 0.5; b - 0.25; c - 0.125; d - 0.125 a forrás eloszlása. Ekkor a Huffman kódolás szerint a kódok: 1; 01; 001; 000. Az eloszlás 2 hatványai szerinti, ilyenkor pedig az Entrópia megegyezik az átlagos kódszóhosszal. $H(X) = 1,75 = L_x$ $h = 100\%$.

3.Példa

Legyen a - 0.25; b - 0.25; c - 0.25; d - 0.25, azaz a forrás egyenletes eloszlású. Ekkor a hozzárendelt Huffman kód például 00; 01; 10; 11. A forrás entrópiája $H(X) = 4 \cdot 0,25 \cdot log_2 \frac{1}{0,25} = 2$. Az átlagos kódszóhossz $L_x = 4 \cdot 0.25 \cdot 2 = 2$. A kód hatékonysága h = 100%.

4.9. Forráskiterjesztés

Ha a forrás eloszlása nagyon messze van az egyenletes eloszlástól, azaz ha az entrópiája kicsi, akkor a Huffman kód hatékonysága alacsony. Legyen például a forrás eloszlása a - 1/16; b - 1/16; c - 14/16. Az előző képleteket alkalmazva H(X) = 0.67, L_x = 1,12. A kód hatékonysága tehát $\approx 59\%$.

Ilyen esetben célszerű lehet az eredeti szimbólumok {a,b,c} helyett {aa, ab, ac, ba, bb, bc, ca, cb, cc} szimbólumokat kódolni. Ekkor ugyanis a forrásszimbólumok eloszlása egyenletesebb lesz. Feltételezve a szimbólumok függetlenségét a két szimbólum egymás utáni észlelésének valószínűsége a két

szimbólum valószínűségének szorzata. A forrás eloszlása így $P(x_i) = \{1/256$ $1/256$ $14/256$ $1/256$ $1/256$ $14/256$ $14/256$ $14/256$ $196/256\}$. Ezt nevezzük forrás kiterjesztésnek. Ezzel a módszerrel ténylegesen csökkenthető az átlagos kódszóhossz. Hiszen a kiterjesztett forráseloszlásra érvényes

$$H(A_{kit}) \leq L_{A_{kit}} < H(A_{kit}) + 1 \tag{4.14}$$

Ahol $H(A_{kit})$ az eredeti forrás entrópiájának N-szerese

$$N \cdot H(A) \leq L_{A_{kit}} < N \cdot H(A) + 1 \tag{4.15}$$

Ebből az egy szimbólumra eső kódbitek számához N-el kell osztani

$$H(A) \leq L_A < H(A) + \frac{1}{N} \tag{4.16}$$

A fenti levezetés azt demonstrálja, hogy az átlagos kódszóhossz tetszőlegesen megközelítheti a forrás entrópiáját. Továbbá az előzőekből az is látható, hogy a forrás eloszlásának nem pontos ismerete nem befolyásolja jelentősen a kódolás hatékonyságát. Ha például az első példában vett eloszlásban a két 1,5/16 valószínűségű szimbólumot 1/16-ra ls 2/16-ra változtatjuk a kódolás még mindig azonos módon zajlik le.

További fontos észrevétel, hogy egyenletes eloszlásnál fölösleges forráskiterjesztést alkalmazni, hiszen ekkor a forrás entrópiája maximális. Továbbá a kettő hatványai szerinti eloszlásnál is fölösleges e módszer alkalmazása, hiszen ekkor a Huffman kódolás 100%-os hatékonyságú kódot ad.

4.10. Aritmetikai kódolás

"Ez a kódolási módszer hasonlít a Huffman-kódhoz, amennyiben a forráseloszlás a priori ismeretét igényli. Az algoritmus alapötlete az, hogy minden forrásszimbólumnak a valószínűsége arányában megfeleltetjük a [0,1) intervallum valamekkora részét. Ha például A=a, b, c=0.4, 0.4, 0.2, akkor három részintervallumot képezünk: [0, 0.4), [0.4, 0.8) és [0.8, 1).

Az első szimbólum (legyen például b) kiválasztja valamelyik részintervallumot (jelen esetben a [0.4, 0.8)-at). Ezután már ezt tekintjük alap-

intervallumnak, és ugyanúgy felosztjuk részintervallumokra (a valószínűségek arányában), mint a [0,1) intervallumot. A példa szerint azt kapjuk, hogy [0.4, 0.56), [0.56, 0.72) és [0.72, 0.8). Ezek közül a második szimbólum (például c) választ egyet (a [0.72, 0.8)-at), és így tovább. A feldolgozott szimbólumok számával az aktuális részintervallum egyre szűkül, ha kis valószínűségű szimbólumok jönnek, akkor gyorsabban. Végül, ha már nincs több kódolandó szimbólumunk, akkor az utolsó részintervallumból választott bármelyik valós szám meghatározza az egész addig kódolt sorozatot."[1]

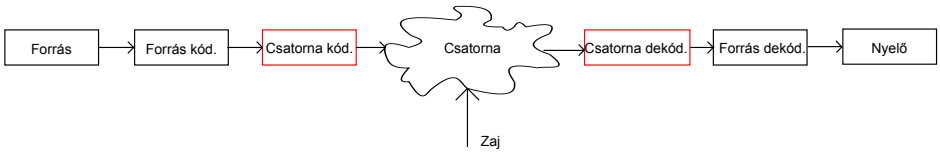
Ez a kód úgy teljesíti az átlagos kódszóhosszra támasztott követelményeket, hogy egy valószínű szimbolumsorozathoz nagyobb intervallum tartozik, így nagyobb az esélye, hogy egy rövid kettedes törtet találunk, míg a kevésbé valószínű szimbolumsorozathoz rövidebb intervallum és így hosszabb kettedes tört tartozik.

"A dekódolásnál problémát okoz, hogy ha a szimbólumok egy adott hosszúságú sorozatát kódoljuk mindig egy kódszóba, akkor mi garantálja azt, hogy az így kapott változó hosszúságú kód megfejthető lesz? Ha viszont azonos hosszúságú kódszavakat alakítunk ki, azaz akkor hagyjuk abba a kódolást, mikor egy adott kettedestört-hosszat elértünk, akkor honnan tudja a dekóder, hogy mikor kell leállni? Erre a problémára egy új STOP szimbólum beiktatása lehet a megoldás. Ezt a forrásABC egyéb szimbólumaival azonos módon kell kezelni, valószínűséget kell hozzá rendelni."[1]

5. Csatornakódolás

5.1. Csatornakódolás alapjai

A csatorna kódolás feladata, hogy a forrás kimenetén lévő üzenethez redundáns információt fűzzön hozzá, ezzel lehetővé tegye a zajos csatorna okozta hibák detektálását és javítását. Az optimális forráskódoló kimenetén egyenletes eloszlású korrelálatlan üzenetek vannak, azaz az entrópia maximális, és az üzenetek redundancia mentesek.



5.8. ábra. Információ átvitel zajos csatornán

Jelölje $\underline{u}$ az **U** üzenettér egy elemét, amelyben egy szimbólum hossza m és a kódolt üzenet hossza K. Tehát $\underline{u} = [u_1 u_2 ... u_K]$ egy K hosszú vektor, amelynek u_i elemei bináris esetben például 0 illetve 1 értéket vehetnek fel (m = 2). Jelölje $\underline{c}$ a **C** kódtér egy elemét, amelyben egy szimbólum hossza q és a kódolt üzenet hossza N. Tehát $\underline{c} = [c_1 c_2 ... c_N]$ egy N hosszú vektor, amelynek c_i elemei bináris esetben 0 illetve 1 értéket vehetnek fel (q = 2). Ekkor a kódolás Ω_c egy olyan hozzárendelés, amely az $\underline{u}$ vektort $\underline{c}$ vektorba viszi át. $\Omega_c(\underline{u}) = \underline{c}$.

5.2. Hamming távolság

Ha $\underline{x}$ és $\underline{y}$ két kódot jelöl, akkor a

$$d(\underline{x}, \underline{y}) = \sum_{i=0}^{n} \chi(x_i \neq y_i) \tag{5.17}$$

összefüggés az $\underline{x}$ és $\underline{y}$ vektor Hamming távolsága, ahol χ az un. igazságfüggvény: értéke 1, ha a mögötte lévő kifejezés igaz, és 0, amennyiben a mögötte lévő kifejezés hamis.

5.3. Minimális Hamming távolság

A Hamming távolság alapján definiálhatjuk a minimális Hamming távolságot is. Ez nem más mint két kódvektor kódszavanként vett hamming távolságainak minimuma.

$$d_{min} = \min\{d(\underline{c}, \underline{c}')\} \tag{5.18}$$

5.4. A dekódolás feladata

A dekódolás két részre osztható. Az első rész a demodulátor kimenetén megjelenő $\underline{v}$ szimbólumhoz a hozzá legközelebb eső $\underline{c}$' érvényes kódszó megkeresése. A második lépés az $\Omega^{-1}(\underline{c}') = \underline{u}$ üzenetvektor előállítása. A dekódolás **triviális**, amennyiben $\underline{v} = \underline{c}$, azaz az adott és vett üzenetvektor megegyezik, **megoldhatatlan**, ha $\underline{v} = \underline{c}' \neq \underline{c}$, tehát olyan érvényes kód, amely nem az adó oldali kódszó és **lehetséges**, amennyiben $\underline{v} \neq \underline{c}'$.

5.5. A jelezhető hibák száma

Ha egy kódban az átvitel során, a minimális Hamming távolsággal megegyező hiba keletkezik, a legrosszabb esetben az egyik kód átcsúszik a másikba. Azonban ha ennél eggyel kevesebb hiba történik, érvénytelen kódot kapunk, amely jelzi a hibát. Egy kód által jelezhető hibák száma tehát, a kódszavak minimális Hamming távolságánál eggyel kisebb érték.

$$t_{jel} = d_{min} - 1 \tag{5.19}$$

5.6. A javítható hibák száma

A javítható hibák száma, az a szám, ahány bit meghibásodása esetén a dekódoló még el tudja dönteni, melyik az a kódszó, amelyet az adó oldalon kibocsátottak.

$$t_{jav} = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor \tag{5.20}$$

5.7. Törléses hibák

Egyes vevőberendezésekben a demodulátor képes jelezni, ha egy bit értékében bizonytalan. Ekkor a demodulátor plusz információt bocsát a dekódoló rendelkezésre, miszerint megmondja a bit pozícióját, ahol a meghibásodás történhetett. Ezen pluszinformáció segítségével a dekódoló több hibát képes javítani.

$$t_{tor} = d_{min} - 1 \tag{5.21}$$

Legyen például $\underline{c}$ = [000 110 101 011], ekkor a minimális Hamming távolság 2. A fenti összefüggés szerint a javítható hibák száma 1. Legyen a demodulátor kimenetén megjelenő érték x01. Egyetlen olyan érték létezik, amelynél a 2. és 3. pozícióban 0, illetve 1 érték szerepel ez pedig az 101. Hasonlóan 1x1 és 10x esetén is helyesen dekódolható a kódszó.

5.8. Singleton-korlát

Legyen m = q, ekkor a lehetséges kódolatlan üzenetek száma $m^k = M$. A kérdés az, mennyi lehet a kódolatlan üzenetek száma, adott kód szimbólumhossz (q), kódszóhossz (N) és minimális Hamming távolság mellett? Ezutóbbi a kód hibajavító képességére tesz megkötést. A választ a Singleton korlát 5.22 egyenlet szerinti kifejezése adja.

$$M \leq q^{N - d_{min} + 1} \tag{5.22}$$

Bizonyítás

Nyilvánvaló, hogy az üzenetek száma kisebb vagy egyenlő, mint az előállítható üzenetek száma m^K és q = m, azaz

$$M \leq q^K \tag{5.23}$$

Az is belátható, hogy a minimális Hamming távolság kisebb, mint 1 + a bővítési faktor, amellyel a kódszóhossz nagyobb mint az üzenethossz. Az 1 onnan jön, hogy az 1 hosszúságú kódszavak Hamming távolsága 1.

$$d_{min} \leq 1 + N - K \tag{5.24}$$

A fenti egyenletet átrendezve

$$K \leq N - d_{min} + 1 \tag{5.25}$$

Ezt az 5.23 egyenletbe behelyettesítve éppen a 5.22 egyenlet szerinti Singleton korlátot kapjuk.

5.9. Hamming-korlát

A Hamming korlát arra a kérdésre ad választ, hogy egy adott t_{jav} hibajavító képességgel rendelkező kódhoz milyen N, K illetve q érték választható.

Azon pontok száma, amelyek egy adott kódtól maximum t_{jav} távolságra vannak

$$\nu_d = \sum_{i=0}^{t_{jav}} \binom{N}{i} (q-1)^i \tag{5.26}$$

Például i = 1 esetén az N dimenziós üzenettérben a szomszédos kódok száma N. A szomszédos kódok összesen N darab különböző pozícióban q-1 más értéket vehetnek fel (mint a viszonyítási pontban levő kód). Így a t_{jav} = 1 javító képességű kódok száma $N \cdot (q-1)$. Hasonlóan i = 2 -re azon pontok száma amelyek 2 értékben térnek el $\binom{N}{2}$, hiszen N-ből 2 értéket kell kiválasztani, amelyeket megváltoztatunk. Az értékek pedig összesen $(q-1)^2$ más értéket vehetnek fel, és így tovább i nagyobb értékeire.

A Hamming korlát kifejezése tehát

$$m^K \cdot \sum_{i=0}^{t_{jav}} \binom{N}{i} (q-1)^i \leq q^N \tag{5.27}$$

Speciális esetben m = q

$$\sum_{i=0}^{t_{jav}} \binom{N}{i} (q-1)^i \leq q^{N-K} \tag{5.28}$$

Bináris üzenet és kód szimbólumokra m = q = 2

$$\sum_{i=0}^{t_{jav}} \binom{N}{i} \leq 2^{N-K} \tag{5.29}$$

5.10. Kód-perfekció

Egy kód perfekt, a Hamming korlát kifejezésében az egyenlőség teljesül. Ez bináris esetben szemléletesen azt jelenti, hogy az N dimenziós kódtérben a legalább t_{jav} hibát javítani képes kódok száma pontosan kettő azon hatványa, amennyivel hosszabb a kód mint az üzenet. Másképpen fogalmazva a kódszóhossz bővítésével nyert kódok száma ugyanannyi, mint a legalább t_{jav} hibát javítani képes kódok száma.

$$\sum_{i=0}^{t_{jav}} \binom{N}{i} = 2^{N-K} \tag{5.30}$$

K	$t_{jav} = 1$	$t_{jav} = 2$
1	3	5
2	7	-
4	7	-
11	15	-
57	63	-
78	-	90 !!

5.1. táblázat. Perfekt kódok m = q = 2

5.11. Kódsebesség

A perfekt kódok közül azokat részesítjük előnyben, amelyek azonos t_{jav} mellett az adott üzenethez a legkevesebb redundáns bitet fűzik hozzá. Ennek

mérőszáma az un. kódsebesség.

$$R = \frac{K}{N} \tag{5.31}$$

A 5.10 táblázat alapján ez a kód a 78/90-es lenne de ilyen kód nem létezik. Hogyan lehetséges ez? A Hamming korlát csak szükséges feltétel, de nem elégséges.

6. Lineáris Kódok

6.1. Bináris Lineáris Kódok

Lineárisnak nevezünk egy bináris kódteret, ha a bináris összeadás nem vezet ki a térből. Például ilyen kódtér a 000,110,101,011 kódtér, hiszen bármely kettőt modulo kettő összeadva olyan értéket kapunk, amely a lineáris tér eleme. Ellenpélda a 111,001,010,100. Bár ezek minimális Hamming távolsága érdekes módon szintén 2, például az 111 és a 001 modulo 2 összege 110, amely nem a tér eleme.

A lineáris tér bázisának nevezzük annak lineáris független generátorrendszerét, azaz olyan lineárisan független vektorok összességét, amelyek lineárkombinációjával a tér elemei előállíthatóak. A fenti példában a 000 vektoron kívül bármely kettő kiválasztható a tér bázisának.

6.2. Bináris Hamming kód

Az 1 bitet javítani képes, lineáris, perfekt (blokk-) kódokat Hamming kódnak nevezzük. Ha ezen felül a kód bináris akkor Bináris Hamming kódnak nevezzük. A Hamming kódok maximális kódsebességgel rendelkeznek, az azonos hibajavító képességgel rendelkező kódok közül.

6.3. Generátormátrix

A generátormátrix a bináris lineáris tér bázisaiból képzett mátrix, a fenti példából bázisnak választva 110 és 101 vektorokat, a generátormátrix

$$\underline{\underline{G}} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

.

A generátormátrix az üzenettér eleméhez a kódtér egy elemét rendeli. K sora és N oszlopa van.

$$\underline{c} = \underline{u} \cdot \underline{\underline{G}} \tag{6.32}$$

A fenti példát folytatva $\underline{u} = [00\ 01\ 10\ 11]$ üzenetvektort $\underline{\underline{G}}$ generátormátrixszal megszorozva,

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

.

6.4. Paritás Ellenőrző Mátrix

Vezessük be $\underline{\underline{H}}$ paritásellenőrző mátrixot a következőképpen

$$\underline{\underline{G}} \cdot \underline{\underline{H}}^T = \underline{\underline{0}} \tag{6.33}$$

Ekkor nyilván

$$\underline{u} \cdot \underline{\underline{G}} \cdot \underline{\underline{H}}^T = \underline{0} \tag{6.34}$$

Ebből pedig

$$\underline{c} \cdot \underline{\underline{H}}^T = \underline{0} \tag{6.35}$$

Valamint kihasználva hogy $\underline{c} \cdot \underline{\underline{H}}^T = \underline{\underline{H}} \cdot \underline{c}^T$

$$\underline{\underline{H}} \cdot \underline{c}^T = \underline{0} \tag{6.36}$$

6.5. Szindróma vektor

Ha a kódvektor helyett, a demodulátor kimenetén megjelenő vektort helyettesítjük 6.36 egyenletbe, akkor az un. Szindróma vektort kapjuk. A hibavektor $\underline{e} = \underline{v} - \underline{c}$ kifejezését használva, mindkét oldalon beszorozva $\underline{\underline{H}}$-val a szindróma vektor:

$$\underline{s}^T = \underline{\underline{H}} \cdot \underline{v}^T - \underline{\underline{H}} \cdot \underline{c}^T = \underline{\underline{H}} \cdot \underline{e}^T \tag{6.37}$$

Mivel többes hiba is előfordulhat az átvitel során, a szindróma vektor nem egyértelmű.

6.6. Szisztematikus kódkeresés

Egy N, K paraméterű lineáris kód szisztematikus, ha minden kódszavára igaz, hogy annak első vagy utolsó N-K szimbólumát elhagyva éppen a neki megfelelő K hosszúságú üzenetet kapjuk, más szavakkal a K hosszúságú üzenetet egészítjük ki N-K karakterrel. Egy kód szisztematikus tehát, ha a generátormátrixa elején vagy végén tartalmazza az egységmátrixot.

Szisztematikus kód esetén a kódolásban szereplő Ω_c művelet inverzének elvégzése így tulajdonképpen a kódszó egy részének (elejének vagy végének) elhagyását jelenti.

Szisztematikus kód esetén a generátor mátrix a 6.38 egyenlet szerinti alakú

$$\underline{\underline{G}} = [\underline{I}, \underline{\underline{P}}] \quad vagy \quad \underline{\underline{G}} = [\underline{\underline{P}}, \underline{I}] \tag{6.38}$$

Ahol $\underline{\underline{I}}$ KxK-s egységmátrix, $\underline{\underline{P}}$ pedig egy Kx(N-K)-s mátrix. A paritásellenőrző mátrix kifejezése pedig rendre

$$\underline{\underline{H}} = [-\underline{\underline{P}}^T, \underline{\underline{I}}] \quad vagy \quad \underline{\underline{H}} = [\underline{\underline{I}}, -\underline{\underline{P}}^T] \tag{6.39}$$

Ahol $\underline{\underline{P}}^T$ egy (N-K)xK-s mátrix és $\underline{\underline{I}}$ (N-K)x(N-K)-s egységmátrix,. Bináris esetben igaz még, hogy -$\underline{\underline{P}}^T$ = $\underline{\underline{P}}^T$. A továbbiakban az első alakot fogjuk használni.

1.Példa

Határozzuk meg annak a szisztematikus kódnak a Paritásmátrixát melynek Generátorrendszere

$$\underline{\underline{G}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

N = 3, K = 2; Tehát $\underline{\underline{I}}$: 2x2-es egységmátrix $\underline{\underline{P}}$ pedig 2x1-es mátrix, tehát oszlopvektor. Így

$$\underline{\underline{H}} = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

például a $\underline{v}$ = 001-hez tartozó szindrómavektor így $\underline{s}^T = 1$

2.Példa

$$\underline{\underline{G}} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

N = 5, K = 2; Tehát $\underline{\underline{I}}$: 2x2-es egységmátrix $\underline{\underline{P}}$ pedig 2x3-es mátrix. A paritásmátrixban szereplő egységmátrix így 3x3-as.

$$\underline{\underline{H}} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

A szindrómavektor $\underline{v}$ = 10000 -hoz például,

$$\underline{s}^T = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \end{pmatrix}$$

Ha a szindróma vektort megvizsgáljuk, akkor látjuk, hogy a Paritás mátrix 1. oszlopával egyezik meg. Azaz megmutatja nekünk, hogy az 1. helyiértéken történt a bithiba. Hasonló képpen, ha 01000, 00100, 00010, 00001 kódokat vesszük, a szindrómavektor rendre 101,100,010,001 azaz a paritásmátrix 2.,3.,4. és 5. oszlopával egyezik meg.

6.7. Hibajavítás metódusa

A Hamming kódok hibajavítási metódusa a következő. A paritásellenőrző mátrixot összeszorozzuk a demodulátor kimenetén lévő v^T vektorral, ezáltal megkapjuk a szindróma vektor transzponáltját. Ez a vektor kijelöli a Paritásellenőrző mátrixnak azon oszlopát, amelyik pozícióban a hiba történt. Ezen index szerinti bitet invertálva a vett jel vektorában, egy érvényes kódszót kapunk, ami szerencsés esetben megegyezik a küldött kódszóval.

6.8. Generátor és Paritásmátrix előállítása

Minden bináris Hamming kódot egy adott számhármas (N,K,q) - (kódszóhossz,üzenethossz,kódszimbólumhossz) jellemez. Ezek ismeretében a kódhoz tartozó szisztematikus paritásmátrix előállítható. Vegyük a (N-K)x(N-K) méretű egységmátrixot és illesszük a paritásmátrix végére. Ezek után a Paritásmátrix elején található (N-K)xK-s mátrixot úgy állíthatjuk elő, hogy oszloponként felsoroljuk a $[1, 2^{N-K-1}]$ tartomány azon elemeit, amelyeket az egységmátrix nem tartalmaz. Hiszen a paritásmátrix oszlopainak tartalmaznia kell a $[1, 2^{N-K-1}]$ tartomány összes elemét, mert ezáltal tudja kijelölni a lehetséges bitpozíciók közül a meghibásodottat. (Megjegyzés : a csupa 0 kombinációt azért nem tartalmazza, mert ez pontosan azt jelenti, hogy érvényes kódszó lépett fel a demodulátor kimenetén.)

1.Példa

Határozzuk meg a (N,K,q)=(7,4,2) szisztematikus kódnak a Paritásmátrixát!

A paritásmátrix végén lévő 3x3-as egységmátrix felsorolja $[1, 2^3]$ tartomány azaz 1,2,3,4,5,6,7 elemek közül az 1,2,4 elemeket. Tehát a paritásmátrix elején lévő mátrixnak a 3,5,6,7 oszlopokat kell tartalmaznia. Így a paritásmátrix:

$$\underline{\underline{H}} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

És ebből a megfelelő szabállyal előállított Generátormátrix

$$\underline{\underline{G}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Most nézzük azt az esetet, amikor a vett vektor $\underline{v}$=(0,1,0,0,0,1,0). Ebben egyszeres bithiba fordul elő a 4. pozícióban. Ha a paritásmátrixot összeszorozzuk ennek transzponáltjával akkor az (1,1,1) vektort kapjuk, ami a paritásmátrix 4. oszlopa, tehát itt történt a hiba.

6.9. Nem bináris Hamming kódok

Egy fokkal nehezebb feladatnak tűnik, amennyiben a perfekt kódokra vonatkozó 5.30 egyenletben $q \neq 2$. Tekintsük a legegyszerűbb ilyen esetet, azaz amikor q = 3. Ekkor az első perfekt kód az (N,K,q) = (4,2,3) számhármassal jellemezhető. Ennek kódsebessége R = $\frac{K}{N} = \frac{1}{2}$. A kódok szorzásánál, illetve osztásánál ilyenkor természetesen a modulo 3 összeadási és szorzási szabályok érvényesülnek. Negatív számok modulo értékeit például a következőképpen számolhatjuk. $mod_7(-13) = mod_7(-13 + 2 \cdot 7) = mod_7(1) = 1$.

Mivel a kód nem bináris, nem lehetünk biztosak abban, mi a hiba értéke, ha meghibásodás történt. Másképpen fogalmazva, a hibának nemcsak helye van hanem *értéke* is. A lehetséges kódszavak közül a paritásmátrixot alkotóknak az alábbi három szabály kell teljesíteniük.

1. A kódszavak közül hagyjuk el a csupa 0 kombinációt.
2. Az első nem 0 eleme a kódszónak legyen 1-es.
3. A kódszavak ne legyenek egymás konstans szorosai.

Tehát a {00,01,02,10,11,12,20,21,22} kódszavak közül a fenti szabályok figyelembe vételével a {01,10,11,12} elemeket kapjuk. Ezekből megalkothatunk egy szisztematikus paritásmátrixot.

$$\underline{\underline{H}} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$$

Az ebből előállítható generátor mátrix alább látható, a modulo 3 szabályok figyelembe vételével. Fontos megjegyezni továbbá, hogy immár nem bináris esetben vagyunk tehát $-P^T \neq P^T$.

$$\underline{\underline{G}} = \begin{pmatrix} 1 & 0 & -1 & -1 \\ 0 & 1 & -1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

Ezek után például az üzenettérből vett {20} vektort megszorozva a generátormátrixszal kapjuk a {2011} kódvektort. Tegyük fel ezek után, hogy a második pozícióban 2-es értékű hiba lép fel, azaz a vett vektor legyen v = {2211}. A szindróma vektor ekkor:

$$\underline{s}^T = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 2 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

A paritásmátrix konstruálásakor figyeltünk rá, hogy minden oszlop első nem 0 elem 1-es legyen. Ezáltal a szindrómavektor első (nem nulla) eleme megadja a hiba értékét. A hiba érétékével elosztva a szindrómavektort megkapjuk a paritásmátrix azon oszlopát, amelyik pozícióban a hiba előfordult. Tehát s^T = {2,1} esetén a hiba értéke 2. Ezzel eloszva a szindrómavektort modulo 3 szabályok szerint: $mod_3(2/2) = mod_3(1) = 1$. $mod_3(1/2) = mod_3(1/2) + mod_3(3/2) = mod_3(4/2) = mod_3(2) = 2$. Ezen egyenlőségek figyelembe vételével $\frac{s^T}{2}$ = {1 2} a paritásmátrix 2. oszlopa, így a hiba pozíciója is 2.

6.10. Galois Testek (GF - Galois Fields)

[2]

A Galois testek véges elemszámú testek, melyekben létezik egységelem és nullelem. A műveletek nem vezetnek ki a térből, azaz a modulo p aritmetikában összeadásra, szorzásra, kivonásra, osztásra zártak.

6.11. Prím hatványú Galois Testek (GF(p))

Amennyiben a test elemei p prím szám hatványai, Prím hatványú Galois testről beszélünk. Ezen test elemei {0,1,...p-1}.

6.12. Primitív elem

A Galois test bármely olyan nem nulla elemét, amelyet hatványozva először a p-1-edik hatványon lesz egyenlő az egységelemmel, primitív elemnek nevezünk. Azaz α primitív elem, ha

$$0 \neq \alpha \in GF(p), \quad \alpha^{p-1} = 1, \quad de \quad \alpha^{w} \neq 1, \quad ha \quad 0 \neq w < p-1 \qquad (6.40)$$

1.Példa

Legyen p = 5, ekkor a Galois test elemei {0,1,2,3,4}. Vizsgáljuk meg 2 primitív elem-e! $mod_5(2^1) = 2$, $mod_5(2^2) = 4$, $mod_5(2^3) = 3$, $mod_5(2^4) = 1$, azaz 2 primitív eleme a testnek. vegyük most a 4-et. Vizsgáljuk meg ez primitív elem-e! $mod_5(2^4) = mod_5(4^2) = 1$ tehát a 4 nem primitív eleme a testnek.

A primitív elemnek egy érdekes tulajdonságára világít rá ez a példa. A primitív elem hatványozva végigmegy a Galois test összes elemén, és csak a legutolsó hatványon veszi fel az 1 értéket.

[2]Ez itt matematikailag biztos nem percíz és egzakt

6.13. Ciklikus kódok

Ciklikus kódok olyan lineáris blokk kódok, amelyeknél minden érvényes $\underline{c}$ kódszó eltoltja $\underline{c}^e$ is érvényes kódszó.

$$\underline{c} = \{c_0, c_1, ...c_{N-2}, c_{N-1}\}, \quad \underline{c}^e = \{c_{N-1}, c_0, c_1, ...c_{N-2}\}. \tag{6.41}$$

Legyen $\underline{c} = \{c_0, c_1, ... c_{N-1}\}$ egy érvényes kódvektor. Ezen kódvektorhoz hozzárendelhető egy $c(p) = c_{N-1}p^{N-1} + c_{N-2}p^{N-2} + ... + c_1p + c_0$ polinom, mely a fenti érvényes kódszó polinom reprezentációja. Ez egy megfeleltetés az N dimenziós lineáris bináris tér és a N-1-ed fokú polinomok tere között.

Végezzük el ekkor a következő átalakításokat

$$c(p) = c_{N-1}p^{N-1} + c_{N-2}p^{N-2} + ... + c_1p + c_0 \tag{6.42}$$

$$pc(p) = c_{N-1}p^N + c_{N-2}p^{N-1} + ... + c_1p^2 + c_0p \tag{6.43}$$

Alkalmazzk a teveszabályt.[3]

$$pc(p)+c_{N-1}-c_{N-1} = c_{N-1}(p^N+1)+c_{N-2}p^{N-1}+...+c_1p^2+c_0p-c_{N-1} \tag{6.44}$$

Vezessük be a következő jelölést $c_1(p) = c_{N-2}p^{N-1} +...+ c_1p^2 + c_0p + c_{N-1}$, ezt megtehetjük hiszen ez egy N-1 -ed fokú polinom, tehát megfelelő reprezentációja egy kódnak. Itt felhasználtuk, hogy bináris esetben még igaz $c_{N-1} = -c_{N-1}$ is. Azaz

$$pc(p) = c_{N-1}(p^N + 1) + c_1(p) \tag{6.45}$$

osszuk el az egyenlet mindkét oldalát $(p^N + 1)$ -el. Ekkor

$$\frac{pc(p)}{(p^N + 1)} = c_{N-1} + \frac{c_1(p)}{(p^N + 1)} \tag{6.46}$$

[3]Adjunk hozzá 0-t az egyenlet mindkét oldalához

így azt kapjuk, hogy a p-vel való szorzás tulajdonképpen ciklikus eltolásnak felel meg, a $p^N + 1$ polinomosztás maradékát tekintve.

6.14. Ciklikus kód generálása

Adott (N,K,q) -hoz, azaz $(p^N + 1)$ -hez generáljunk olyan két polinomot tényezőkre bontással, hogy

$$p^N + 1 = g(p)h(p) \tag{6.47}$$

ahol g(p) generátorpolinom, és h(p) paritásellenőrző polinom. Ekkor a kódok az u(p) üzenetpolinomból a következőképpen állíthatóak elő

$$c(p) = u(p)g(p) \tag{6.48}$$

ahol, u(p) K-1 -ed fokú, g(p) N-K-ad fokú és c(p) N-1-ed fokú polinomok. Ezek után írhatjuk

$$c(p)h(p) \ \ mod \ \ (p^N + 1) = u(p)g(p)h(p) \ \ mod \ \ (p^N + 1) = 0 \tag{6.49}$$

6.15. CRC - Cyclic Redundancy Check

"A CRC (Cyclic Redundancy Check) kódok csak hibajelzésre alkalmasak, tipikusan valamilyen hibajavító kódolással kombinálva alkalmazzák őket. A CRC kódok speciális ciklikus kódok, melyek nagyméretű (pl. K=1023) blokkhoz készítenek rövid (pl. r=24) ellenőrző összeget. Ha ezután akár a blokkban, akár az ellenőrző összegben változás történik, akkor az ismételten kiszámított CRC összeg nagy valószínűséggel nem fog egyezni a blokk végén található CRC összeggel. A CRC kódokat, illetve a szindrómát éppúgy polinomosztással lehet generálni, mint a többi ciklikus kódot"[1]

Kódgenerálási mechanizmusa

$$c(p) = u(p)p^{N-K} - \frac{(u(p)p^{N-K})}{g(p)} \ \ mod \ \ p \tag{6.50}$$

6.16. Reed Solomon kód

A Reed - Solomon kód olyan nem bináris blokkód amelyben a kódszóhossz eggyel rövidebb a szimbólumhossznál. Azaz N = q-1. t = t_{jav} jelölje a javítható hibák számát. Ekkor

$$N - K = 2t \quad d_{min} = 2t + 1 \tag{6.51}$$

Továbbá legyen $\alpha \in GF(q)$ galois test primitív eleme eleme. Definiáljuk a Reed-Solomon kódot az alábbi generátorpolinommal

$$g(x) = (x + \alpha)(x + \alpha^2)...(x + \alpha^{2t}) \tag{6.52}$$

Ekkor az u(x) = $u_0 + u_1 x + ... + u_{N-1}x^{N-1}$ üzenetpolinomhoz rendelt kódpolinom c(x) = $u(\alpha^0) + u(\alpha^1) + ... + u(\alpha^{N-1})$, azaz a primitív elem hatványainak üzenetpolinomba való behelyettesítésével származtatható.

Mátrix reprezentációban a Reed-Solomon kód az alábbi generátormátrixszal jellemezhető

$$\underline{\underline{G}} = \begin{pmatrix} 1 & 1 & 1 & ... & 1 \\ 1 & \alpha & \alpha^2 & ... & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & ... & \alpha^{2(N-1)} \\ \vdots & & & \ddots & \vdots \\ 1 & & & ... & \alpha^{(K-1)(N-1)} \end{pmatrix} \tag{6.53}$$

És így a kódok előállítása a $\underline{c} = \underline{u} \cdot \underline{\underline{G}}$ képletnek megfelelően történik.

1. Példa

Legyen (N,K,q) = (4,2,5) már fent láttuk hogy 2 primitív eleme GF(5) Galois testnek. Állítsuk elő a $\underline{\underline{G}}$ generátormátrixot. A generátormátrix az 6.53 egyenletnek megfelelően állítható elő (természetesen itt is modulo q osztást alkalmazunk). Azaz

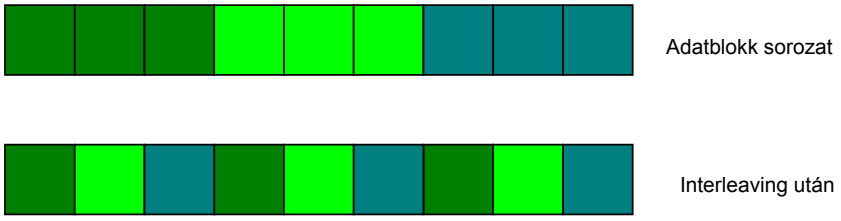
$$\underline{\underline{G}} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \end{pmatrix} \tag{6.54}$$

Ez a mátrix azonban nem szisztematikus, mivel nem tartalmazza az egységmátrixot. Szerencsére szisztematikussá tehető Gauss eliminációval. Vonjuk ki az első sort a másodikból, majd a másodikat az elsőből, és így kapjuk

$$\underline{\underline{G}} = \begin{pmatrix} 1 & 0 & -2 & -1 \\ 0 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 3 & 4 \\ 0 & 1 & 3 & 2 \end{pmatrix} \tag{6.55}$$

6.17. Interleaving - Átszövés

Az adatátvitel során fellépő Burst-ös hibák ellen úgy védekezhetünk, hogy az adatblokkokat feldaraboljuk, majd beírjuk egy mátrixba sorfolytonosan és oszlopfolytonosan kiolvassuk, ezután a csatornán való átjutás után az előző műveletet ismét elvégezve visszakapjuk az eredeti adatsorozatot. Ezzel a módszerrel, nem egy adatblokk hibásodik meg kritikusan, hanem sok adatblokk enyhén. Mivel az ellenőrző összegek a blokkok végén vannak, az egyes blokkokban lévő enyhe hibák még javíthatóak, holott a blokk nagyobb részének meghibásodása nem lett volna az.

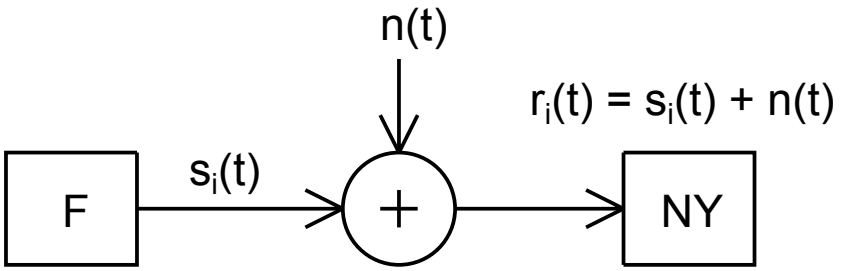


6.9. ábra. 3x3 interleaving

7. Döntéselmélet

Az adatátvitel során a forrás által kibocsátott $S_i(t)$ jelalakokkal reprezentált jelekhez a csatornán additív n(t) zaj adódik, és így a vevőre kerülő jel a hasznos jel és a zaj összege. A Döntéselmélet során hipotéziseket állítunk fel, melyek azt hivatottak megbecsülni, a forrás mely szimbólumot bocsátotta ki.

Az első feladatunk a döntéselmélet során, hogy a megfigyelt szimbólumokat tartalmazó teret - a megfigyelési teret (OS - Observation Space) - olyan



7.10. ábra. Zajos csatorna

részekre osszuk fel, amelybe eső minták alapján az egyik illetve másik hipotézis javára döntünk. Bináris esetben, ha a forrás által kibocsátott S_0 szimbólumot a H_0 hipotézis jelöli, míg S_1 szimbólumot a H_1 hipotézis, továbbá $\tilde{H}$ a döntésünk eredménye, akkor a döntés helyessége az alábbi táblázattal adható meg.

F	$\tilde{H}$	
H_0	H_0	OK
H_0	H_1	X
H_1	H_0	X
H_1	H_1	OK

7.1. Bayes-féle Döntés

A következő döntéselméleti módszert Thomas Bayes (1702-1761) angol matematikus dolgozta ki. A Bayes-féle döntéshez bináris esetben az alábbi feltételeknek kell teljesülnie.

1. A forrás statisztikájának ismertnek kell lennie azaz $Pr\{H_0\} = P_0$ és $Pr\{H_1\} = P_1 = 1 - P_0$.

2. Minden döntésnek van költsége, és ez 0 vagy ismert C_{ik}, ahol k annak a hipotézisnek az indexe, amelyik ténylegesen bekövetkezik, míg i annak a hipotézisnek az indexe, amelyik javára döntöttünk. Például C_{01} 1-es érkezett és 0-nak értékeltük.

3. A hibás döntés költsége nagyobb mint a helyesé. $C_{00} < C_{01}$, $C_{11} < C_{01}$.

4. A döntést úgy próbáljuk elvégezni, hogy az átlagos költséget (Kockázat) minimalizáljuk. K = min.

7.2. A Kockázat

$$K = P_0C_{00}Pr\{\tilde{H} = H_0|H_0\} + P_0C_{10}Pr\{\tilde{H} = H_1|H_0\} \\ +P_1C_{11}Pr\{\tilde{H} = H_1|H_1\} + P_1C_{01}Pr\{\tilde{H} = H_0|H_1\} \tag{7.56}$$

$$K = P_0C_{00}\int_{Z0} P(r|H_0)dr + P_0C_{10}\int_{Z1} P(r|H_0)dr \tag{7.57}$$

$$+P_1C_{11}\int_{Z1} P(r|H_1)dr + P_1C_{01}\int_{Z0} P(r|H_1)dr\} \tag{7.58}$$

ahol, $P(r|H_1)$ annak a valószínűségi sűrűsége, hogy a H_1 hipotézis mellett döntünk, feltéve, hogy a megfigyelt érték r. Mivel Z0 és Z1 együtt a megfigyelési tartományt adják,

$$\int_{Z0}(.)dr + \int_{Z1}(.)dr = 1 \rightarrow \int_{Z1}(.)dr = 1 - \int_{Z0}(.)dr \tag{7.59}$$

Kockázat 7.57-7.58 egyenletből a következőképp írható

$$K = P_1(C_{01} - C_{11})\int_{Z_0} P(r|H_1)dr - P_0(C_{10} - C_{00})\int_{Z_0} P(r|H_1)dr \tag{7.60}$$

A fenti kifejezés minimalizálásához, a H_1-es hipotézis esetén a következő egyenlőtlenséget kell teljesíteni

$$\tilde{H} = H_1 \rightarrow P_1(C_{01} - C_{11})\int_{Z_0} P(r|H_1)dr > P_0(C_{10} - C_{00})\int_{Z_0} P(r|H_0)dr \tag{7.61}$$

H_0 hipotézis esetén

$$\tilde{H} = H_0 \rightarrow P_1(C_{01} - C_{11})\int_{Z_0} P(r|H_1)dr < P_0(C_{10} - C_{00})\int_{Z_0} P(r|H_0)dr \tag{7.62}$$

Vagy másképp ($\tilde{H} = H_1$ a felső, $\tilde{H} = H_0$ az alsó reláció teljesülését jelenti)

$$\frac{\int_{Z_0} P(r|H_1)dr}{\int_{Z_0} P(r|H_0)dr} \begin{array}{c} > \\ \hline < \end{array} \frac{P_0(C_{10} - C_{00})}{P_1(C_{01} - C_{11})} \tag{7.63}$$

továbbá figyelembe véve, hogy a sűrűségfüggvények pozitívak lehetnek

$$\frac{P(r|H_1)dr}{P(r|H_0)dr} \begin{array}{c} > \\ \hline < \end{array} \frac{P_0(C_{10} - C_{00})}{P_1(C_{01} - C_{11})} \tag{7.64}$$

írható, ekkor a jobboldalon álló kifejezés csak a mérési eredményektől, r-től függ, ezt mostantól $\Lambda(r)$-el jelöljük. A jobboldali kifejezés pedig pontosan a megfigyelési tér Bayes féle optimális felosztása. Ezt mostantól η-val jelöljük. Tehát

$$\Lambda(r) = \frac{P(r|H_1)dr}{P(r|H_0)dr} \ , \ \eta = \frac{P_0(C_{10} - C_{00})}{P_1(C_{01} - C_{11})} \tag{7.65}$$

bevezetések után a döntést meghatározó egyenlőtlenség

$$\Lambda(r) \begin{array}{c} > \\ \hline < \end{array} \eta \tag{7.66}$$

1. Példa

Tekintsük azt az esetet, amikor $S_1 = \mathrm{A}$, és $S_0 = 0$. Továbbá feltételezzük, hogy az átvitelkor additív Gauss zaj lép fel. Ekkor $\Lambda(r)$ kifejezése a következő alakú lesz.

$$\Lambda(r) = \frac{\prod_{i=1}^{N} \frac{1}{\sqrt{2\pi}\sigma} \exp\left[-\frac{1}{2\sigma^2} \cdot (r_i - A)^2\right]}{\prod_{i=1}^{N} \frac{1}{\sqrt{2\pi}\sigma} \exp\left[-\frac{r_i^2}{2\sigma^2}\right]} \begin{array}{c} > \\ \hline < \end{array} \eta \tag{7.67}$$

Logaritmus képzéssel, valamint a számlálóból és a nevezőből kiemelve kapjuk

$$ln\Lambda(r) = \frac{ln(\frac{1}{\sqrt{2\pi}\sigma})^N}{ln(\frac{1}{\sqrt{2\pi}\sigma})^N}\left(\sum_{i=1}^{N} -\frac{1}{2\sigma^2}(r_i - A)^2 - \sum_{i=1}^{N} -\frac{1}{2\sigma^2}r_i^2\right) \tag{7.68}$$

$$ln\Lambda(r) = \frac{1}{2\sigma^2}\sum_{i=1}^{N}\left(2r_i - A^2\right) = \frac{A}{2\sigma^2}\sum_{i=1}^{N} 2r_i - \frac{NA^2}{2\sigma^2} \begin{array}{c} > \\ < \end{array} ln(\eta) \tag{7.69}$$

Végül a mérési eredményekre kifejezve

$$\sum_{i=1}^{N} r_i \begin{array}{c} > \\ < \end{array} \frac{\sigma^2}{A}ln(\eta) + \frac{NA^2}{2} \tag{7.70}$$

A fenti eredmény arra mutat rá, hogy a döntéshez nem feltétlenül kell az összes minta értékét egyenként tudnunk. Jelen esetben elég, ha az összegüket tudjuk. Ez az un. Elégséges statisztika.

1. Feladat

Legyen $S_0 = 0$, azaz egyáltalán nincs jel a csatornán. S_1 legyen 0 körül Gaussi fehérzaj tulajdonságú jel, szórásnégyzete σ_s^2. A csatornán fellépő zaj szintén gaussos 0 várható értékkel és σ_n^2 szórásnégyzettel. Adjuk meg a döntési szabályt és az elégséges statisztikát

2. Példa

Legyenek $S_0(t) = m_0$, $S_1(t) = m_1$ Poisson eloszlású valószínűségi változók, ismerjük P_0-t és P_1-t és a megfigyelési idő legyen T. Ekkor az ezalatt beérkező n mintára

$$H_0 = Pr\{n\} = \frac{m_0^n \cdot e^{-m_0}}{n!}, \quad H_1 = Pr\{n\} = \frac{m_1^n \cdot e^{-m_1}}{n!} \tag{7.71}$$

Általában feltehetjük $C_{00} = C_{11} = 0$, azaz a helyes döntés költsége 0. Továbbá válasszük $C_{01} = C_{10} = 1$ -et. Ekkor $\eta = \frac{P_0}{P_1}$

$$\frac{\frac{m_1^n \cdot e^{-m_1}}{n!}}{\frac{m_0^n \cdot e^{-m_0}}{n!}} = \frac{m_1^n \cdot e^{-m_1}}{m_0^n \cdot e^{-m_0}} \begin{array}{c} \geq \\ \leq \end{array} \eta \tag{7.72}$$

Megemlítjük, hogy a diszkrét eloszlás miatt az egyenlőség is megengedett Logaritmusképzéssel és átrendezéssel kapjuk, hogy

$$n \begin{matrix} \geq \\ \leq \end{matrix} \frac{ln(\eta) + m_1 - m_0}{ln\frac{m_1}{m_0}} \tag{7.73}$$

A jobboldalon álló kifejezésre bevezetjük a 'k' küszöbérték jelölést. Azaz, ha a vizsgálati idő alatt a beérkező minták száma meghalad egy értéket akkor a H_1 hipotézis javára döntünk, ha pedig ezen érték alatt marad, akkor pedig H_0 javára, a köztes esetekbnen pedig "hol így, hol úgy".

$$\begin{array}{ll} n > k & \tilde{H} = H_1 \\ n < k & \tilde{H} = H_1 \\ n = k & \tilde{H} = QH_1 + (1-Q)H_0,\ Q \in \{\{0\},\{1\}\}, P_0 = 0.5 = P_1 \end{array} \tag{7.74}$$

7.3. Döntés Kettőnél Több Hipotézisre

Ha 7.1 fejezetben tárgyalt követelmények teljesülnek, valamint $C_{ii} = 0$, $C_{ik\neq i} = 1$, akkor

$$\Lambda(r) \begin{matrix} \geq \\ < \end{matrix} \frac{P_0}{P_1} \tag{7.75}$$

$$P_1(p(r|H_1)) \begin{matrix} \geq \\ < \end{matrix} P_0(p(r|H_0)) \tag{7.76}$$

Általánosítva

$$\tilde{H} = H_i, \quad amelyre \quad P_i(p(r|H_i)) = max_i \tag{7.77}$$

A Bayes tételt felhasználva

$$p(r|H_i) = \frac{(p(r,H_i))}{P(H_i)} = \frac{(p(r,H_i))}{P_i} \ \ valamint \ \ P(H_i|r) = \frac{(p(r,H_i))}{p(r)} \tag{7.78}$$

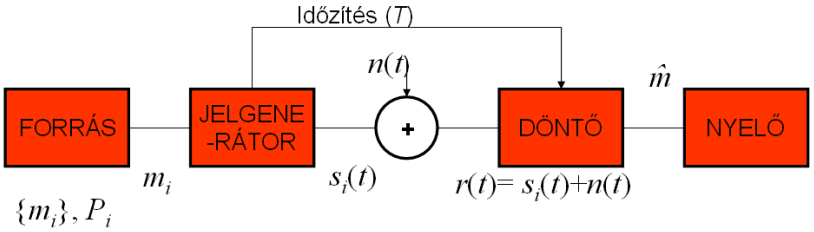
$$P(H_i|r)p(r) = p(r|H_i)P_i = max \tag{7.79}$$

Azaz a maximum a posteriori valószínűségre kell dönteni

$$P(H_i|r) = max_i \tag{7.80}$$

8. Digitális Átvitel

A vizsgálataink során először a következő modellel fogunk dolgozni. A forrás által kibocsátott m_i szimbólum, amely M féle lehet a jelgenerátorba jutva az $S_i(t)$ jelalakot generálja. A jel ezután az additív gaussi fehér zajjal (AWGN - Additive White Gaussian Noise) terhelt csatornán át a Döntő áramkörbe jut, amely a becsült $\tilde{m}$-et bocsátja ki. Feltételezzük továbbá, hogy az időzítési információ egy külön útvonalon átjutva már ismert a döntőben.



8.11. ábra. Digitális átvitel

A vizsgálataink során először az olyan eseteket tekintjük, amikor az $m_i \Leftrightarrow S_i(t)$ hozzárendelés kölcsönösen egyértelmű.

8.1. Termikus Zaj - Additív Gaussi Fehér Zaj

Az additív gaussi zajt jellemezhetjük az időbeli mintáival $n_i(t)$-vel. Továbbá igaz rá, hogy stacionárius, valamint a 'fehér' jelző arra utal, hogy a spektrális teljesítmény sűrűsége konstans.

$$S_n(\omega) = \frac{N_0}{2}, \quad ahol \quad N_0 = FkT \tag{8.81}$$

Ahol F az eredő zajtényező, k a Boltzmann állandó és T az abszolút hőmérséklet. N_0 egzakt kifejezése, amely kis frekvencián közelíthető a fentivel

$$N_0 = F \cdot \frac{hf}{e^{\frac{hf}{kT}} - 1},\ hf << kT,\ N_0 \approx F\frac{hf}{1 + \frac{hf}{kT} - 1} = FkT \tag{8.82}$$

Rádiófrekvencián, tehát élhetünk a fehér zaj közelítéssel a termikus zaj esetében, optikai tartományban azonban már nem. Ekkor az értéke közel exponenciálisan csökken a frekvenciával.

8.2. A Jeltér Alapfogalmai

Legyenek { $S_1(t)$, $S_2(t)$ ... $S_M(t)$ } a jelgenerátor kimenetén fellépő jelalakok és { $\phi_1(t)$, $\phi_2(t)$ ... $\phi_D(t)$ } a jeltér egy ortonormált bázisa. Ekkor az $S_i(t)$ függvények sorbafejthetőek a tér bázisaival.

$$S_i(t) = \sum_{j=1}^{D} a_{ij}\phi_j(t) \tag{8.83}$$

Ahol a_{ij} sorfejtési együtthatókat a következő kifejezés adja[4]

$$a_i(t) = \int_0^T S_i\phi_j(t)dt \tag{8.84}$$

Matematikailag bizonyítható, hogy az M féle jelalak sorfejtéséhez legfejjebb M bázisfüggvényre van szükségünk, tehát dim{D}≤dim{M}. Azaz kölcsönösen egyértelmű leképezés létezik $S_i(t)$ jelalakok és $\underline{s}_i = (a_{i1},a_{i2}...a_{iD})$ jelvektor között.

$$S_i(t) \Longleftrightarrow S_i = (a_{i1}, a_{i2}...a_{iD}) \tag{8.85}$$

Definiálhatóak a következő fogalmak is

Skalárszorzat

$$\underline{s}_i \cdot \underline{s}_l = \int_0^T S_i(t)S_l(t)dt \tag{8.86}$$

[4] a_{ij} hej hó o_{ij} hej hó... /Balu kapitány/

Jelenergia

$$E_i = |\underline{s}_i|^2 = \int_0^T (S_i(t))^2 dt \tag{8.87}$$

8.3. Gram-Schmidt Ortogonalizáció

Ezt az eljárást arra használjuk, hogy tetszőleges vektorrendszerből egy ortonormált bázisát állítsuk elő az adott térnek. Az eljárás a következő. Az első vektort tetszőlegesen megválaszthatjuk, majd leosztjuk a hosszával, így éppen egységnyi hosszúságú vektort kapunk. A második vektort úgy választjuk meg, hogy egy tetszőleges vektorból levonjuk az első vektorra vett vetületét (ez éppen a skalár szorzatuk szorozva az első egységvektorral (irány megadása). Ezután a második vektort is leosztjuk a hosszával, immáron 2 egymásra merőleges, egységnyi hosszúságú vektorunk van. Az eljárás így folytatható, ameddig el nem érjük az adott tér dimenzióját. A vektorból levonjuk az első egységvektor irányába vett vetületét majd a második vektor irányába vett vetületét... Mindezt képletekkel kifejezve D = 3-ra:

$$\phi_1 = \frac{\underline{v}_1}{|\underline{v}_1|} \tag{8.88}$$

$$\underline{h}_2 = \underline{v}_2 - (\underline{v}_2\underline{\phi}_1)\underline{\phi}_1, \;\; \phi_2 = \frac{\underline{h}_2}{|\underline{h}_2|} \tag{8.89}$$

$$\underline{h}_3 = \underline{v}_3 - (\underline{v}_3\underline{\phi}_1)\underline{\phi}_1 - (\underline{v}_3\underline{\phi}_2)\underline{\phi}_2, \;\; \phi_3 = \frac{\underline{h}_3}{|\underline{h}_3|} \tag{8.90}$$

Érdemes megnézni létezik-e negyedik egységvektor, azaz van-e ϕ_4?

$$\underline{h}_4 = \underline{v}_4 - (\underline{v}_4\underline{\phi}_1)\underline{\phi}_1 - (\underline{v}_4\underline{\phi}_2)\underline{\phi}_2 - (\underline{v}_4\underline{\phi}_3)\underline{\phi}_3 = \underline{v}_4 - \underline{v}_4 = 0 \tag{8.91}$$

Azaz nincsen ϕ_4 hiszen D = 3 esetén, minden vektor kikeverhető a három bázis és együtthatók lineárkombinációjaként, ahol az együtthatókat éppen a vetületek adják.

A fenti módszert a jeltérben megvalósítva az alábbiak írhatóak

$$\phi_1(t) = \frac{S_1(t)}{\sqrt{E_1}},\ \ h_2(t) = S_2(t) - \phi_1(t) \int_0^T S_2(t) \cdot \phi_1(t) dt... \tag{8.92}$$

8.4. Bináris FSK

A bináris FSK (Frequency Shift Keying) egy olyan modulációs technika, amelyben a két jelalakot egymáshoz eltolt frekvencián lévő azonos amplitúdójú jeladja. Az egyik jelalak a 0-s a másik az 1-es bitnek felel meg. A következőkben a Gram Schmidt ortogonalizációt hajtjuk végre, illetve kiszámoljuk az a_{ij} együtthatókat a Bináris FSK jelre.

$$S_1(t) = \sqrt{(2)} A \cdot cos(\omega_c t),\ \ S_2(t) = \sqrt{(2)} A \cdot cos(\omega_c t + \delta\omega t) \tag{8.93}$$

Az első jel energiája

$$E_1 = \int_0^T 2A^2 \cdot cos^2(\omega_c t) dt = \int_0^T 2A^2 \cdot \left(\frac{1}{2} + \frac{cos(2\omega_c t)}{2} \right) dt \tag{8.94}$$

Mivel a cos fv Egy periodusra vett integrálja 0 ezért az Első jel energiájának értéke

$$E_1 = A^2 T \tag{8.95}$$

Az a_{21} együtthatót ezek után az $S_2(t)$ jel és a $\phi_1(t)$ bázisvektor ($S_1(t)$ E_1-el normalizált alakja) skaláris szorzata.

$$a_{21} = \int_0^T \sqrt{2} A \cdot cos(\omega_c t + \delta\omega t) \cdot \sqrt{\frac{2}{T}} \cdot cos(\omega_c t) dt \tag{8.96}$$

Elemi trigonometrikus átalakításokkal kapjuk:

$$a_{21} = A\sqrt{T} \cdot \frac{sin(\delta\omega T)}{\delta\omega T} \tag{8.97}$$

$$h_2(t) = \sqrt{2}A \cdot cos(\omega_c t + \delta\omega t) - A\sqrt{T} \cdot \frac{sin(\delta\omega T)}{\delta\omega T}\sqrt{\frac{2}{T}}cos(\omega_c t) \tag{8.98}$$

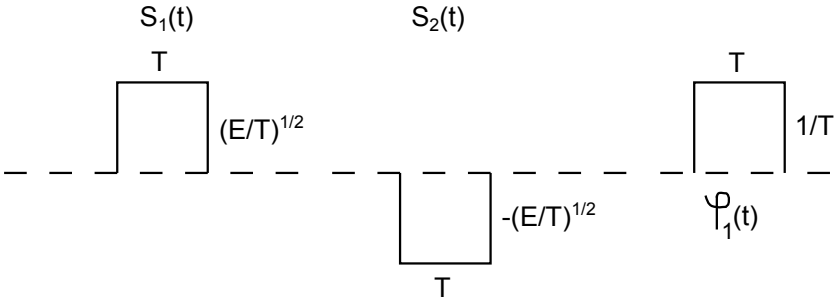
$$\phi_2(t) = \frac{h_2(t)}{E_{h2}} \tag{8.99}$$

A fenti módszer elég körülményesnek tűnik a_{21} meghatározására, próbáljunk meg valami egyszerűbbet! Eddig tudjuk, hogy $a_{11} = \mathrm{A}\sqrt{T}$, és $a_{21} = 0$. Azt is tudjuk, hogy a két jel energiája megegyező, hiszen a frekvenciában való eltolás ezt nem változtatja. Azt is beláttuk, hogy $a_{21} = A\sqrt{T} \cdot \frac{sin(\delta\omega T)}{\delta\omega T}$. Mivel a jel energiája a két együttható négyzete:

$$E_2 = E_1 = a_{21}^2 + a_{22}^2 \uparrow \quad a_{22} = A\sqrt{T}\sqrt{1 - \left(\frac{sin(\delta\omega t)}{\delta\omega t}\right)^2} \tag{8.100}$$

8.5. Alapsávi NRZ jelkészlet

Az információ legegyszerűbb kódolása az M = 2, D = 1, NRZ (Non-Return-To-Zero) kódolás. Ilyenkor $S_1(t)$ = -$S_2(t)$. Ez az un. Antipodális jelkészlet. Mivel D = 1. Ezért csak bázisvektorunk/bázisfüggvényünk van, ennek mentén mozogva, helyezhetjük el az értékeket. Ezt mutatja a 8.13 ábra.

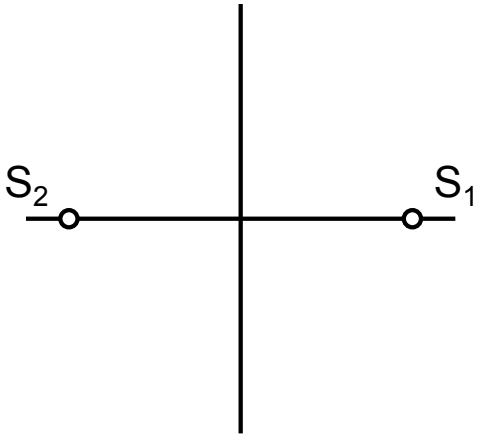


8.12. ábra. Non-Return-To-Zero

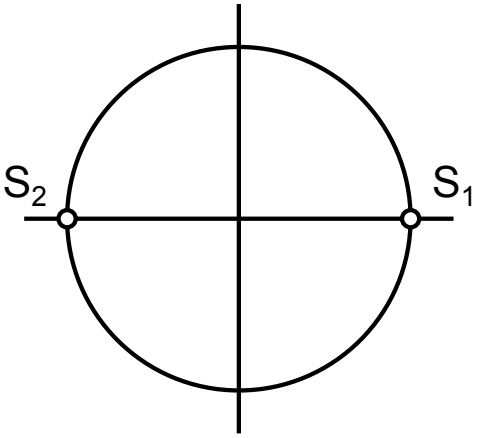
8.6. BPSK - Binary Phase Shift Keying

M = 2, D = 2 Esetben 2 egymásra merőleges bázisfüggvényünk van és két jalalakunk. Leggyakrabban alkalmazott eset, amikor $\Phi = \pi$.

$$\begin{array}{ll} S_1(t) = \sqrt{2}A \cdot cos(\omega_c t) & \phi_1(t) = \sqrt{\frac{2}{T}} cos(\omega_c t) \\ S_2(t) = \sqrt{2}A \cdot cos(\omega_c t + \Phi) & \phi_2(t) = \sqrt{\frac{2}{T}} sin(\omega_c t) \end{array} \tag{8.101}$$



8.13. ábra. NRZ



8.14. ábra. BPSK

8.7. QPSK - Quaternary Phase Shift Keying

M = 4, D = 2 Azaz 4 jelalakunk van és 2 bázisfüggvényünk.

$$\begin{array}{ll} S_1(t) = \sqrt{2}A \cdot cos(\omega_c t) & S_3(t) = -S_1(t) \\ S_2(t) = \sqrt{2}A \cdot sin(\omega_c t + \Phi) & S_4(t) = -S_2(t) \end{array} \tag{8.102}$$

8.8. Orthogonal QFSK - Quaternary Frequency Shift Keying

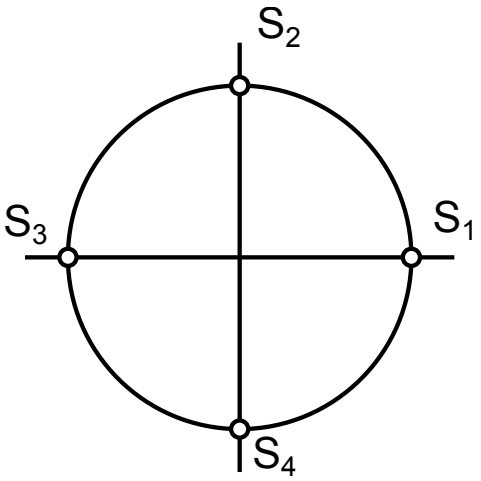
M = 4, D = 4

$$S_i(t) = \sqrt{2}A \cdot cos(\omega_c t + i\frac{2\pi t}{T}) \tag{8.103}$$

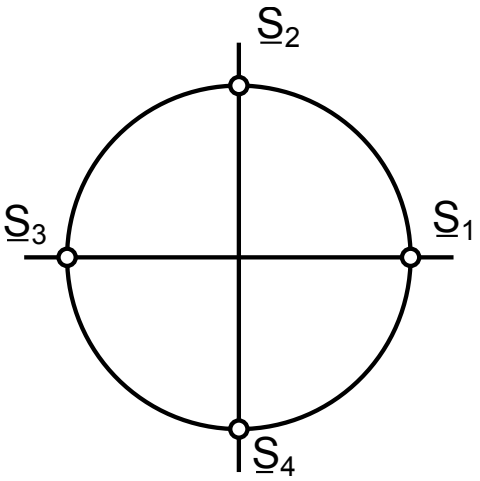
8.9. Bi-Orthogonal QFSK

Az előző speciális esete

$$\begin{array}{ll} S_1(t) = \sqrt{2}A \cdot cos(\omega_c t) & S_3(t) = -S_1(t) \\ S_2(t) = \sqrt{2}A \cdot cos(\omega_c t + \frac{2\pi t}{T}) & S_4(t) = -S_2(t) \end{array} \tag{8.104}$$



8.15. ábra. QPSK



8.16. ábra. QFSK

8.10. M-QAM - M Quadrature Amplitude Modulation

D = 2,

$$\begin{array}{ll} S_1(t) = a_i \cdot A \cdot cos(\omega_c t) + q_j \cdot A \cdot sin(\omega_c t) & \\ a_i = \frac{2i-1}{\sqrt{(M)}-1} & q_j = \frac{2j-1}{\sqrt{(M)}-1} \end{array} \tag{8.105}$$

8.11. A Jeltér Felosztása

A döntés során a jelteret úgy kell felosztani, hogy a hiba minimális legyen. $P_\epsilon = \min$, ha $\Pr\{H_i|r\} = max_i$

$$Pr\{H_i|r\} = Pr\{s_i|r\} = P_i \cdot p(r|s_i) = max_i \tag{8.106}$$

gaussos esetetben

$$P_i \cdot p(r|s_i) = P_i \cdot \frac{1}{(\pi N_0)^{D/2}} \cdot exp\left(-\frac{|r-s_i|^2}{N_0}\right) = max_i \tag{8.107}$$

logaritmus vége

$$ln(P_i) - \frac{D}{2} ln(\pi N_0) - \frac{|r-s_i|^2}{N_0} = max_i \tag{8.108}$$

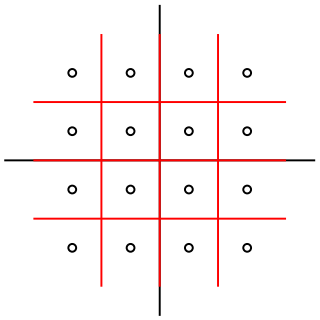
A konstans tagokat a maximalizálás szempontjából elhagyva

$$ln(P_i) - \frac{|r|^2 - 2rs_i - E_i}{N_0} = max_i \tag{8.109}$$

$$ln(P_i) + \frac{E_i - 2rs_i}{N_0} = max_i \tag{8.110}$$

$$\frac{1}{2} ln(N_0 \cdot ln(P_i) - E_i) + rs_i = max_i \tag{8.111}$$

1. Példa

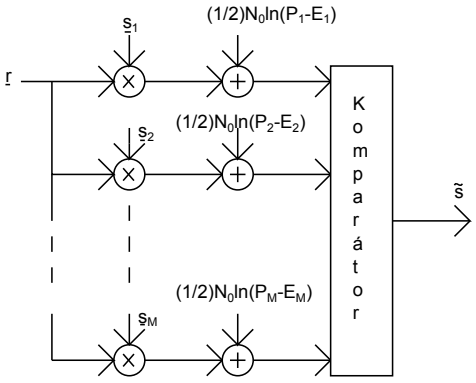


8.17. ábra. 16QAM

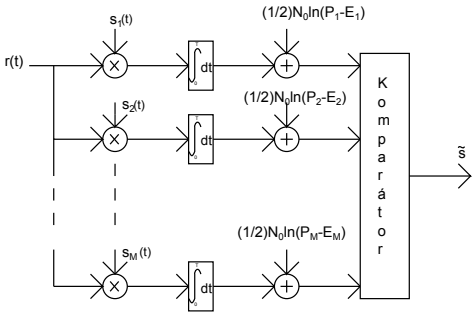
Vegyük azt az esetet amikor M szibmbólum esetén $P_i = \frac{1}{M}$. Ekkor lévén P_i ugyanakkora minden értékre, $-|r-s_i|^2$-et kell maximálisra választani ez

ugyanaz mintha azt mondanánk $|r - s_i|^2$ legyen minimális, továbbá $|r - s_i|$ legyen minimális. Tehát aszerint kell dönteni, hogy a megfigyelt érték melyik konstellációs ponttól van a legkisebb távolságra. Ezen döntési tartományokat szemlélteti a következő ábra 16-QAM-re

8.12. A Döntő Felépítése



8.18. ábra. Döntő vektorokra



8.19. ábra. Döntő Jelalakokra

8.13. Döntés Zajos Csatorna Esetén

Legyen $\{\phi_1, \phi_2 ... \phi_D\}$ teljese ortonormált bázis. A zaj időfüggvénye sorbafejthető az ortonormált bázisra D $\to \infty$ esetén. Ha azonban a bázisunk véges tagból áll, akkor a zaj időfüggvénye csak közelítőleg fejthető sorba.

$$n_j = \int_0^T n(t)\phi_j(t)dt, \;\; n(t) = \sum_{j=1}^{D} n_j\phi_j(t) + \tilde{n(t)} \tag{8.112}$$

Azaz a zaj időfüggvényéhez rendelhető D hosszúságú vektor nem kölcsönösen egyértelmű leképezés. A zaj és a csatorna utáni jel sűrűségfüggvényei Gaussi zaj és jel esetére a következőképp néznek ki.

$$p(\underline{n}) = \frac{1}{(\pi N_0)^{D/2}} e^{-\frac{|\underline{n}|^2}{N_0}} \;\; p(r) = \frac{1}{(\pi N_0)^{D/2}} e^{-\frac{(n-s_i)^2}{N_0}} \tag{8.113}$$

Írjuk fel a 8.112 egyenletben szereplő $\tilde{n}$ kifejezését végtelen számú bázisvektorra vett sorfejtéssel.

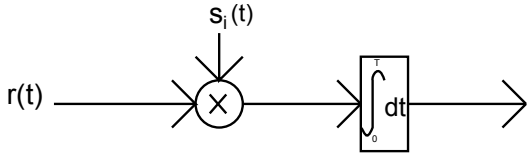
$$n(t) = \sum_{j=1}^{D} n_j \phi_j(t) + \sum_{j=D+1}^{\infty} n_j \phi_j(t) \tag{8.114}$$

Ekkor

$$r(t) = \sum_{j=1}^{D} (a_{ij} + n_j)\phi_j(t) + \sum_{j=D+1}^{\infty} n_j \phi_j(t) \tag{8.115}$$

A feladatunk egy olyan döntő felépítése, amelyben a második tag nem játszik szerepet. Térjünk át vektor reprezentációra. Ekkor az amennyiben $\underline{s}_l$ olyan alakú, hogy a D+1-től ∞-ig csak 0-kat tartalmaz, az $\underline{r} \cdot \underline{s}_l$ skalárszorzatból D+1-től ∞-ig lévő tagok kiesnek.

Ez tulajdonképpen egy szűrést valósít meg a jelen, ezért tekinthetjük szűrőnek is. Ennek felépítése tehát a következő.



8.20. ábra.

$$y(t) = r(t) * s_i(t) \tag{8.116}$$

Hivatkozások

[1] Információelmélet Kivonatos jegyzet Veszprémi Egyetem, Műszaki Informatika Szak Dr. Vassányi István, Š 2002-2005.