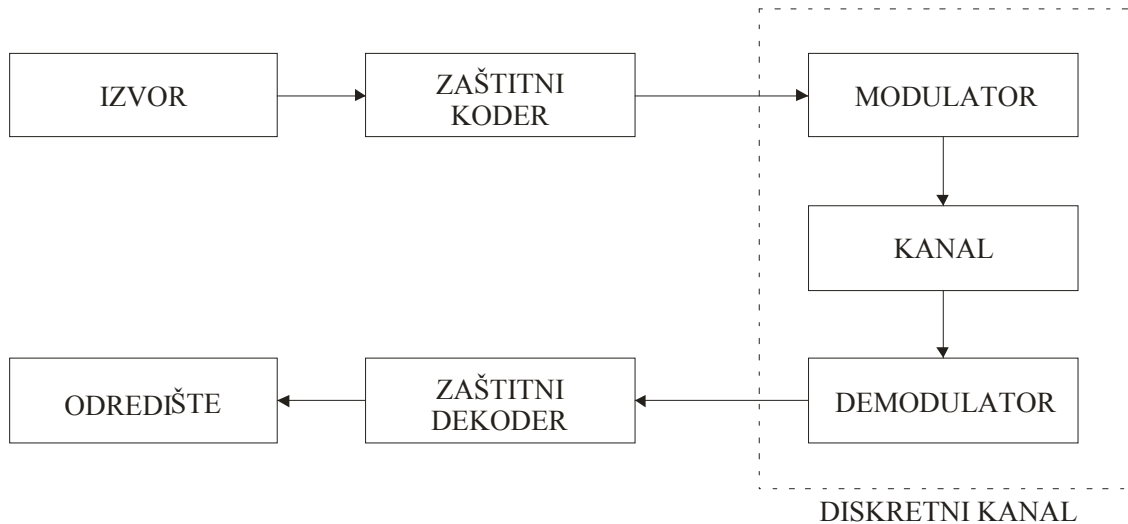


## ***KANALI ZA PRENOS INFORMACIJA***

Prema blok šemi izloženoj na početku predavanja, sada dolazi na red zaštitni koder. Međutim, ovaj koder se uvodi zbog kanala – da bi se otklonile i eventualno ispravile greške koje nastaju u kanalu. Slično kao što su podijeljeni izvori, i kanali se mogu podijeliti na diskretne i kontinualne kanale. Diskretni kanali se mogu dalje podijeliti na diskretne kanale bez memorije i diskretne kanale sa memorijom.



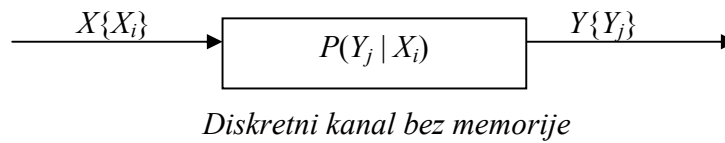
Prije nego što pređemo na zaštitno kodovanje proučicemo kanale s gledišta teorije informacija. Neka izvor emituje poruku bita (informacioni biti) koje treba dostaviti odredištu. U zaštitnom koderu se informacionim bitima dodaju zaštitni (kontrolni, sa informacione tačke gledišta suvišni) biti koji omogućavaju da se greške pri prenosu otkriju, pa eventualno i isprave u zaštitnom dekoderu.

U slučaju kada pojavljivanje simbola na izlazu diskretnog kanala ne zavisi od prethodno primljenih (tj. emitovanih) signala, radi se o **kanalu bez memorije**.

### ***Diskretni kanali bez memorije***

Diskretni kanal bez memorije je definisan (opisan) sa listom ulaznih simbola  $X\{X_1, X_2, \dots, X_r\}$ , listom izlaznih simbola  $Y\{Y_1, Y_2, \dots, Y_s\}$  i skupom odgovarajućih uslovnih vjerovatnoća pojavljivanja izlaznih simbola kada se emituje jedan (bilo koji) ulazni simbol  $P(Y_j | X_i)$  ( $i=1, 2, \dots, r, j=1, 2, \dots, s$ ).

Dakle,  $P(Y_j | X_i)$  je uslovna vjerovatnoća da će se na izlazu kanala pojaviti simbol  $Y_j$ , ako je poslat simbol  $X_i$ .



Broj izlaznih simbola ne mora da bude jednak broju ulaznih simbola.

U slučaju da kanal ne unosi nikakva izobličenja i kada u njemu ne bi bilo nikakvih smetnji (šumova) i kada bi mu karakteristike bile poznate i nepromjenljive u vremenu, po prijemu jednog signala ne bi uopšte postojala nedoumica koji je simbol poslan. Međutim, u realnim kanalima, postoje smetnje i šumovi koji mogu odlučivač da dovedu u nedoumicu – da po prijemu signala ne može da bude potpuno siguran koji je signal (tj. simbol) emitovan. Sve se ovo izražava preko vjerovatnoće i kanal je okarakterisan ovim uslovnim vjerovatnoćama.

Skup uslovnih vjerovatnoća može se prikazati u obliku tzv. kanalne matrice, gdje indeks  $i$  pokazuje redni broj vrste (tj. ulaznog simbola), a indeks  $j$  redni broj kolone (izlaznog simbola)

$$P = [P_{ij}] = \begin{bmatrix} P(Y_1 | X_1) & \dots & P(Y_s | X_1) \\ P(Y_1 | X_2) & \dots & P(Y_s | X_2) \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ P(Y_1 | X_r) & \dots & P(Y_s | X_r) \end{bmatrix}_{r \times s}$$

gdje je  $r$  – broj ulaznih simbola (ulazna lista)  
 $s$  – broj izlaznih simbola (izlazna lista)

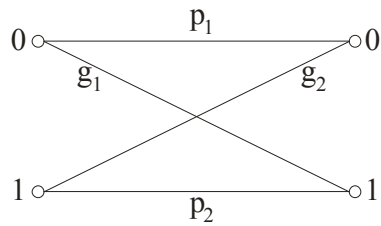
**Zbir vjerovatnoća po vrstama mora biti jednak jedinici**

$$\sum_{j=1}^s P(Y_j | X_i) = 1 \quad (i = 1, 2, \dots, r)$$

Kanal sa najmanjim brojem simbola je **Binarni kanal (BC)** čija je matrica:

$$P_{BC} = \begin{bmatrix} p_1 & g_1 \\ g_2 & p_2 \end{bmatrix} \quad \begin{array}{l} P(0 | 0) = p_1 \\ P(1 | 1) = p_2 \end{array} \quad \begin{array}{l} P(1 | 0) = g_1 \\ \underbrace{P(0 | 1) = g_2}_{\text{vjerovatnoća da je došlo do greške}} \end{array}$$

Umjesto kanalnom matricom, kanal se često može predstaviti i grafom koji je prikazan na sledećoj slici:



Poseban oblik binarnog kanala je **Binarni simetrični kanal (BSC)** definisan kanalnom matricom:

$$P_{BSC} = \begin{bmatrix} p & g \\ g & p \end{bmatrix} \quad (p + g = 1)$$

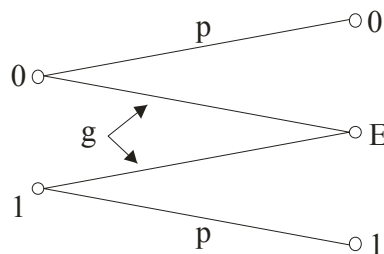
Pod simetrijom se podrazumijeva da su vjerovatnoće prelaska **0** u **1** i **1** u **0** podjednake. Ovo je najjednostavniji mogući kanal opisan samo jednim parametrom  $p(g)$  za koji se pokazuje da mu je vrijednost jednaka vjerovatnoći greške ( $Q_e$ ). U ovom slučaju vjerovatnoća greške ne zavisi od vjerovatnoća pojavljivanja simbola na ulazu u kanal.

Međutim, kod običnog binarnog kanala **vjerovatnoća greške** je:

$$Q_e = P(X_1) \cdot g_1 + P(X_2) \cdot g_2$$

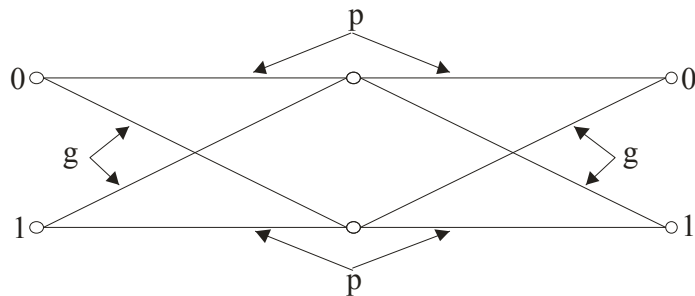
U slučaju kada je ulaz kanala binarni (0, 1), a na izlazu se pojavljuju tri različita simbola (0, 1 i E), tj. pojavljuje se niz tipa 010E10EE010....., simbol E znači da je bit koji se posmatra vjerovatno pogrešan. Ovo se zove **Binarni kanal sa brisanjem (BEC)** čija je kanalna matrica:

$$P_{BEC} = \begin{bmatrix} p & g & 0 \\ 0 & g & p \end{bmatrix} \quad (p + g = 1)$$



Graf za BEC

U slučaju kada imamo kaskadnu vezu više BC ili BSC kanala, postavlja se pitanje da li se ova kaskadna veza može zamijeniti jednim ekvivalentnim kanalom?



*Kaskadna veza dva identična BSC*

Ekvivalentni kanal je opet BSC, a njegova matrica se dobija množenjem kanalnih matrica osnovnog binarnog kanala.

$$P_{EKV} = \begin{bmatrix} p^2 + g^2 & 2pg \\ 2pg & p^2 + g^2 \end{bmatrix}$$

Kada broj kaskadno vezanih kanala raste, vjerovatnoća greške na ukupnoj trasi sve više teži ka 0,5 pa neće biti moguć nikakav prenos.

## ***Odnosi vjerovatnoća u kanalu***

Neka je dat diskretni kanal bez memorije definisan matricom  $P$  dimenzija  $r \times s$ . Njeni elementi su uslovne vjerovatnoće pojavljivanja simbola na izlazu kada je emitovan simbol u kanal  $P(Y_j | X_i) = P_{ij}$ , možemo ih zvati i **vjerovatnoće prelaza**.

Ako su poznate i vjerovatnoće ulaznih simbola  $P(X_i)$  ( $i = 1, 2, \dots, r$ ) – **ulazne vjerovatnoće**, tada se mogu naći i vjerovatnoće izlaznih simbola (**izlazne vjerovatnoće**) kao:

$$P(Y_j) = \sum_{i=1}^r P(X_i) \cdot P_{ij} \quad (j = 1, 2, \dots, s)$$

Dakle, na osnovu ulaznih i prelaznih vjerovatnoća mogu se uvijek naći izlazne vjerovatnoće.

I ulazne i izlazne vjerovatnoće moraju zadovoljavati jednakosti:

$$\sum_{i=1}^r P(X_i) = 1 \quad \sum_{j=1}^s P(Y_j) = 1$$

**Primjer:**

Neka je dat BSC gdje je  $p = g = 0,5$  i neka je  $P(X_1) = a$  i  $P(X_2) = b$  ( $a + b = 1$ ) tada je:

$$P(Y_1) = P(X_1) \cdot P(Y_1 | X_1) + P(X_2) \cdot P(Y_1 | X_2) = a \cdot p + b \cdot g = 0,5(a + b) = 0,5$$

$$P(Y_2) = P(X_1) \cdot P(Y_2 | X_1) + P(X_2) \cdot P(Y_2 | X_2) = a \cdot g + b \cdot p = 0,5(a + b) = 0,5$$

**Zaključak:**

$P(Y_1) = P(Y_2) = 0,5$  bez obzira kolike su ulazne vjerovatnoće.

U slučaju kada znamo koji je izlazni simbol  $Y_j$  primljen tada vjerovatnoću da je poslat  $X_i$  računamo po formuli:

$$P(X_i | Y_j) = \frac{P(X_i) \cdot P(Y_j | X_i)}{P(Y_j)} = \frac{P(X_i) \cdot P(Y_j | X_i)}{\sum_{i=1}^r P(X_i) \cdot P(Y_j)}$$

Ove vjerovatnoće se zovu **aposteriorne vjerovatnoće**.

**Primjer:**

Neka je dat BC definisan matricom:

$$P = \begin{bmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{10} & \frac{9}{10} \end{bmatrix}$$

Treba odrediti sve nepoznate vjerovatnoće ako su ulazne vjerovatnoće:

$$P(X_1) = \frac{3}{4} \text{ i } P(X_2) = \frac{1}{4}$$

**a) Izlazne vjerovatnoće su:**

$$P(Y_1) = P(X_1) \cdot P(Y_1 | X_1) + P(X_2) \cdot P(Y_1 | X_2) = \frac{3}{4} \cdot \frac{2}{3} + \frac{1}{4} \cdot \frac{1}{10} = \frac{21}{40}$$

$$P(Y_2) = P(X_1) \cdot P(Y_2 | X_1) + P(X_2) \cdot P(Y_2 | X_2) = \frac{3}{4} \cdot \frac{1}{3} + \frac{1}{4} \cdot \frac{9}{10} = \frac{19}{40}$$

$$P(Y_1) + P(Y_2) = \frac{21}{40} + \frac{19}{40} = 1 \text{ (provjera)}$$

**b)** Aposteriorne vjerovatnoće su:

$$P(X_1 | Y_1) = \frac{P(X_1) \cdot P(Y_1 | X_1)}{P(Y_1)} = \frac{20}{21}; \quad P(X_2 | Y_2) = \frac{P(X_2) \cdot P(Y_2 | X_2)}{P(Y_2)} = \frac{9}{19}$$

Na sličan način se mogu naći i dvije preostale aposteriorne vjerovatnoće. Međutim, može se računati i mnogo jednostavnije znajući da je:

$$P(X_1 | Y_1) + P(X_2 | Y_1) = 1 \Rightarrow P(X_2 | Y_1) = 1 - P(X_1 | Y_1) = \frac{1}{21}$$

$$P(X_1 | Y_2) + P(X_2 | Y_2) = 1 \Rightarrow P(X_1 | Y_2) = 1 - P(X_2 | Y_2) = \frac{10}{19}$$

**c)** Združene vjerovatnoće su:

$$P(X_1, Y_1) = P(Y_1) \cdot P(X_1 | Y_1) = \frac{20}{21} \cdot \frac{21}{40} = \frac{1}{2}$$

ili

$$P(X_1, Y_1) = P(X_1) \cdot P(Y_1 | X_1) = \frac{3}{4} \cdot \frac{2}{3} = \frac{1}{2}$$

Ostale združene vjerovatnoće su:

$$P(X_1, Y_2) = \frac{1}{4}; \quad P(X_2, Y_1) = \frac{1}{40}; \quad P(X_2, Y_2) = \frac{9}{40}$$

## ***Apriorna i aposteriorna entropija***

Apriorna entropija ulazne liste, mjera neizvjesnosti o tome koji će simbol biti emitovan:

$$H(X) = \sum_{i=1}^r P(X_i) \cdot \log\left(\frac{1}{P(X_i)}\right)$$

Apriorna entropija izlazne liste, mjera neizvjesnosti o tome koji će simbol biti primljen:

$$H(Y) = \sum_{j=1}^s P(Y_j) \cdot \log\left(\frac{1}{P(Y_j)}\right)$$

Uslovna (aposteriorna) entropija ulazne liste, mjera neizvjesnosti o tome šta je emitovano, ako se zna šta je primljeno (neki autori je zovu "entropija šuma"):

$$H(X | Y) = \sum_{i=1}^r \sum_{j=1}^s P(X_i, Y_j) \cdot \log\left(\frac{1}{P(X_i | Y_j)}\right)$$

Uslovna (aposteriorna) entropija izlazne liste, mjera neizvjesnosti o tome koji će simbol biti primljen, ako se zna koji je simbol emitovan:

$$H(Y | X) = \sum_{i=1}^r \sum_{j=1}^s P(X_i, Y_j) \cdot \log \left( \frac{1}{P(Y_j | X_i)} \right)$$

Združena entropija, mjera neizvjesnosti o sistemu u cjelini:

$$H(Y, X) = \sum_{i=1}^r \sum_{j=1}^s P(X_i, Y_j) \cdot \log \left( \frac{1}{P(X_i, Y_j)} \right)$$

### ***Međusobne informacije (prenesene)***

Sada je definisano dovoljno elemenata da se sa gledišta teorije informacija opiše kako se informacije prenose kroz kanal i da se odredi količina informacija koja se prenosi.

Srednja količina prenesenih informacija po jednom simbolu je:

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

### ***Osobine količine prenesenih informacija:***

1.  $I(X; Y) \geq 0$
2.  $0 \leq I(X; Y) \leq H(X)$
3.  $I(X; Y) = I(Y; X)$

**Primjer:**

Neka je dat BSC definisan kanalnom matricom:  $P_{BSC} = \begin{bmatrix} p & g \\ g & p \end{bmatrix}$  ( $p + g = 1$ )

i neka su vjerovatnoće ulaznih simbola  $P(X_1) = a$ ,  $P(X_2) = b$  ( $a + b = 1$ )

Vjerovatnoće izlaznih simbola su:

$$P(Y_1) = ap + bg \quad P(Y_2) = ag + bp$$

Međusobna informacija je:

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y, X) = H(Y) - \sum_{i=1}^r \sum_{j=1}^s P(X_i, Y_j) \cdot \log \left( \frac{1}{P(Y_j | X_i)} \right) = \\ &= H(Y) - \sum_{i=1}^r P(X_i) \sum_{j=1}^s P(Y_j | X_i) \cdot \log \left( \frac{1}{P(Y_j | X_i)} \right) = \\ &= H(Y) - \sum_{i=1}^r P(X_i) \left( p \cdot \log \frac{1}{p} + g \cdot \log \frac{1}{g} \right) = \\ &= H(Y) - \left( \underbrace{a+b}_1 \right) \cdot \left( p \cdot \log \frac{1}{p} + g \cdot \log \frac{1}{g} \right) = \\ &= H(Y) - \left( p \cdot \log \frac{1}{p} + g \cdot \log \frac{1}{g} \right) = \\ &= (ap + bg) \cdot \log \left( \frac{1}{ap + bg} \right) + (ag + bp) \cdot \log \left( \frac{1}{ag + bp} \right) - \left( p \cdot \log \frac{1}{p} + g \cdot \log \frac{1}{g} \right) \end{aligned}$$



## ***Kapacitet kanala (C)***

Kapacitet kanala je mjera koja kaže koliko se informacija može dobiti korišćenjem kanala, tj. ako je kapacitet kanala 0,7 bita, to znači da za jedan simbol ulaznog alfabeta koji je emitovan u kanal, na izlazu dobijamo 0,7 bita korisne informacije.

Kapacitet kanala (C) je jednak **maksimalnoj vrijednosti** međusobne (prenesene) informacije:

$$C = \max[I(X; Y)]$$

### ***Osobine:***

1.  $C \geq 0$
2.  $C \leq H(X) = \log r$  - gdje je  $r$  broj ulaznih simbola
3.  $C \leq H(Y) = \log s$  - gdje je  $s$  broj izlaznih simbola

## ***Kapaciteti nekih kanala***

### ***1. Kanal bez smetnji***

Kod ovog kanala za svako  $X$  na ulazu dobijamo odgovarajuće  $Y$  na izlazu.

$$C = \max[I(X; Y)] = \max[H(X) - H(X | Y)] = \max[H(Y) - H(Y | X)]$$

$$C = \max[H(X)] \text{ ili } \max[H(Y)]$$

$$C = \log r \text{ ili } C = \log s$$

U slučaju binarnog kanala, kada su ulazni simboli jednako vjerovatni:

$$P(X) = \left\{ \frac{1}{2}, \frac{1}{2} \right\} \quad C = 1 \text{ bit}$$

### ***2. Kanal sa šumom nedovoljnim da promjeni poslanu informaciju***

U slučaju binarnog kanala sa podjednako vjerovatnim ulazima:

$$P(X) = \left\{ \frac{1}{2}, \frac{1}{2} \right\} \quad C = 1 \text{ bit}$$

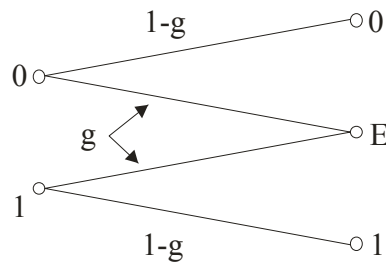
**3. Kanal za prenos binarnih poruka sa vjerovatnoćom greške  $g$**

$$C = 1 - H(g)$$

gdje je:  $H(g) = g \cdot \log \frac{1}{g} + (1 - g) \log \frac{1}{1 - g}$

**4. Binarni kanal sa brisanjem**

$$P_{BEC} = \begin{bmatrix} 1 - g & g & 0 \\ 0 & g & 1 - g \end{bmatrix}$$



Vjerovatnoća da je prenos korektan je  $1 - g$ , dok je vjerovatnoća da je poruka izbrisana i nije primljena  $g$ .

$$I(X; Y) = H(Y) - H(Y | X) = H(Y) - H(g)$$

$$C = 1 - H(g)$$