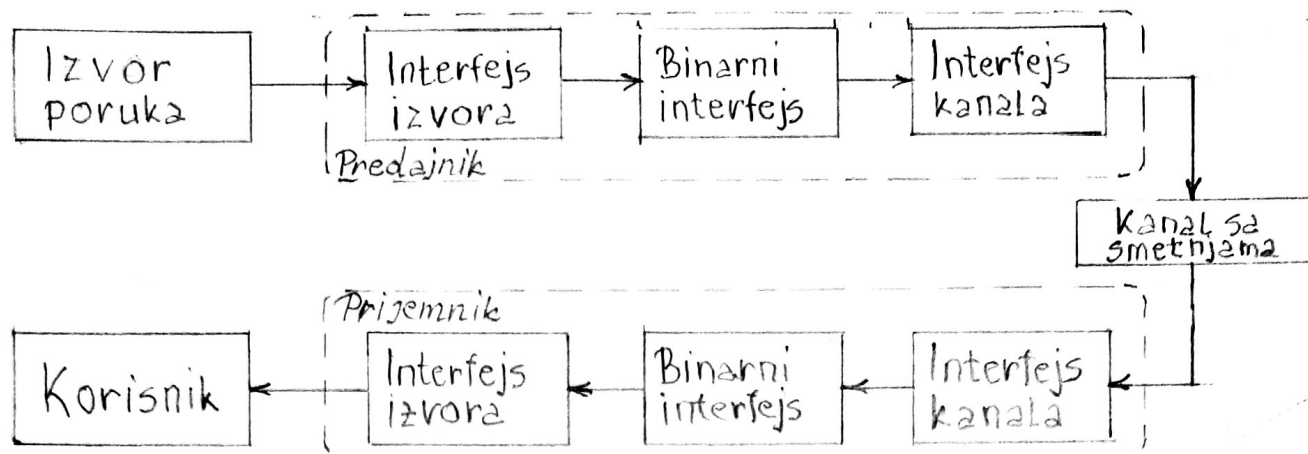


P.M.T. Domaći 1

1.



Izvor - emituje poruke, može biti kontinualan ili diskretan, analogan ili digitalan i deterministički ili slučajen

Interfejs izvora - dizajnira se u skladu sa osobinama izvora, kontinualni signal diskretizacijom pretvara se u niz realnih brojeva koji kvantizacijom prelaze u sekvencu digitalnih simbola koje statistički koder pretvara u binarne simbole.

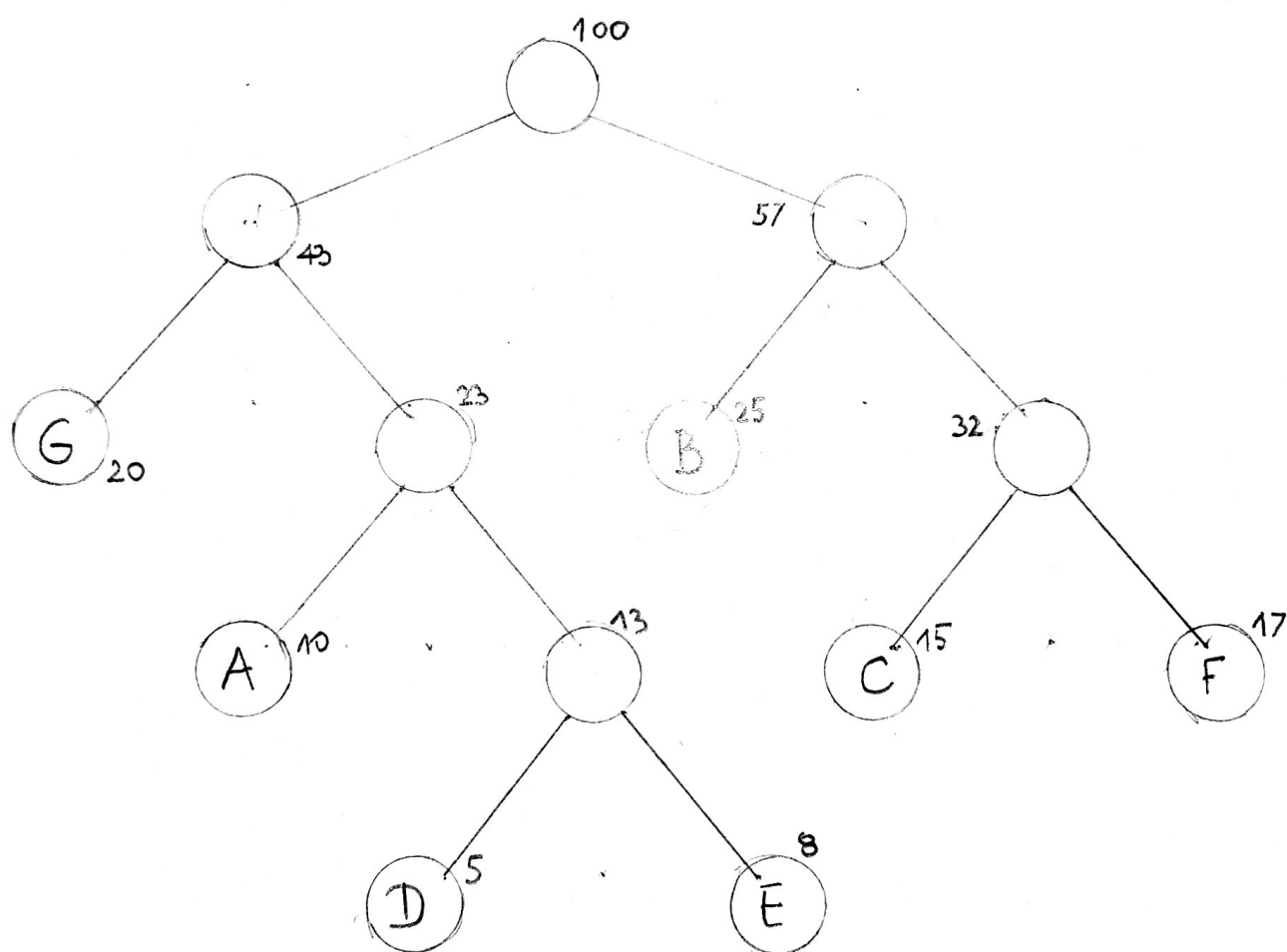
Binarni interfejs - obrada i skladištenje podataka se obavlja u njemu, koristi digitalni hardver. Jednostavno spaja podatke iz različitih izvora, tj. on ne zavisi od tipa poruka izvora ili medijuma za prenos.

Interfejs kanala - zavisi od osobina kanala, čine ga zaštitni koder; koji sekvencu binarnih simbola menja tako da bude više otporna na greške i modulator; koji pretvara binarne simbole u signal pogodan za prenos preko kanala (kontinualni signal).

Kanal - medijum koji služi za prenos informacija (bakarna žica, atmosfera), u njemu dolazi do slabljenja i izobličenja signala usled nesavršenosti fizičkog medijuma.

2. Konstrukcija Huffmanovog koda pomoću stabla se vrši tako što:
1. poredamo simbole u niz po njihovim verovatnoćama po neopadajućem redosledu
 2. uzmemo dva simbola sa najmanjim verovatnoćama i stavimo ih za sinove novog čvora, čija je verovatnoća njihov zbir.
 3. ubacimo taj novi čvor u niz.
 4. vratimo se na 1. korak sve dok nam ne ostane samo jedan čvor

Za date verovatnoće proces konstrukcije stabla je:



Kod Huffmanovog stabla simboli su isključivo u listovima i ono ima sibling property zato lako možemo da proverimo da li je ovo Huffmanovo stablo.

$$H = -(0.1 \log_2(0.1) + 0.25 \log_2(0.25) + 0.15 \log_2(0.15) + 0.05 \log_2(0.05) + 0.08 \log_2(0.08) + 0.17 \log_2(0.17) + 0.2 \log_2(0.2)) = 2.65$$

$$L = 0.1 \cdot 3 + 0.25 \cdot 2 + 0.15 \cdot 3 + 0.05 \cdot 4 + 0.08 \cdot 4 + 0.17 \cdot 3 + 0.2 \cdot 2 = 2.68$$

$$\eta = \frac{H}{L} \cdot 100\% = 98.9\%$$

$$P = \frac{\lceil \log_2 9 \rceil}{L} = 1.12$$

3. Kod sa ponavljanjem šalje isti bit kroz kanal više puta:

Prvi način odlučivanja je FEC - ako niz bitova koji dođe na prijemnik ima barem jedan bit koji se razlikuje od ostalih od predajnika se traži da se ponovo pošalje ta sekvenca bitova.

Drugi način odlučivanja je ARQ - iz niza bitova koji dođe na prijemnik se prebroji broj jedinica i broj nula, za dekodovan bit se uzima onaj kojih ima više.

Verovatnoća greške za oba su za $n=9$, $p=10^{-1}$:

FEC

$$p^n = (10^{-1})^9 = 10^{-9}$$

ARQ

$$p^n - \binom{n}{n-1} p^{n-1} (1-p)^{n-8} + \binom{n}{n-2} p^{n-2} (1-p)^{n-7} + \binom{n}{n-3} p^{n-3} (1-p)^{n-6} + \binom{n}{n-4} p^{n-4} (1-p)^{n-5} = 8.91 \cdot 10^{-4}$$

Maksimalni kodni količnik je

$$I_{MAX} = 1 - (1-p) \log_2\left(\frac{1}{1-p}\right) - p \log_2\left(\frac{1}{p}\right) = 0.531$$

4. Hemingov 7,4 kod označava da ima 7 bitova ukupno, od kojih su 4 informaciona, a ostala 3 zaštitna. Zaštitni bitovi se nalaze na pozicijama stepena dvojke počevši od nultog i računaju se kao XOR određenih informacionih bitova.

Ako nam ne treba neki od informacionih bitova možemo da

skratimo naš kod tako što uklonimo bit sa najviše pozicije, na taj način se od Fleming 7,4 može dobiti Fleming 6,3.

Takođe, na najvišoj poziciji, možemo dodati jedan specijalan zaštitni bit, bit provere parnosti, koji se računa kao XOR svih bitova pre njega, i tako od Fleming 6,3 dobijamo 7,3.

Ako nemamo bit parnosti i na ulaz nam stigne sekvenca koja daje da je sindrom 0 onda to tumačimo kao da nemamo grešku, ako sindrom nije 0 on će da pokazuje na mesto na kome se desila greška u slučaju da je bila samo jedna greška, ako je bilo više grešaka ispravljanje sindroma samo može da pogorša stvari.

Ako imamo bit parnosti, a on i sindrom su 0 znači da nije bilo greške pri prenosu, ako je u ovom slučaju bit parnosti 1 onda je greška na bitu parnosti. Ako je sindrom veći od 0, a bit parnosti je 1 znači da imamo neparan broj grešaka i ako je broj tih grešaka jedan, sindrom pokazuje na njenu poziciju.

Ako nam sindrom nije 0, a bit parnosti jeste onda imamo paran broj grešaka.

55. Na jednom kraju generišemo neki prost broj p i neke brojeve g i a koji su manji od $p-1$. Od njih napravimo broj $A = g^a \bmod p$ koji šaljemo kroz kanal drugom kraju zajedno sa g i p .

Na drugom kraju pravimo broj b koji mora biti isto manji od $p-1$ i računamo ključ $K = A^b \bmod p$ i broj $B = g^b \bmod p$ koji šaljemo kroz kanal prvom kraju koji ga koristi da izračuna ključ identičan onome koji je na drugom kraju $K = B^a \bmod p$.

Ovim načinom smo omogućili da obe strane imaju isti ključ, a da on nikad nije prošao kroz kanal, a parametre za računanje ključa a i b ne možemo da jednoznačno odredimo zato što

se ovde radi o diskretnom Logaritmu koji ima više rešenja za iste brojeve i time mi čuvamo tajnost ključeva.

Pretinja ovom algoritmu je man-in-the-middle napad koji se oslanja na činjenicu da strane međusobno ne proveravaju da li je poruka stvarno stigla od suprotne strane ili je neko izmenio, dodao ili obrisao neke poruke.

Zadatak 1

Parametar N je 3, a K je 8.

Kodne reči:

000000 - $d=0$

011001 - $d=3$

111111 - $d=6$

100110 - $d=3$

010101 - $d=3$

001101 - $d=2$

101010 - $d=3$

110011 - $d=4$

Broj kodnih reči sa težinom:

$d=0-1$

$d=1-0$

$d=2-1$

$d=3-4$

$d=4-1$

$d=5-0$

$d=6-1$

Ovaj kod može da detektuje 1 grešku, a ispravi 0 grešaka.

Zadatak 2

Ako bi se umesto generišuće matrice iz prvog zadatka usvojila

0	0	0	1	1	1
0	1	1	0	0	1
1	0	1	0	1	0

generišuća matrica koja detektuje i ispravlja jednu grešku, bi mogla da otkloni sve greške za parametre interlivera veće ili jednake 4, a manje od 16, tako da su za te parametre informacije na ulazu i izlazu identične.

7

Verovatnoća greške u ovom kodu koji detektuje i ispravlja samo 1 grešku se računa kao suma verovatnoći da se greška pojavi na više od jednog bita, to jest:

$$\binom{6}{6}p^6 + \binom{6}{5}p^5(1-p) + \binom{6}{4}p^4(1-p)^2 + \binom{6}{3}p^3(1-p)^3 + \binom{6}{2}p^2(1-p)^4$$