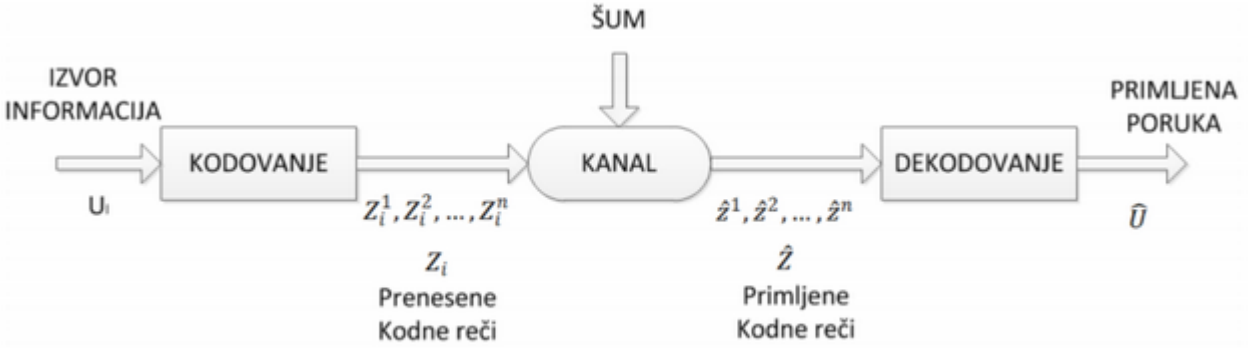
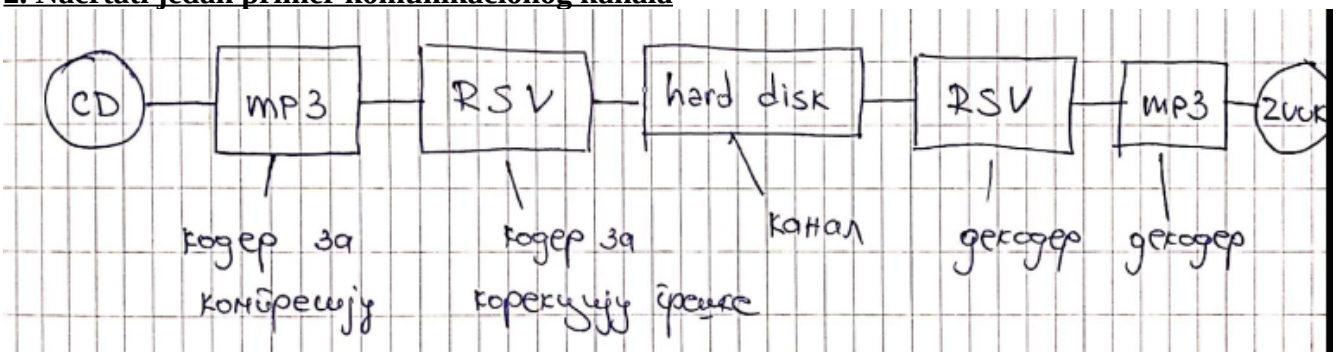
1. <u>Nacrtati opšti model komunikacionog kanala</u>



2. <u>Nacrtati jedan primer komunikacionog kanala</u>



3. <u>Šta je entropija? Napisati formulu</u>

Entropija jeste mera neizvesnosti posmatrača o nekom izvoru informacija. Što su posmatrane verovatnoće sličnije to je entropija bliža jedinici. Da bismo izračunali entropiju prvo moramo da posmatramo nešto što se zove iznenadjenje, na primer, ako imamo 10 kuglica, od toga 5 crevene boje (p = 0.5), 4 plave (p = 0.4) i jednu žutu (p = 0.1) moramo se zapitati koliko ćemo "se iznenaditi" ako izvučemo žutu u našem slučaju naše "iznenadjenje" biće 1 / 0.1 = 10 za slučaj žute, 1 / 0.4 = 2.5 za plavu i 1 / 0.5 = 2 za crvenu. Vidimo da je najmanje iznenadjenje izvući crvenu.
Sada, mi možemo izračunati i koliko je nasumičan naš rezultat, tj. koliko "haosa" i nepredvidljivosti ima u našem izvlačenju kuglica. To računamo formulom:

$$E = \sum p_i * \log_2(\frac{1}{p_i})$$

Tj. entropija je jednaka sumi proizvoda verovatnoće sa logaritmom (osnova 2) iznenadjenja. U našem primeru dobijamo da je E = 1.36 što nam govori da je faktor haosa koji vlada u našem izvlačenju jednak 1.36.

4. <u>Osobine entropije</u>

Entropija ima 4 glavne osobine:

1. **Kontinualnost** - entropija je neprekidna funkcija svojih argumenata
2. **Simetričnost** - entropija se ne menja ako se menja redosled simbola
3. **Ekstremna vrednost** - kad su svi simboli podjednako verovatni, entropija treba da ima maksimalnu vrednost
4. **Aditivnost** - entropija unije 2 nezavisna dogadjaja mora biti jednaka zbiru njihovih entropija

5. Napisati formulu za dužinu kodne reči

$$L = \sum (l_i * p_i)$$

l - dužina bitova datog simbola
p - verovatnoća datog simbola

6. Gde se najčešće koristi Hemingov kod?

Hemingov kod se koristi prilikom ispravljanja grešaka koje su nastale prilikom transfera informacija. U umreženom sistemu, takve greške se vrlo retko dešavaju jer šum nije prevelik, ali ako govorimo o komunikaciji satelita sa zemljom, onda može doći do velikih gubitaka i promena, a konzistentnost je mnogo bitnija od efikasnosti. Takodje, implementira se ovakav vid ispravljanja grešaka u hardverskom delu jer je relativno lako implementirati ga. ECC RAM koristi Hemingov kod da ispravi jednu grešku i da izbaci upozorenje da je došlo do dveju ili više grešaka.

7. Šta je Hemingovo rastojanje? Dati primer

Hemingovo rastojanje izmedju dve reči iste dužine, tj. dva niza dužine n je broj simbola (pozicija) u kojima se te dve reči razlikuju.

$z_1 = 101010$
$z_2 = 001011$
$d(z_1, z_2) = 2$

8. Šta je težina kodne reči?

Težina kodne reči jeste broj nenultih simbola u datoj reči, npr: w(10110) = 3, w(000000) = 0

9. Hemingov kod (12, 8) - šta označavaju brojevi kod oznake 12 i 8?

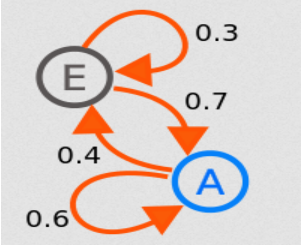
Hemingovi kodovi su porodica kodova za linearno ispravljanje grešaka. Kod ovih kodova enkodovanje je objašnjeno paritetom (jednakošću) bitova, koji primalac koristi prilikom ispravljanja grešaka.
Kod (12, 8) označava da se posle svakih 8 bitova dodaju 4-bitni pariteti. 12 označava koliko ukupno ima bitova (8 + 4), a 8 koliko ih ima bez pariteta. Ovaj kod može da ispravi 1-bitne greške na svakom bajtu.

10. Šta su Markovljevi izvori?

Markovljevi izvori informacija, ili jednostavno, Markovljevi izvori su izvori informacija čija je dinamika odredjena stacionarnim konačnim Markovljevim lancem.
Markovljevi izvori se često koriste u teoriji komunikacija kao model odašiljača. Ako je dat Markovljev izvor, čiji je Markovljev lanac nepoznat moguće je, preko tehnika "sakrivenog Markovljevog modela", kao što je Viterbijev algoritam, dobiti i Markovljev izvor.

11. Homogeni Markovljev lanac

Homogeni Markovljev lanac je sekvenca nasumičnih promenljivih, poznatija kao stohastički proces, u kome vrednost sledeće promenljive zavisi samo od vrednosti trenutne promenljive, bez obzira na promenljivu iz prošlosti.
Na primer, ako mašina ima dva stanja A i E, ako je u stanju A, postoji 40% šansa da će preći u stanje E, a 60% da će ostati u stanju A. Kada je u stanju E, postoji 70% šansa da će preći na A i 30% da će ostati na E. Ako odredimo X_0 ... X_n da su promene stanja (ili ostajanje u istom) onda je X_0 početno stanje, a X_{10} nasumična promenljiva koja opisuje stanje nakon 10 tranzicija.



12. Markovljevi lanci s kontinuiranim parametrom

Isto kao homogeni lanci, samo se stanje menja na osnovu eksponencijalne nasumične promenljive

13. Napisati Kraft-Mekmilanovu nejednakost

Kraft-Mekmilanova nejednakost kaže da postoji binarni prefiks kod sa dužinom kodne reči l_1, ..., l_n ako i samo ako se zadovoljava sledeća formula:

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

14. Polje Galoa

Konačno polje, ili polje Galoa (GF) jeste polje koje sadrži konačan broj elemenata u kom su definisana pravila operacija množenja, deljenja, sabiranja i oduzimanja, kao i neka osnovna pravila. Najčešći primeri konačnih polja su u celim brojevima po modulu *p*, gde je *p* prost broj. Pa tako za GF(2) možemo koristiti samo brojeve 0 i 1 (binarne), u slučaju GF(5) možemo koristiti 0, 1, 2, 3 i 4, a u tom polju važi 4 + 2 = 1

15. Prva Šenonova teorema

Prva Šenonova teorema, ili Šenonova teorema o izvoru koda (takodje i teorema kodovanje bez šumova), uspostavlja granice moguće kompresije podataka, uz to daje i praktično značenje Šenonove entropije. 1948. godine ovu teoremu dokazao je Klod Šenon koji je zaključio da je nemoguće izvršiti kompresiju, a da prosečan broj bita po simbolu bude manji od entropije izvora datih simbola, tj. ako je manji - dolazi do gubitka informacije.

Medjutim, on je ustanovio da je moguće vršiti kompresiju gde će broj bita po simbolu biti približan entropiji sa malom verovatnoćom gubitka informacije.

Kompresija može najviše ići do nivoa gde se svaki simbol u proseku predstavlja sa onoliko bita koliko iznosi entropija izvora.

$$\lim_{n \to \infty} \frac{L_{sr,n}}{nH(s)} = 1$$

16. Druga Šenonova teorema

Druga Šenonova teorema, ili teorema kodiranja kanala sa šumom, iskazuje da za bilo koji stepen kontaminacije šumova u komunikacionom kanalu, moguće je (u teoriji) raditi primopredaju diskretnih podataka (digitalne informacije) gotovo bez greške do maksimalnog protoka kroz kanal.

Šenonov limit, ili Šenonov kapacitet, komunikacijskog kanala označava maksimalni protok podataka bez grešaka koji se teoretski mogu preneti kroz kanal uz odredjen šum.

Sama teorema opisuje maksimalnu moguću efikasnost ispravljačkih metoda protiv interferencije šumova i korumpiranja podataka.

17. <u>Diskretni kanali bez memorije</u>

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

Diskretni kanal bez memorije je definisan sa listom ulaznih simbola X $\{X_1 \dots X_n\}$ i listom izlaznih simbola Y $\{Y_1 \dots Y_n\}$ i skupom odgovarajućih uslovnih verovatnoća pojavljivanja izlaznih simbola kada se emituje jedan (bilo koji) ulazni simbol $P(Y_j \mid X_i)$ (i = 1, 2, ..., r ; j = 1, 2, ..., s). Dakle. simbol $P(Y_j \mid X_i)$ je uslovna verovatnoća da će se na izlazu kanala pojaviti simbol Y_j ako je poslat simbol X_i.

Bitno je napomenuti da broj izlaznih simbola ne mora biti jednak broju ulaznih simbola.

18. <u>Diskretni kanali sa memorijom</u>

Kao i kod kanala bez memorije i u ovim kanalima izlazni simbol zavisi od tekućeg ulaznog simbola uz pretpostavku da se ne radi o kanalu sa anticipacijom, tj. da tekući izlazni simbol ne zavisi od budućih ulaznih simbola (već samo od trenutnih). Može se smatrati da je kanal sa memorijom opisan skupovima ulaznih i izlaznih simbola, skupom stanja i skupom uslovnih verovatnoća pojave izlaznog simbola prelaska u novo stanje, kada se znaju tekući ulazni simbol i prethodno stanje.

19. <u>Kapacitet kanala</u>

Kapacitet kanala meri sposobnost jednog kanala da prenosi informacije. To je maksimalna prosečna količina informacija koje ulaz kanala može preneti na izlaz.

Kapacitet se označava sa C i u slučaju diskretnog kanala bez memorije formula glasi:

$$C = \max_{px} = I(X;Y)$$

Gde je X ulaz u kanal sa verovatnoćama pX(x), a Y izlaz kanala. Maksimalna informacija kroz kanal se računa:

$$I_{max} = \max_{p(xi)} = I(X;Y)$$

Gde se maksimiranje vrši variranjem skupa ulaznih verovatnoća koje moraju biti veće od 0, a njihov zbir mora biti jednak jedinici.

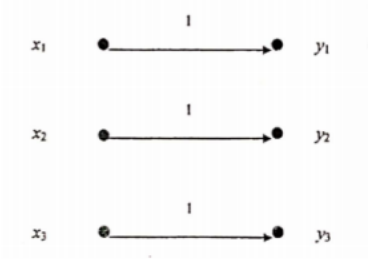
20. <u>Idealni kanal</u>

Kanal je idealan ako njegova kanalna matrica ima po jedan nenulti element u svakoj vrsti i svakoj koloni. Taj element mora biti jednak jedinici, a prenumerisanjem simbola ova matrica se može svesti na jediničnu matricu:

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Kod idealnog kanala važi:

$$I_{max} = max\, H(X) = max\, H(Y) = 1\,d\,r = 1\,d\,s$$



21. Rejlijev slučajni proces

Rejlijev slučajni proces, ili Rejlijeva distribucija, jeste kontinualna distribucija verovatnoće ne-negativnih nasumičnih vrednosti. Najčešće se koristi kada je intenzitet vektora u nekom prostoru u relaciji sa svojim direkcionalnim komponentama (smerom i pravcem).
U teoriji informacija ova distribucija se koristi za modeliranje prijemnika koji obradjuje gusto razbacane signale.

22. Rajsov slučajni proces

Ova distribucija se koristi u analizi prijemnika prilikom radio komunikacije.

23. Hojtov slučajni proces

Zove se i Nakagami-q proces. Koristi se u proučavanju odnosa signal-ka-šumu na prijemnicima.

24. Nakagami-m slučajni proces

Ova distribucija je u vezi sa gama distribucijom. Koristi se radi modeliranja fizičkih fenomena, kao što su oni koji se dobijaju prilikom ultra zvuka u medicini, komuniciranju, meteorologiji, hidrologiji, multimediji itd.

25. Šta su trenutni statistički kodovi?
Ne znam

26. Šta su binarni BCH kodovi?

Bose - Chaudhuri - Hocquenghem kodovi formiraju klasu cikličnih kodova za ispravljanje grešaka koji se konstruišu pomoću polinoma nad konačnim poljem. Ključna karakteristika ovih kodova jeste što prilikom implementiranja postoji precizna kontrola nad ispravljanjem grešaka u simbolima - moguće je dizajnirati binarne BCH kodove koji mogu ispraviti (nama) najbitnije greške.
Još jedna prednost je lakoća dekodovanja BCH kodova primenom algebarske metode poznate kao dekodiranje sindroma, što prilikom primene u stvarnom svetu troši vrlo malo hardverskih resursa.

27. Šta predstavlja verovatnoća greške?

Verovatnoća greške predstavlja verovatnoću prelaska 0 u 1 i 1 u 0 prilikom prenosa informacija, kod binarnog simetričnog kanala, verovatnoća greške je jednaka, dok je kod običnog binarnog kanala verovatnoća greške:

$$P_{BSC} = \begin{bmatrix} p & g \\ g & p \end{bmatrix}$$

$$Q_e = P(X_1) * g_1 + P(X_2) * g_2$$

28. Objasniti FDMA

Frequency-division multiple access je metoda za pristup kanalu koja se koristi u nekim višestruko-pristupnim (multiple-access) protokolima. FDMA omogućava više korisnika da šalju podatke kroz jedan komunikacioni kanal, kao što je kabl ili preko mikrotalasa, tako što deli protok kanala na nekoliko nepreklapajućih frekvencija koje se nazivaju "sub-channels" (tj. potkanali), gde svaki korisnik ima sebi dodeljen svoj sub-channel. Koristi se u satelitskom komuniciranju i prilikom podele telefonskih poziva.

29. Objasniti TDMA

Time-division multiple access je metoda za pristup kanalu koju koristi nekoliko standarda. Omogućava korišćenje iste frekvencije tako što deli signal u nekoliko vremenskih slotova. To znači da će različite stanice moći da dele isti medij (npr. preko frekvencija radio kanala) dok koriste samo deo svog kapaciteta. Dinamički TDMA omogućava varijabilno rezervisanje vremenskih slotova za varijabilne tokove podataka sa varijabilnim bit-rate-om koji zavisi od zahteva svakog toka.
Koristio se najviše u 2G mrežama.

30. Objasniti CDMA

Code-division multiple access je metoda za pristup kanalu koju koriste različite radio tehnologije. CDMA je primer multiple-access protokola, gde nekoliko odašiljača mogu poslati informaciju istvoremeno preko jednog komunikacionog kanala. Ovo dozvoljava korisnicima da koriste iste frekvencije. Da bi se ovo omogućilo bez interferencije izmedju korisnika, CDMA koristi "spread spectrum" tehnologije i specijalnu šemu za kodiranje da bi se odredjen kod dodelio odredjenom odašiljaču. CDMA optimizuje korišćenje odredjenog protoka jer ne limitira opseg korisničke frekvencije.
Koristi se u mnogim telefonskim standardima, kao npr. u 3G mrežama, ali od 2022. mnogi provajderi (u SAD) su odlučili da prekinu podršku za ovaj vid protokola.

31. Dupleks prenos

Dupleks komunikacioni sistem jeste onaj koji se sastoji iz sistema "2 čvora", tj. sistema koji je sačinjen od dve ili više povezane strane koji mogu komunicirati jedni sa drugima u oba smera. Postoje dva tipa dupleks prenosa:

1. **Half-duplex** - u ovom sistemu obe strane komuniciraju jedna sa drugom istovremeno, ali komuniciranje je samo u jednom smeru. Primeri half-duplex sistema je voki-toki, kao i radio u dva smera koji ima "push to talk" dugme. Kada neko želi da priča sa drugom stranom mora pritisnuti dugme, koje uključuje odašiljač, ali isključuje prijemnik što onemogućava slušanje druge strane, koju možemo čuti samo ako ne držimo dugme - tada se isključuje odašiljač, a uključuje se prijemnik
2. **Full-duplex** - u ovom slučaju obe (ili više) strane mogu komunicirati istovremeno. Primeri full-duplex-a su obični telefonski pozivi. Zvučnik reprodukuje govor druge strane istovremeno dok mikrofon prenosi govor drugoj strani. Komunikacija preko interneta (npr. instagram pozivi, skype, discord, teamspeak...) je full duplex koja zahteva i potiranje eha po najnovijim standardima

Postoji i **simplex** sistem koji ima mogućnost samo slanja podataka u jednom smeru, a po nekim definicijama, simplex jeste half-duplex.

32. Šta su binarne, a šta monohromatske slike?

Binarne slike su one koje imaju tačno dve boje, tj. boje su predstavljene binarnim brojnim sistemom 0 i 1, najčešće su te boje crna i bela, ali mogu biti kombinacija bilo koje dve boje.
Monohromatske slike su slike koje su sastavljene iz jedne boje - obično crno-bele što se zove grayscale, ali može se monohromatska slika napraviti iz bilo koje boje. U ovom slučaju dozvoljene su različite nijanse te boje, ali ne druga boja.
Primer monohromatske slike jeste ona koja se vidi pogledom kroz uredjaj za noćni vid (u tom slučaju boja je obično zelena).

33. Šta su konvolucioni kodovi?

U konvolucionim kodovima, poruka se sastoji iz toka podataka arbitarnih dužina i sekvence izlaznih bitova koji su generisani apliciranjem bulove algebre u sam tok podataka.

U blok kodovima, podaci se sastoje iz bloka podataka definitivne dužine, ali u konvolucionim kodovima, ulazni bitovi nisu podeljeni u blokove, već se ubacuju u tokove bitova, koji prave izlaz na osnovu logike samog enkodera.

Još jedna razlika u odnosu na blok kodove jeste što izlazna kodna reč zavisi, ne samo od trenutnog ulaza, već i od prethodnih ulaza koji se skladište u memoriji.

Za generisanje konvolucionih kodova, informacija se šalje sekvencijalno kroz shift-registar (koji nema beskonačno mnogo stanja). Registar se sastoji i iz generatora funkcija bulove algebre.

Konvolucioni kod se može predstaviti pomoću tri promenljive (n, k, K), gde je:

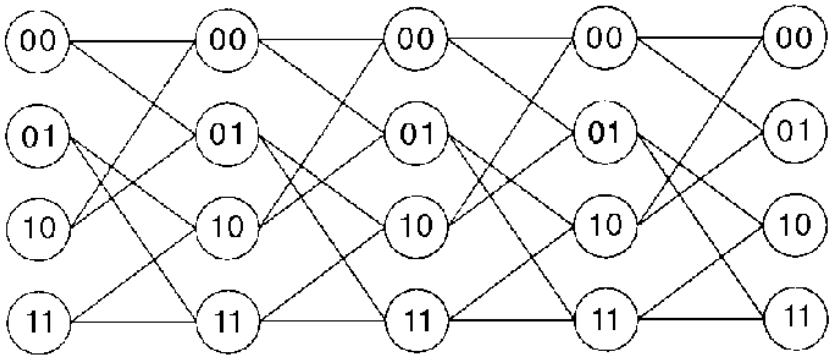
- *k* broj bitova koji se pomeraju (shift-uju) u enkoderu u jednom trenutku (obično je *k = 1*)
- *n* je broj izlaza iz enkodera koji zavise od k informacionih bitova
- Code-rate je $R_C = k / n$.
- Memorija enkodera je ograničena veličinom *k*
- *n* je funkcija trenutnih bitova na ulazu i sadržaja *K*
- Stanje enkodera je dato vrednošću od *(K - 1)* bita

34. Šta je trelis?

U arhitekturi trelis je ram koji se pravi ukrštanjem delova drveta, bambusa ili metala. Sličan izgled ima i trelis kao graf, a dobio je ime upravo zbog toga što liči na arhitektonsku strukturu.

Trelis je graf čiji su čvorovi poredjani u vertikalne isečke gde je svaki čvor u gotovo svakom isečku povezan sa bar još jednim čvorom - ili sa prethodnim ili sa sledećim. Prvi i poslednji isečak imaju samo jedan čvor (zato se kaže **u gotovo svakom**).

Trelisi se koriste u enkodovanju i dekodovanju u teoriji komunikacije i enkripciji. Jedan od primera gde se koriste trelisi je u konvolucionim kodovima



35. Šta je prefiksni kod?

Prefiksni kod je tip koda koji se izdvaja od ostalih jer poseduje "prefiksno svojstvo", koje zahteva da ne postoji cela kodna reč u sistemu koja je prefiks (inicijalni segment) bilo koje druge kodne reči u sistemu. Ako posmatramo {0, 1} možemo reći da je to prefiks kod jer svaki element (i 0 i 1) mogu se zapisati jednoznačno, ako gledamo {0, 1, 01} možemo primetiti da prilikom formiranja 01 mi imamo prefiks 0. Naravno, sve ovo je trivijalno i varijabilno zavisno od same poruke koja se šalje, ukoliko posmatramo prethodni primer {0, 1, 01}, može se desiti da je poslata poruka 10 iz koje je moguće zaključiti da je poruka prefiks (tj. bez njega), jer se jednoznačno odredjuju simboli 1 i 0.

{0, 01, 11, 10} - poruka: 11101 je prefiks, 010 nije

36. Tipovi zaštitnih kodova?

Tipove zaštitnih kodova možemo svrstati u dve grupe:

1. **Blok kodovi** - na osnovu ulaznog bloka podataka dužine *k*, generiše se podatak sa preoširnošću ukupne dužine *n*. Svaki blok dužine *k* se obradjuje nezavisno od prethodnih blokova podataka. Kod sistemskih kodova, *k* informacionih bita ostaju nepromenjeni
2. **Konvolucioni kodovi** - za svaki ulazni blok podataka dužine *k* generiše se izlazni podatak ukupne dužine *n*. Izlazni podatak zavisi i od *m* prethodnih *k*-torki informacionih bita (tj. to su kodovi sa memorijom). Konvolucioni koder je konačni automat, čiji izlaz zavisi od trenutnog stanja

37. Turbo kodovi

U teoriji informacija turbo kodovi su klasa kodova za ispravljanje greške unapred (Forward Error Correction - FEC) visokih performansi koji su se razvili na početku 90ih. Oni su bili prvi kodovi koji su približno dostigli maksimalni kapacitet kanala po Šenonovom limitu (koji označava teoretski maksimalni prenos podataka uz odredjen šum pri kome je komunikacija moguća).

Ovi kodovi se koriste u 3G/4G mobilnoj komunikaciji, kao i u satelitskoj komunikaciji, kao i u svim ostalim poljima gde je poželjan pouzdan prenos informacija preko nekog kanala koji ima mnogo šumova.

Naime, moramo prvo sagledati Šenonov limit i kodne reči. Za kodne reči od 3 bita, imamo ukupno 2^3 (tj. 8) kodnih reči, ako pretpostavimo da nam trebaju kodne reči od 1000 bitova, onda dolazimo do ogromnog broja 2^{1000}, tj. oko 10^{301} i samim tim dekodovanje tih reči postaje eksponencijalno teže dodavanjem bitova. Ovaj problem su kreatori turbo kodova rešili tako što se koriste 2 enkodera na odašiljaču i 2 dekodera na prijemniku.

Turbo proces počinje sa tri kopije bloka podataka koje želimo poslati. Prva kopija ulazi u jedan od enkodera, gde konvolucioni koder uzima bitove iz podataka i kreira bitove pariteta iz njih. Druga kopija ulazi u drugi enkoder, koji sadrži identični konvolucioni koder, ali ovaj enkoder ne dobija isti ulaz, već izmešan od strane sistema koji se zove **interleaver** koji se provlači kroz konvolucioni koder. Na kraju, odašiljač šalje preko kanala treću kopiju originalnih podataka, zajedno sa dva stringa pariteta, Mešanje bitova interleavera je ključni korak za turbo kodove, jer je zbog permutacija moguće napraviti mnogo više kodnih reči.

Na prijemu, postoje dva dekodera koji računaju verovatnoću da je došlo do greške na svakom od bitova. Najčešće se ta verovatnoća izražava u brojevima od -127 do 127, gde je -127 sa 100% sigurnošću da je tu 0, a 127 obrnuto - 100% verovatnoća da je tu 1. Zatim se uporedjuju vrednosti verovatnoće izmedju oba dekodera koji potom ciklično prolaze kroz verovatnoće i medjusobno ih koriguju procesom koji traje obično od 15 do 18 iteracija.

38. Koji je nedostatak Hafmanovog kodovanja?

Najveći nedostatak klasičnog Hafmanovog kodovanja jeste nedostatak odredjenog odvajanja kodnih reči prilikom dekodovanja, ovo stavlja veliki stres na GPU što dovodi do uskog grla prilikom procesuiranja podataka, ali postoje napori da se enkodovanje i dekodovanje Hafmanovim postupkom prilagodi i optimizuju na GPU-ovima modernih arhitektura.

39. <u>CRC kodovi</u>

Cyclic-redundancy check (CRC) kodovi su kodovi koji mogu da detektuju greške i često se koriste u digitalnim mrežama i uredjajima za skladištenje radi detekcije slučajnih promena u digitalnim podacima. Blokovi podataka ulaze u ove sisteme da bi se ukratko proverila vrednost koja je poslata pomoću polinomskog deljenja njihovih (blokovi) sadržaja. Kada se dobije ostatak, celo računanje se ponavlja i ako se ne poklapaju rezultat i početna vrednost moguće je pokrenuti algoritam za ispravljanje grešaka, ukoliko se poklapaju - poruka je uspešno primljena, tj. podaci su validni. Ono što je bitno napomenuti jeste da ovaj sistem ne štiti od internih malverzacija i promena podataka.

CRC se tako zove jer se verifikacija vrši bez dodavanja dodatnih informacija i algoritam je ciklični, a operacija deljenja se vrši u GF(2).

Such is life...

S ljubavlju,
Autor

24 01 2024