31. Средња снага и спектар угаоно модулисаног сигнала.

Угаоно модулисани сигнал у општем случају је

$$u(t) = U_0 cos[\omega_0 t + \varphi(t)] = U_0 cos[2\pi f_0 t + \varphi(t)]$$

Тренутна снага на једноомској отпорности износи

$$p(t) = u^2(t) = U^2 \left\{\frac{1}{2} + \frac{1}{2} cos[2\omega_0 t + 2\varphi(t)]\right\}$$

Ако се модулишућа функција $\varphi(t)$ представи као сума простопериодичних компонената, средњеквадратна вриједност другог сабирка је једнака нули. Тада је средња снага угаоно модулисаног сигнала једнака средњој снази немодулисаног носиоца:

$$P = \overline{u^2(t)} = \frac{U_0^2}{2}$$

Угаона модулација је нелинеаран процес. Уколико се за модулишући сигнал изабере простопериодични тест тон, као резултат фазне или фреквенцијске модулације, добија се бесконачно много фреквенцијских компоненти у спектру модулисаног сигнала. Већина бочних фреквенцијских компоненти има веома мале амплитуде које се могу занемарити. Развој угаоно модулисаног сигнала се постиже разлагањем у Беселове функције прве врсте. Да би се нека спектрална компонента сматрала значајном, конвенција је да носи више од 1% снаге немодулисаног носиоца. Ширина спектра угаоно модулисаног сигнала која обухвата значајне компоненте износи:

$$B = 2f_m(m+1)$$

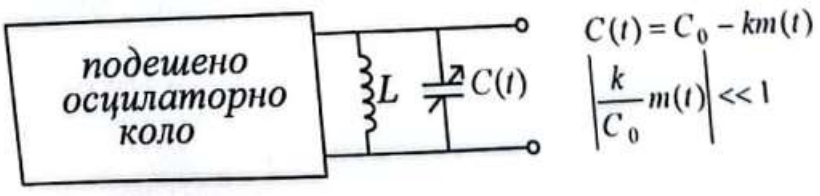
При чему је $m = \frac{\Delta\omega_0}{\omega_m}$ индекс модулације.

32. Модулација FM сигнала.

Генерисање фреквенцијски модулисаног сигнала може се остварити на два начина:

- Директним методама
- Индиректним методама

Директна промјена постиже се промјеном неких од параметара осцилатора.



На слици је приказана шема FM модулатора са LC осцилаторним колом код којег се промјена учестаности постиже промјеном капацитивности подешеног осцилаторног кола. Нпр. код кондензаторског микрофона промјеном звучног притиска мијења се

растојање између плоча, а самим тим и капацитивност. Ако претпоставимо да се промјена одвија по линеарном закону, угаона учестаност осцилаторног кола износи

$$\omega_i = \frac{1}{\sqrt{LC(t)}} = \frac{1}{\sqrt{L(C_0 - km(t))}} = \frac{1}{\sqrt{LC_0}} \frac{1}{\sqrt{1 - \frac{k}{C_0} m(t)}}$$

С обзиром на то да вриједи развој у Маклоренов ред

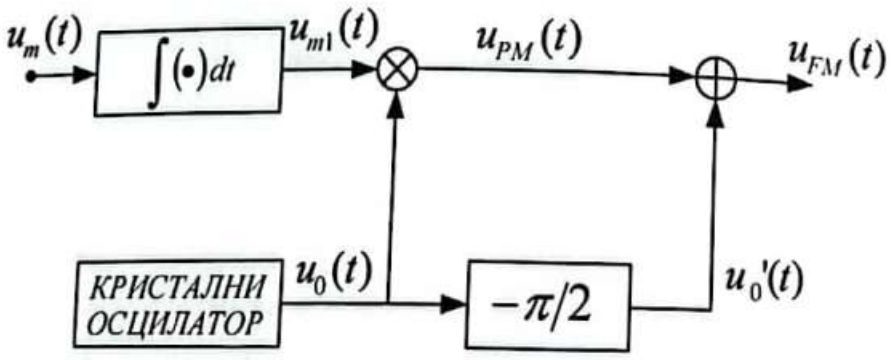
$$\frac{1}{\sqrt{1-x}} \approx \frac{1}{1-\frac{x}{2}} \approx 1 + \frac{x}{2}, \text{за } x \ll 1$$

слиједи да је угаона учестаност

$$\omega_i \approx \omega_c \left(1 + \frac{k}{2C_0} m(t)\right) \approx \omega_c + k_\omega m(t)$$

При томе је $\omega_c = \frac{1}{\sqrt{LC_0}}$ и $k_\omega = \frac{k\omega_c}{2C_0}$. Дакле, тренутна фреквенција се директно, по линеарној зависности мијења под утицајем модулишућег сигнала.

Код индиректних метода фреквенција носиоца се мијења индиректно, под утицајем модулишућег сигнала. Примјер директне FM модулизације је Армстронгов модулатор.



Претпоставимо да је модулишући сигнал тест тон угаоне учестаности ω_m.

$$u_m(t) = U_m \cos(\omega_m t)$$

Из блок шеме слиједе изрази за сигнале на излазима појединих склопова кола.

$$u_{m1}(t) = \int U_m \cos(\omega_m t)\, dt = \frac{U_m}{\omega_m} \sin(\omega_m t)$$

$$u_0(t) = U_0 \cos(\omega_0 t)$$

$$u_{PM}(t) = \frac{U_m U_0}{\omega_m} \sin(\omega_m t) \cos(\omega_0 t)$$

$$u_0(t) = U_0 \sin(\omega_0 t)$$

$$u_{FM}(t) = u_0(t) + u_{PM}(t) = U_0 \sin(\omega_0 t) + \frac{U_m U_0}{\omega_m} \sin(\omega_m t)\cos(\omega_0 t)$$

$$A\sin(x) + B\cos(x) = C\sin(x + \varphi)$$
$$= C\sin(x)\cos\varphi + C\cos(x)\sin\varphi$$
$$A = C\cos\varphi$$
$$B = C\sin\varphi$$
$$A^2 + B^2 = C^2(\cos^2\varphi + \sin^2\varphi) = C^2$$
$$\frac{B}{A} = tg\varphi$$
$$C = \sqrt{A^2 + B^2}$$
$$\varphi = arctg\left(\frac{B}{A}\right)$$

$$u_{FM}(t) = U_0 \sqrt{1 + \left(\frac{U_m}{\omega_m}\right)^2 sin^2(\omega_m t)}\sin\left(\omega_0 t + \varphi(t)\right)$$

$$\varphi(t) = arctg\left(\frac{U_m}{\omega_m}\sin(\omega_m t)\right)$$

Узимајући у обзир да је $arctg(x) \approx x$ (за мало x), уз занемаривање другог сабирка под коријеном, добијамо коначно:

$$u_{FM}(t) \cong U_0 \sin\left(\omega_0 t + \frac{U_m}{\omega_m}\sin(\omega_m t)\right) =$$
$$= U_0 \sin\left(\omega_0 t + \int u_m(t)dt\right).$$

33. Демодулација FM сигнала.

Демодулација се обавља у склопу који се назива демодулатор, чија је улога издвајање сигнала поруке из модулисаног сигнала. Кола за детекцију FM сигнала могу се сврстати у неколико група:

- Конвертори фреквенцијски модулисаних сигнала у амплитудски модулисане
- Дискриминатори са фазним мрежама
- Детектори проласка кроз нулу
- Демодулатори са повратном спрегом

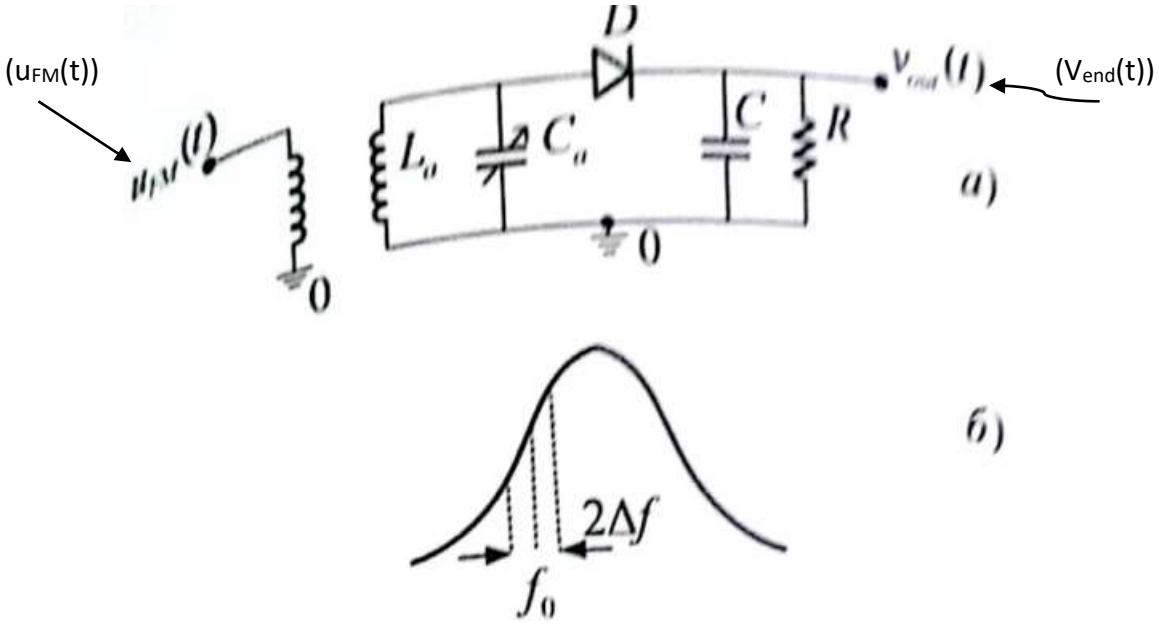
Сви склопови који обављају функцију диференцирања у временском домену могу се користити као **конвертори FM у AM** сигнале. Нека је дат FM сигнал:

$$u_{FM}(t) = U_0 cos\left[\omega_0 t + \Delta\omega_0 \int m(t)dt\right]$$

При томе је $\Delta\omega_0 = k_\omega U_m$ максимална девијација кружне учестаности носиоца, а $u_m(t) = U_m m(t)$ модулишући сигнал. Ако на улаз диференцијатора доведемо овај сигнал, на излазу добијамо сљедећи сигнал:

$$u_{FM\to AM}(t) = U_0[\omega_0 + k_\omega u_m(t)]cos\left[\omega_0 t + \Delta\omega_0 \int m(t)dt + \frac{\pi}{2}\right].$$

Добијени сигнал модулисан је амплитудски и фреквенцијски. Најједноставнија реализација детекције FM сигнала, приказана је на следећој слици. Диференцирање сигнала обавља паралелно осцилаторно коло у линеарном дијелу фреквенцијске карактеристике.



Дискриминатори са фазним мрежама користе склопове са линераном фазном карактеристиком. Идеја на којој се они заснивају је апроксимација диференцирања у временском домену:

$$\frac{d[\varphi(t)]}{dt} \approx \frac{1}{\tau}[\varphi(t) - \varphi(t-\tau)].$$

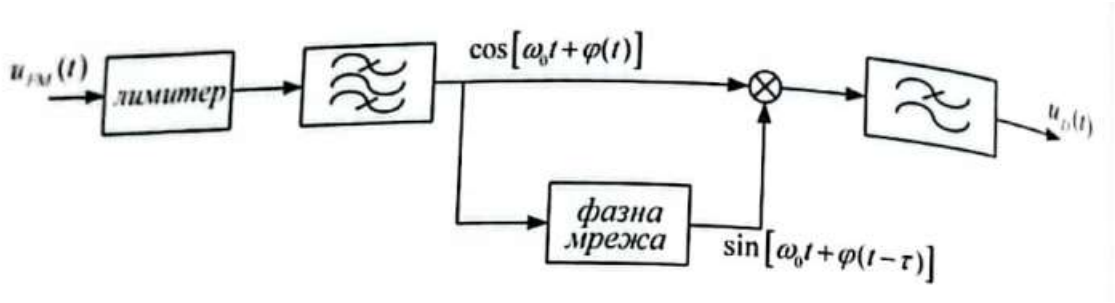
За фреквенцијски модулисан сигнал имамо:

$$\frac{d[\varphi(t)]}{dt} = k_\omega u_m(t).$$

Узимајући у обзир претходне релације, добијамо:

$$\varphi(t) - \varphi(t-\tau) \approx \tau\varphi'(t) = k_\omega \tau\, u_m(t).$$

На слици је приказана шема квадратурног демодулатора.



Ако претпоставимо јединичну амплитуду FM сигнала, на излазу множења се добија:

$$\cos[\omega_0 t + \varphi(t)] \cdot \sin[\omega_0 t + \varphi(t-\tau)]$$

Трансформацијом производа у збир, на улазу нискофреквенцијског филтра је сигнал:

$$\frac{1}{2}\{sin[2\omega_0 t + \varphi(t) + \varphi(t-\tau)] - sin[\varphi(t) - \varphi(t-\tau)]\}$$

Узимајући у обзир да је за $|\varphi(t) - \varphi(t-\tau)| \ll \pi$:

$$sin[\varphi(t) - \varphi(t-\tau)] \approx \varphi(t) - \varphi(t-\tau),$$

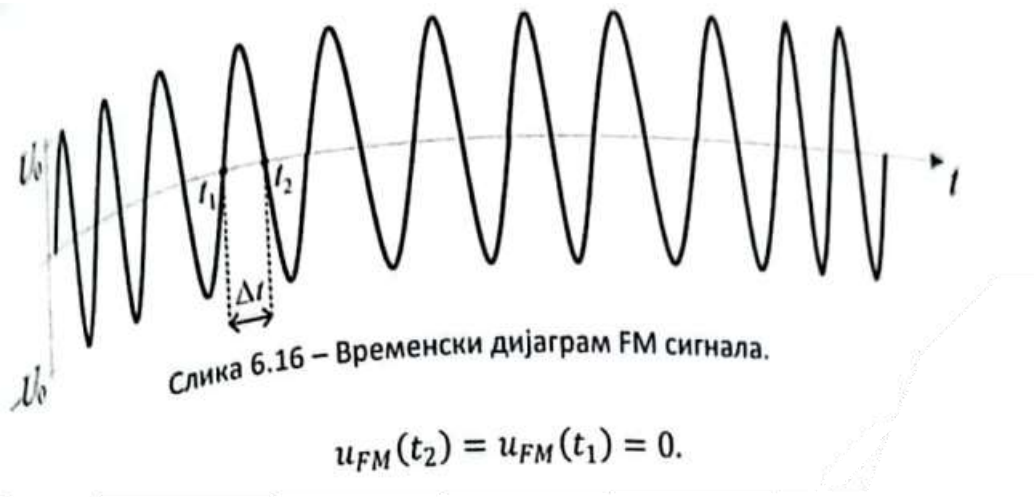
Имамо да је на излазу кола сигнал:

$$u_D(t) \approx k_D k_\omega \tau\, u_m(t).$$

Размотрићемо још **демодулаторе FM сигнала са детекцијом проласка кроз нулу**. Нека је дат FM сигнал:

$$u_{FM}(t) = U_0 cos[\theta(t)], \qquad \theta(t) = \omega_0 t + k_\omega \int_{-\infty}^{t} u_m(\tau) d\tau,$$

И нека t_1 и t_2, ($t_2 > t_1$) представљауј тренутке 2 узастопна проласка кроз нулу, као на слици



Слика 6.16 – Временски дијаграм FM сигнала.

$$u_{FM}(t_2) = u_{FM}(t_1) = 0.$$

С обзиром на то да је разлика тренутних фаза 2 сусједна проласка кроз нулу π, имамо:

ОКИТИ

$$\theta(t_2) - \theta(t_1) = \pi = \omega_0 t_2 + k_\omega \int_{-\infty}^{t_2} u_m(\tau)d\tau - \left[\omega_0 t_1 + k_\omega \int_{-\infty}^{t_1} u_m(\tau)d\tau\right]$$

$$\omega_0(t_2 - t_1) + k_\omega \int_{t_1}^{t_2} u_m(\tau)d\tau = \pi$$

Пропусни опсег модулишућег сигнала је много мањи од опсега модулисаног сигнала, тако да се може сматрати да је модулишући сигнал у интервалу (t_1, t_2) константан за неко $t_1 < t < t_2$.

$$\omega_0 \Delta t + k_\omega u_m(t)\Delta t = \pi$$

Одавде слиједи да је:

$$k_\omega u_m(t) = \frac{\pi}{\Delta t} - \omega_0.$$

34. Бинарна амплитудска модулација.

Бинарна амплитудска модулација представља најједноставнији поступак за транслацију спектра дигиталног сигнала из физичког (основног) у виши фреквенцијски опсег, код које је амплитуда носећег континуалног таласа сразмјерна модулишућем сигналу. Ову модулацију можемо математички представити на сљедећи начин:

$$s(t) = m(t)c(t),$$

гдје је *m(t)* модулишући дигитални сигнал, а *c(t)* синусоидални носилац. Дакле, практична реализација модулатора BASK сигнала је прилично једноставна и своди се на множење модулационог сигнала са сигналом таласа носиоца. За униполарни сигнал без повратка на нулу важи m(t)=1, у случају логичке "1", односно m(t)=0 у случају логичке "0". Овај тип модулације представља специјалан случај *ASK* сигнала и у литератури је познат и под називом *OOK (On-Off Keying)*. Трајање једног бита износи T_b секунди, и називамо га битски интервал. Бинарни *ASK* сигнал можемо изразити на сљедећи начин:

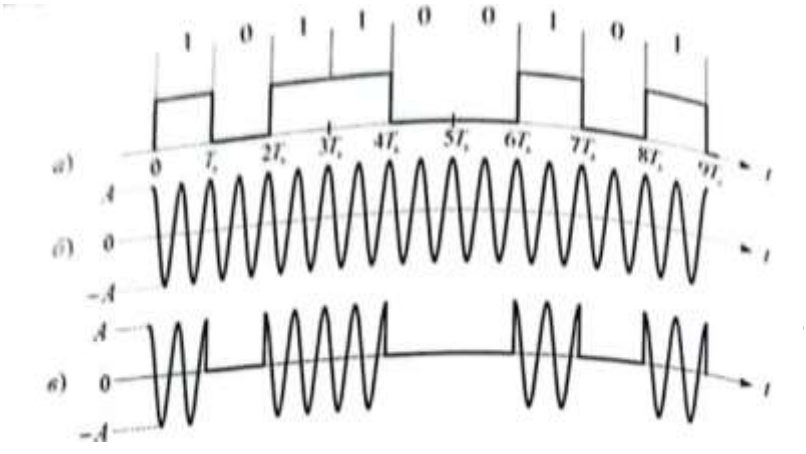
$$s(t) = \begin{cases} s_1(t) = A\cos\omega_0 t, & za\ m(t) = 1 \\ s_2(t) = 0, & za\ m(t) = 0 \end{cases}$$

Дакле, уколико преносимо бинарну нулу не емитујемо носећи талас, а при преносу бинарне јединице емитујемо синусоидални талас $Acos(\omega_0 t)$

а) модулишући сигнал

б) сигнал носиоца

в) модулисани сигнал



35. Бинарна фазна модулација

Бинарна фазна модулација се генерише амплитудском моулацином синусног носиоца са биполарним NRZ сигналом ($m(t) = \pm 1$). За биполарни NRZ сигнал, m(t)=1 у случају логичке “1”, односно, m(t)=-1 у случају логичке ”0” или обрнуто. Предајни сигнал $s(t) = m(t)c(t) = \pm A cos\omega_0 t$, узима фазу “0” или “π” зависно да ли се преноси логичка јединица или нула.

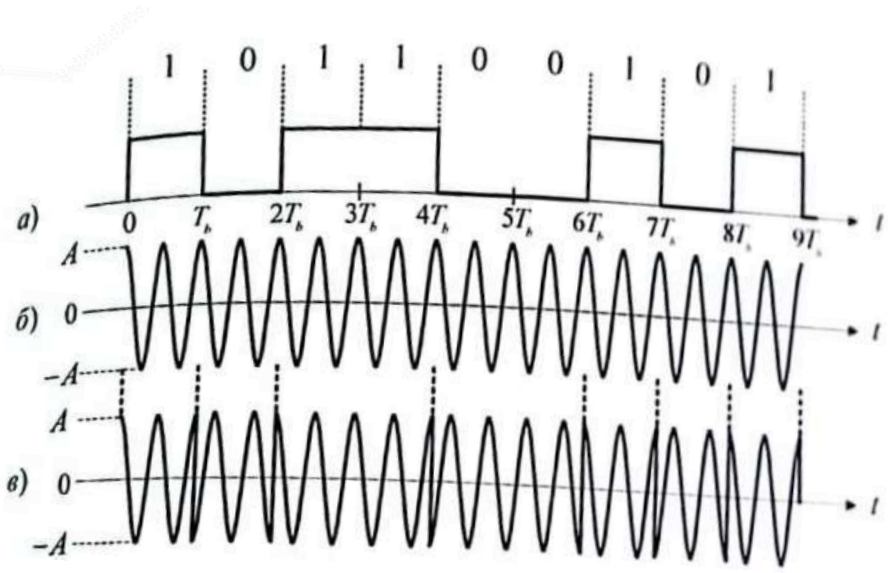
$$s(t) = \begin{cases} s_1(t) = A cos\omega_0 t, & \text{за } m(t) = 1 \\ s_2(t) = -A cos\omega_0 t, & \text{за } m(t) = -1 \end{cases} \qquad 0 < t \leq T_b$$

Дакле, уколико преносимо бинарну нулу, емитујемо носећи талас, чија је почетна фаза π ($A cos(\omega_0 t + \pi) = -A cos(\omega_0 t)$), а при преносу бинарне јединице емитујемо синусоидални талас нулте почетне фазе ($A cos\omega_0 t$). На слици су приказани таласни облици:

а) модулишућег сигнала

б) сигнала носиоца

в) модулисаног сигнала

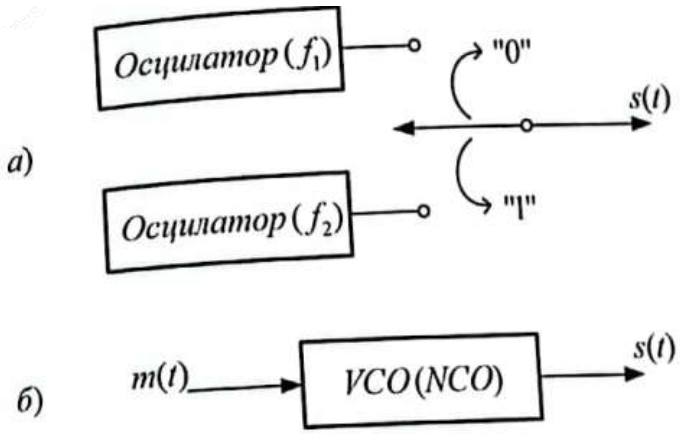


Фреквенција сигнала носиоца се бира тако да буде цјелобројан број периода у току трајања једног бита, односно $f_0 = n/T_b$, n цјелобројан. Наравно, и овдје је задовољено да је $f_0 \gg 1/T_b$.

36. Бинарна фреквенцијска модулација

BFSK сигнал се може генерисати на 2 различита начина. Један начин је тастовање предајног сигнала између 2 различита осцилатора, као што је приказано на слици. У овом случају имамо скоковит прелаз са једне на другу фреквенцију, односно, скоковоту промјену фазе предајног сигнала. Овај тип *FSK* сигнала можемо изразити на сљедећи начин:

$$s(t) = \begin{cases} s_1(t) = A cos(\omega_1 t + \varphi), & \text{за бинарну "0"} \\ s_2(t) = A cos(\omega_2 t), & \text{за бинарну "1"} \end{cases} \qquad 0 < t \leq T_b$$

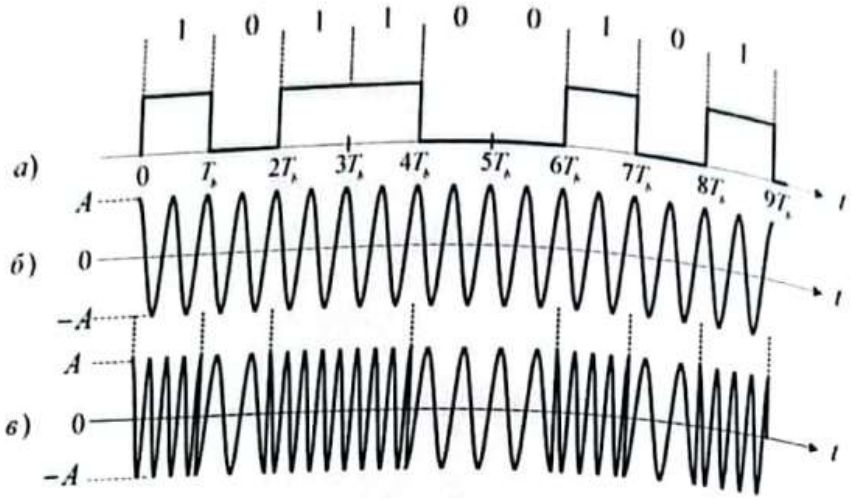


Дакле, када преносимо бинарну нулу емитујемо сигнал фреквенције f_1, а за бинарну јединицу емитујемо сигнал фреквенције f_2. Други, чешћи начин генерисања *FSK* сигнала је коришћење напонски контролисаног осцилатора (VCO) или нумерички контролисаног осцилатора (NCO). На слици су приказани таласни облици:

а) модулишућег сигнала *m(t)*

б) сигнала носиоца *c(t)*

в) модулисаног сигнала *s(t)*



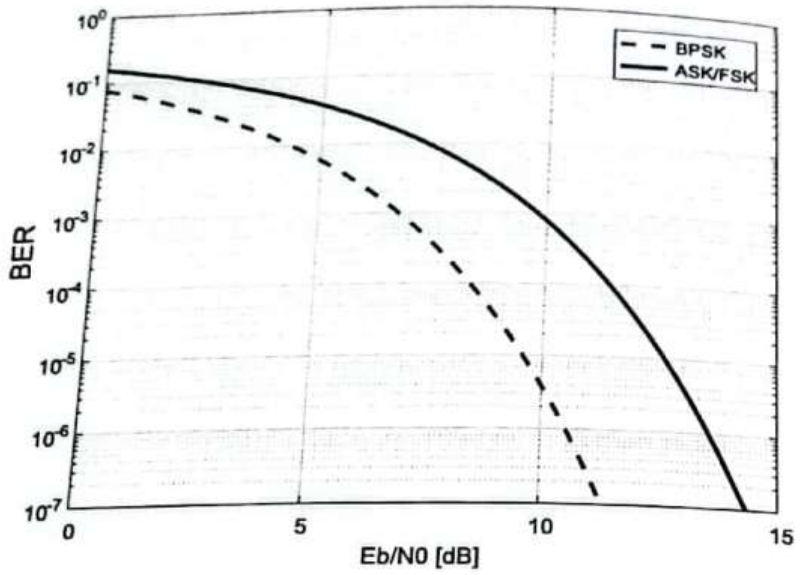
Двије фреквенције сигнала носилаца бирамо тако да буду цјелобројни умношци $1/T_b$, а фреквенције f_1 и f_2 треба да буду ортогоналне.

37. Поређење основних бинарних модулационих поступака.

Да бисмо могли извршити поређење различитих модулационих поступака, неопходно је вјероватноћу грешке изразити преко средње енергије по биту, E_b. Упоредни приказ основних величина за бинарне модулационе поступке је приказан у табели. Из табеле се види да је по питању вјероватноће грешке *BPSK* за 3dB ефикаснија од *BFSK* и *BASK*. То значи да је за исту вриједност *BER*-а код *BPSK* модулационог поступка потребна два пута мања средња енергија по биту у односу на *BFSK* и *BASK.* Треба нагласити да је недостатак *BPSK* пријемника повећана сложеност у односу на *BFSK* и *BASK*, код којих постоји могућност некохерентне демодулације. Код *BFSK* и *BASK* кохерентни системи дају боље перформансе, али су комплекснији од некохерентних поступака. Сложенија реализација кохерентних система је посљедица генерисања синфазног локалног носиоца на

	$s_0(t)$ $(0 < t \leq T)$	$s_1(t)$ $(0 < t \leq T)$	E_b	BER (P_e)	Ширина пропусног опсега
ASK	0	$A\cos(\omega_c t)$	$A^2T_b/4$	$Q\left(\sqrt{\frac{E_b}{N_0}}\right)$	$\frac{2}{T_b}$
PSK	$A\cos(\omega_c t)$	$-A\cos(\omega_c t)$	$A^2T_b/2$	$Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$	$\frac{2}{T_b}$
FSK	$A\cos(\omega_1 t)$	$A\cos(\omega_2 t)$	$A^2T_b/2$	$Q\left(\sqrt{\frac{E_b}{N_0}}\right)$	$(f_2 - f_1) + \frac{2}{T_b}$

пријемној страни. Генерално, бинарне поступке демодулације карактерише једноставност и отпорност на адитивни бијели Гаусов шум (*AWGN*) у каналу. Ширина пропусног опсега је узета по критеријуму прве нуле у спектру. Као што се види, *FSK* модулација има већу потребну ширину пропусног опсега, која зависи од растојања између фреквенција f_2 и f_1 и минимална је у случају кохерентних ортогоналних носилаца када је $f_2 - f_1 = \frac{1}{2T_b}$.



38. Појам информације.

И поред тога што се неријетко поистовјећују, битно је правити разлику између помова података и информације. Нпр. број 9 је само податак и као такав нема посебно значење. Међутим, исказ “Сада је 9 часова.” представља информацију јер је податку додијељено неко значење. Значи, информација се састоји од података и значења које му је додијељено. То можемо видјети и из информационе хијерархије са слике:

Двије дефиниције у вези са појмом информације које су широко прихваћене су:

1. Информација је сазнање пренијето кроз простор/вријеме.
2. Сигнал је физички носилац информације.

Алтернативне дефиниције информације су:

- Информација представља поруку коју је прималац прихватио и разумио.
- Информација представља статистички податак – чињеницу на основу које је могуће донијети закључак.
- Информација представља знање прикупљено студирањем, искуством или подучавањем.
- Информација представља могућност закључивања узрока посматрањем посљедице (ватра -> дим).

39. Мјера количине информација.

Да би се могла вршити анализа за пренос информација потребно је увести мјеру за количину информација. И поред тога што је човјеку интуитивно познат појам информација, поставља се питање на који начин нумерички исказати количину информација коју нека порука носи. Овдје ћемо се ограничити на дискретне изворе информација без меморије код којих је скуп порука које се могу генерисати пребројив. Претпоставимо да је корисник заинтересован за поруку да се догодио неки догађај (s_i) и да је позната вјероватноћа тог догађаја ($P(s_i)$). Два логична услова која намеће бројно исказивање количине информација су:

1. Мање вјероватан догађај носи већу количину информација.
2. Количина информација коју пружају два независна догађаја једнака је збиру количина информација коју пружају догађаји појединачно.

С обзиром на то да се вјероватноћа здруженог догађаја за независне догађаје добија као производ појединачних вјероватноћа, а имајући у виду да логаритамска функција

пресликава производ у збир, за задовољење оба постављена услова је дефинисана количина информација дата изразом:

$$Q(s_i) = \log \frac{1}{P(s_i)} = -\log[P(s_i)]$$

Адитивност количина информација независних порука се може показати сљедећим изразом:

$$Q(s_i, s_j) = \log \frac{1}{P(s_i, s_j)} = \log \frac{1}{P(s_i)P(s_j)}$$
$$= \log \frac{1}{P(s_i)} + \log \frac{1}{P(s_j)} = Q(s_i) + Q(s_j).$$

База логаритма се може произвољно узети и утиче само на јединицу мјере. Хартли је предложио декадски логаритам, тако да се може писати:

$$Q(s_i) = \log_{10} \frac{1}{P(s_i)} [hartley].$$

Ако се узима база природног логаритма добија се скраћеница *nat.*

$$Q(s_i) = \ln \frac{1}{P(s_i)} [nat].$$

Коначно, ако се узме логаритам по бази 2 добијамо:

$$Q(s_i) = \log_2 \frac{1}{P(s_i)} [Sh].$$

Умјесто јединице *шенон* користи се и назив јединице *информациони бит.* Ако извор информација генерише симболе из бинарног алфабета који су подједнако вјероватни ($P(s_1) = P(s_2) = 0.5$), имамо $Q(s_1) = Q(s_2) = 1$[Sh]. Значи кажемо да смо добили количину информација од једног шенона ако само сазнали исход догађаја са 2 једнако вјероватна исхода (нпр. глава-писмо код бацања новчића). С обзиром на то да се у телекомуникацијама најчешће појављују сигнали са 2 нивоа (бинарни), разумљиво је зашто је за базу логаритма одабран број 2.

40. Ентропија дискретног извора без меморије.

Дат је дискретан извор без меморије S са листом симбола $\{S_1, S_2, \ldots, S_q\}$ и одговарајућим скупом вјероватноћа $P(s_i)$, $i=1,2,\ldots,q$. Претпоставља се да емитовање симбола представља потпун систем хипотеза, тј. $\sum_{i=1}^{q} P(s_i) = 1$. Средња количина информација (односно математичко очекивање) коју емитује извор по једном симболу износи:

$$H(S) = E[Q(s_i)] = \overline{Q(s_i)} =$$

$$= \sum_{i=1}^{q} P(s_i) log_2 \frac{1}{P(s_i)} = -\sum_{i=1}^{q} P(s_i) log_2 P(s_i) \left[\frac{Sh}{simb}\right]$$

По аналогији са ентропијом идеалног гаса у термодинамици, гдје ентропија представља мјеру неуређености система, Шенон је за просјечну количину информација такође увео појам ентропија. При том, у теорији информација ентропија представља мјеру неизвјесности (неопредијељености) примаоца шта ће извор емитовати.

41. Разлози увођења кодовања.

Три су основна разлога зашто вршимо кодовање:

1. Кодовање ради компресије података – циљ овог начина кодовања је избацивање сувишности (редундансе) јер готово сваки извор информација има одређени ''вишак'' информација. Овај вид кодовања се назива статистичко (ентропијско) кодовање. Неки од примјера овог начина кодовања су *Шенон-Фаноов* поступак, *Хафменов* поступак, *Лампел-Зипов* поступак, аритметичко кодовање итд.
2. Кодовање у циљу квалитетнијег преноса усљед дјеловања шума или сметњи у каналу – задатак овог начина кодовања је додавање сувишних (редундантних) бита у улазну информацију како би се на пријему могла извршити контрола квалитета преноса, односно откривање (детекција) и евентуално исправљање (корекција) грешака насталих током преноса. Ово кодовање се назива заштитно (каналско) кодовање. Неки од примјера су код са провјером на парност, код са понављањем поруке, *Хемингов* код, *Рид-Соломонов* код итд.
3. Кодовање ради тајности – циљ овог начина кодовања је да информације буду доступне само ауторизованим корисницима. Овај начин кодовања се назива и шифровање, а један од најстаријих видова је тзв. *Цезарово* шифровање (слово А у шифрованом тексту се мијења словом D, В се мијења словом Е итд).

42. Сардинас-Патерсонов критеријум

Потребан и довољан услов да би код био једнозначно декодив дали су Сардинас и Патерсон. Поступак утврђивања се своди на креирање таблице следећим поступком:

- Прву и другу колону таблице формирају изворна кодна листа и одговарајуће кодне ријечи, респективно. Листа кодних ријечи у другој колони се назива ''нулта сегментна класа'' (***seg 0***).
- У сљедећој колони се формира прва сегментна класа (***seg 1***) која садржи суфиксе кодних ријечи које за префикс имају кодну ријеч мање дужине. Значи, испитујемо у ***seg 0*** да ли је нека кодна ријеч префикс неке друге кодне ријечи.

- Затим се формира друга сегментна класа, па трећа, итд. Као опште правило се узима *i*-та сегментна класа (***seg i***) садржи суфиксе кодних ријечи из ***seg 0*** којима је префикс кодна ријеч из ***seg i-1***, а такође од суфикса из кодних ријечи из ***seg i-1*** којима је префикс нека ријеч из ***seg 0***.

Потребан и довољан услов једнозначне декодибилности је да се у вишим сегментним класама не појављују ријечи из нулте сегментне класе. Кашњење при декодовању (l_d) је дато изразом:

$$\left\lceil \frac{d}{2} \right\rceil l_{min} < l_d \leq \left\lceil \frac{d+1}{2} \right\rceil l_{max}$$

При том је d редни број прве празне сегментне класе, а l_{min} и l_{max} минимална и максимакна дужина кодне ријечи из ***seg 0***. Угласте заграде $\lceil x \rceil$ означавају најмањи цијели број који није мањи од x.

43. Крафтова неједнакост.

Крафтова неједнакост даје потребан и довољан услов да би тренутни (префиксни) код са кодним ријечима дате дужине постојао. Нека је дат извор информација S са листом симбола $\{S_1, S_2, \ldots, S_q\}$ и нека је кодна листа димензије r. У случају бинарног кодовања кодна листа {0, 1} је димензије 2. Нека је дужина кодне ријечи X_i која одговара симболу s_i једнака l_i. Потребан и довољан услов за постојање тренутног кода са кодним ријечима дужине $l_1, l_2, \ldots, l_q$ је да буде задовољена следећа (Крафтова) неједнакост:

$$\sum_{i=1}^{q} r^{-l_i} \leq 1$$

Битно је нагласити да Крафтова неједнакост даје одговор на питање да ли постоји тренутан код са задатим дужинама кодних ријечи, али не и како конструисати код.

Нпр. код {1, 00, 10} није тренутан иако задовољава Крафтову неједнакост.

$$\sum_{i=1}^{q} r^{-l_i} = 2^{-1} + 2^{-2} + 2^{-2} = 1$$

Крафтова неједнакост каже да постоји тренутан бинарни код са дужинама кодних ријечи 1, 2 и 2 (и заиста то је код).

44. Прва Шенонова теорема.

Шенон је у свом раду из 1948. године дао одговор на суштинско питање из статистичког кодовања, односно колико износи фундаментално ограничење у погледу компресије података. Теорема се још среће под називом ''Теорема о кодовању без шумова''.

Шенонова теорема о кодовању без шумова – Дио I

Нека је дат дискретни извор информације без меморије S са ентропијом *H(S)*. За било који бинарни префиксни код датог извора средња дужина кодних ријечи је већа или једнака од ентропије извора, односно:

$$\bar{L} \geq H(S)$$

Теорема даје једну границу средње дужине кодних ријечи. Поставља се питање да ли има још ограничења. Јасно је да овај израз постаје високо вредновaн ако покажемо да је та граница уједно и најбоља могућа. Шенон је у поменутом раду конструисао код који, иако није у општем случају компактан, довољно се добро приближава доњој граници. Идеја се своди на избор дужине кодне ријечи l_i тако да вриједи $l_i = \left\lceil \log_2 \frac{1}{p_i} \right\rceil$. При том $\lceil x \rceil$ означава најмањи цијели број који није мањи од x, односно, вриједи $x \leq \lceil x \rceil < x + 1$. Прво се поставља питање да ли код са предложеним дужинама постоји. Одговор је потврдан што слиједи из Крафтове неједнакости. По дефиницији функције $\lceil x \rceil$ слиједи да је:

$$l_i \geq log_2 \frac{1}{p_i}$$

$$\sum_i 2^{-l_i} \leq \sum_i 2^{log_2 p_i} = \sum_i p_i = 1$$

Сада одредимо колико је овај код добар у погледу средње дужине кодних ријечи. По дефиницији функције $\lceil x \rceil$ слиједи да је:

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

Ако обе стране једнакости помножимо са p_i и сумирамо по *i* добијамо:

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

$$\bar{L} < H(S) + 1$$

Из посљедње релације се види да је средња дужина кодних ријечи *Шенон-Фаноовог* кода удаљена највише за 1 од ентропије извора. То значи да је овај код прилично добар, поготово за веће вриједности ентропије. Међутим, за мање вриједности ентропије може се пронаћи бољи код (са мањом средњом дужином кодних ријечи). Проведена анализа нам омогућава да формулишемо други дио теореме.

<u>Шенонова теорема о кодовању без шумова – Дио II</u>

За било који дискретни извор информација без меморије S са ентропијом *H(S)* постоји бинарни префиксни код са средњом дужином кодних ријечи $\bar{L} < H(S) + 1$. Да би се могло квантитативно одредити колико се средња дужина кодних ријечи конструисаног кода приближава ентропији извора, дефинишемо ефикасност кода помоћу релације:

$$\eta = \frac{H(S)}{\bar{L}} \cdot 100\ [\%]$$

Редунданса (сувишност) кода је такође мјера квалитета статистичког кодовања. То је у ствари комплемент ефикасности до јединице.

$$R = \frac{\bar{L} - H(S)}{\bar{L}} \cdot 100 = 100 - \eta\ [\%]$$

Прва Шенонова теорема даје увид у ограничења статистичког кодовања у погледу перформанси али не даје поступак како за дати извор информација конструисати компактан код.

45. Хафменов поступак

За разлику од *Шенон-Фаноове* методе, *Хафменов* поступак у потпуности води до компактног кода. Може се једноставно програмски реализовати и не захтијева испитивање више варијанти. Има велику примјену у компресији слике и видеа. Опет ћемо се ограничити на случај бинарног кодовања без губитка општости. Поступак се темељи на двије основне теореме:

1. У оптималном коду, симболи са већим вјероватноћама имају кодне ријечи мање дужине од оних са мањим вјероватноћама.
2. У оптималном коду, два симбола са намјањим вјероватноћама имају кодне ријечи исте дужине.

Новина коју је Хафмен увео је конструкција бинарног стабла од листова према коријену, за разлику од Фаноовоф поступка.

Нека је дат извор $S=\{S_1, S_2, \ldots, S_q\}$ код којег су вјероватноће појављивања $P_i(i=1, 2, \ldots, q)$. Алгоритам се може описати сљедећим корацима:

1. Симболи се поређају по нерастућим вриједностима. Ако симболи имају исте вјероватноће, њихов распоред при уређивању није важан.
2. Два најмање вјероватна симбола се замијењују једним еквивалентним симболом, чија је вјероватноћа једнака збиру вјероватноћа симбола које он замјењује. На тај начин је извор S са q симбола сведен на извор S_1 са $q-1$ симболом. Симболи се поново поредају по нерастућим вјероватноћама, јер новоформирани симбол не мора имати најмању вјероватноћу.
3. Врши се редукција извора S_1 на исти начин (групишу се 2 најмање вјероватна симбола) и формира се извор S_2 са $q-2$ симбола. Процес се понавља док се не добију само 2 симбола.

Кодовање се врши тако што се почиње од редукованог извора са 2 симбола и једном се додијели бит 0, а другом 1. Затим се иде корак уназад и врши растављање еквивалентног

симбола. При сваком растављању се на одговарајуће мјесто додаје 0 или 1, док се не дође на првобитни извор *S*.

46. Лемпел-Зивово кодовање.

И поред тога што *Хафменов* поступак води до конструисања компактног кода, постоји неколико озбиљних недостатака при практичној реализацији.

- Извор информација се третира као извор без меморије.
- Потребно је познавање вјероватноће симбола.
- Поступак је осјетљив на губитак синхронизације (кодне ријечи су у општем случају промјенљиве дужине).
- Поступак је осјетљив на грешке при преносу (каналске грешке).

Наведени проблеми су довели до идеје универзалног кода. То је код који врши компресију секвенци података без априорног познавања статистичких особина. *Лемпел-Зивов (LZ)* поступак кодовања је врста универзалног кодовања код којег не постоји експлицитни модел. Поред тога што је једноставнији за програмску реализацијју од *Хафменовог* алгоритма, кодне ријечи су фиксне дужине што је погодно у случају синхроног преноса.

Основне идеје LZ кодовања ће бити објашњене на примјеру бинарног извора, иако исти принципи вриједе и за димензију алфабета већу од 2. Основна идеја се заснива на томе да се ''улазна секвенца дијели (рашчлањује) на најкраће сегменте који се још нису појавили у претходно примљеном дијелу секвенце''. Кодер и декодер имају меморисане сегменте који су се претходно појавили, тако да се при појави новог сегмента шаље само адреса претходно меморисаног сегмента и нови бит (или симбол), или његова адреса која је на почетку дефинисана. Такође, новопристигли сегмент, за један бит дужи, добија своју адресу.

47. Модел дискретног канала без меморије.

Пренос информација може да буде из једне тачке у другу (нпр. од једног до другог мобилног телефона у мобилној телекомуникационој мрежи) или кроз вријеме када се информација меморише у једном, а ишчитава у другом, будућем, тренутку. У оба случаја се сусрећемо са појмом поузданог преноса информација. Шум у каналу може дјеловати на један од следећих начина:

1. У условима изузетно великог шума није могуће обавити поуздан пренос информација (добро је познат ефекат ''пролома облака'' у сателитској телевизији.)
2. Ниво шума је такав да се информације могу преносити тако да реконструисани сигнал на пријему буде прихватљивог квалитета.
3. Шум у каналу утиче на тај начин да реконструисани сигнал у пријемнику није прихватљивог квалитета, али се примјеном заштитног кодовања вјероватноћа грешке може учинити по вољи малом. Основна идеја заштитног кодовања је

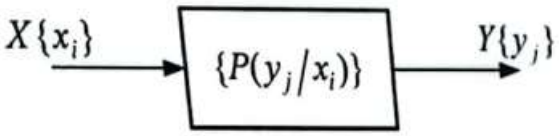
додавање редундансе, односно сувишних бита, тако да и поред грешака у каналу постоји довољно информација да се реконструише послата порука са задатим нивоом грешке.

Неки примјери комуникационог сигнала су:

- модем -> телефонска линија -> модем,
- сателит -> етер (RF таласи) -> Земља,
- ћелија родитеља -> ћелија дјетета,
- меморија рачунара -> диск рачунара -> меморија рачунара итд.

Дискретни канал без меморије се може описати са:

i. листом улазних симбола $X=\{x_i\}$, $i=1, 2, \ldots, r$
ii. листом излазних симбола $Y = \{y_j\}$, $j=1, 2, \ldots, s$
iii. скупом условних вјероватноћа $\{P(y_j|x_i)\}$ $i=1, 2, \ldots, r$ и $j=1, 2, \ldots, s$.



У општем случају број излазних симбола не мора да буде једнак броју улазних симбола. Претпоставља се да је канал стациониран, односно да му се карактеристике не мијењају у току времена. Нека је $p_{ij} \triangleq P(y_j|x_i)$. Скуп условних вјероватноћа се може приказати у форми каналске матрице:

$$\boldsymbol{P} = [P_{ij}] = \begin{bmatrix} p_{11} p_{12} & p_{1s} \\ p_{21} p_{22} \cdots p_{2s} \\ \vdots \quad \vdots \quad \cdots \quad \vdots \\ p_{r1} p_{r2} & p_{rs} \end{bmatrix}$$

При том, индекс *i* показује редни број врсте, а *j* редни број колоне. Очигледно је да матрица *P* треба да буде стохастичка, односно да сума елемената сваке врсте буде једнака јединици.

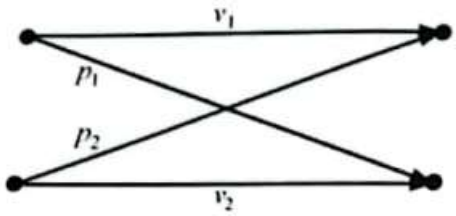
$$\sum_{j=1}^{s} p_{ij} = 1, \qquad \forall i \in \{1,2,..,r\}$$

С обзиром на то да се у дигиталним телекомуникацијама преносе симболи из бинарног алфабета, дискретни канал са најмањим бројем симбола на улазу и излазу је бинарни канал. Матрица бинарног канала је:

$$\boldsymbol{P_{BC}} = \begin{bmatrix} v_1 & p_1 \\ p_2 & v_2 \end{bmatrix}.$$

Као што је речено, $v_1 + p_1 = v_2 + p_2 = 1$. Граф који одговара бинарном каналу је приказан на слици:

ОКИТИ



Посебан случај бинарног канала је канал код којег је вјероватноћа преласка из 0 у 1 једнака вјероватноћи преласка из 1 у 0 ($p_1 = p_2 = p$). Такав канал је окарактерисан са само једним параметром p (јер је $v_1 = v_2 = 1\text{-}p$) и назива се бинарни симетрични канал. Код таквог канала вјероватноћа грешке P_ε не зависи од вјероватноће појављивања улазних симбола.

$$P_\varepsilon = P(0) \cdot P(1|0) + P(1) \cdot P(0|1) = p \cdot \big(P(0) + P(1)\big) = p$$

48. Капацитет канала.

Шенон је показао да капацитет канала (изражен у b/s) са бијелим Гаусовим шумом зависи од:

- средње снаге сигнала ***P_{sr}[W]***,
- спектралне густине снаге шума ***N_0[W/Hz]***, и
- ширине пропусног опсега ***B[Hz]***.

Израз за капацитет канала је дат изразом:

$$C = B\log_2\left(1 + \frac{P_{sr}}{BN_0}\right)$$

Уводећи смјену $P_{sr} = R_b E_b$, гдје је бинарни проток канала $R_b[bit/s]$, а E_b енергија по биту $[Ws/b]$, релацију можемо изразити као:

$$C = B\log_2\left(1 + \frac{E_b}{N_0}\frac{R_b}{B}\right)$$

Даље, постоји минимална вриједност односа E_b/N_0, при којој је могућ пренос са произвољно малом вјероватноћом грешке за канал са неограниченим пропусним опсегом $(B \to \infty)$, што се добија примјеном Лопиталовог правила:

$$\frac{C}{R_b} = \frac{E_b}{N_0}\frac{1}{ln2} > 1,$$

Из услова да је капацитет канала већи од бинарног протока,

$$C = \lim_{B\to\infty} B\log_2\left(1 + \frac{E_b}{N_0}\frac{R_b}{B}\right) = \frac{E_b}{N_0}\frac{R_b}{ln2},$$

слиједи:

$$\frac{E_b}{N_0} = \frac{1}{log_2 e} = ln2 = 0.693\ (-1.6\ dB)\ .$$

Вриједност добијена у претходном изразу се назива Шенонова граница и представља теоријску минималну вриједност односа сигнал-шум по биту (E_b/N_0) при којој се може обављати пренос са произвољно малом вјероватноћом грешке. Смањивање вјеровантоће грешке се може остварити избором модулационог поступка и избором заштитног кодовања. Најчешће се при пројектовању анализира допринос здруживања оба поступка. II Шеноновом теоремом доказано је да је могућ пренос информација са произвољно малом вјероватноћом грешке све док је битска брзина мања од капацитета сигнала $R_b \leq C$. За битске брзине $R_b > C$ ниједан модулациони поступак не обезбјеђује произвољно малу вјероватноћу грешке. Другим ријечима, могућ је поуздан пренос кроз непоуздан канал, све док је битска брзина мања од капацитета канала. Шенонов рад је показао да вриједности P_{sr}, N_0 и B ограничавају брзину преноса, а не вјероватноће грешке. Друга Шенонова теорема даје одговр на питање колико износи фундаментално ограничење брзине преноса у телекомуникационом каналу. Обе Шенонове теореме разматрају ограничења брзине преноса, али не дају одговор како и на који начин те крајње домете постићи. Због тога је послије Шенонових радова из 1948. развијена посебна грана Теорије информација посвећена каналском кодовању. За нешто више од пола вијека научници су развили сложене алгоритме заштитног кодовања који су се по перформансама приближили теоријским границама постављеним у Шеноновим радовима. Неки од тих заштитнох кодова су *LDPC, Турбо* и *Рид-Соломонови* кодови.

49. Код са понављањем.

Најелементарнији начин заштитног кодовања који се своди на вишеструко понављање једног симбочла. На примјер, нека се један бит понавља 3 пута. Тада је за двије послате поруке **111** и **000**, због грешака у каналу, могуће на пријемној страни добити 8 различитих порука, као што је приказано на слици:

Логично се намеће доношење одлуке на бази већинске логике. На овај начин смо извршили детектовање и корекцију једноструких грешки, те смањили укупну вјероватноћу грешке. Такође, јасно је да ћемо за двоструке и троструке грешке у датим низовима 111 и 000 имати погрешно декодовану поруку. Међутим, вјероватноћа грешке на пријему је мања него код преноса без понављања. Претпоставимо да је канал без меморије, па су грешке статистички независне. На примјер, нека је вјероватноћа грешке по симболу (биту) p=10^{-2}, и одлуку доносимо већинском логиком ''два од три'''. Односно, када се приме комбинације с мањим бројем јединица може се сматрати да је емитована кодна ријеч 000 (порука 0), а када се прими порука са већим бројем јединица, одлучује

се да је емитована кодна ријеч 111 (порука 1). Овај поступак декодовања је директна примјена правила метода максималне вјеродостојности. Грешке ће бити погрешно интерпретиране, тј. неће бити откривене, уколико се при преносу посматране кодне ријечи сва три бита погрешно пренесу или да буду погрешна било која два бита у кодној ријечи од три бита, што даје уједно и вјероватноћу неоткривене грешке:

$$P_e = \binom{3}{3} p^3 + \binom{3}{2} p^2(1-p) \approx 3p^2 = 3 \cdot 10^{-4}$$

У општем случају, за понављање поруке непаран број пута $n = 2n_0 + 1$, при чему $n_0 \in N$, вјероватноћа неоткривене грешке износи:

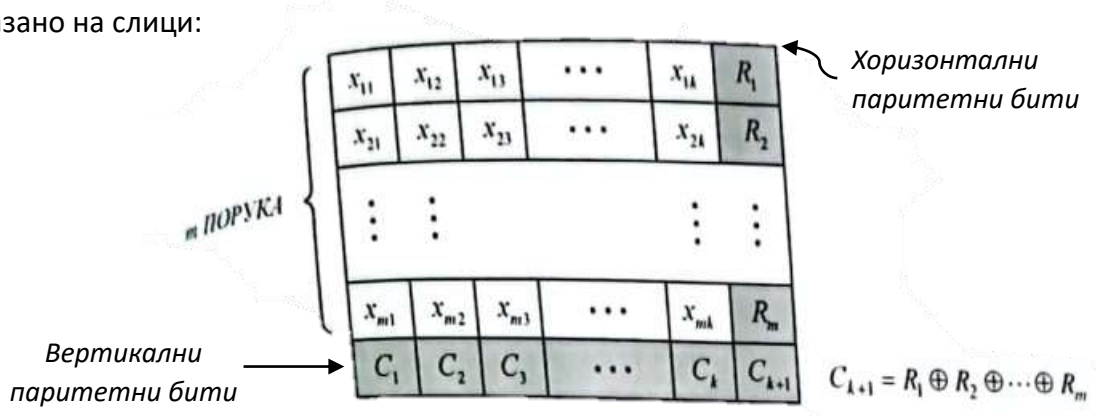
$$P_e = \sum_{k=n_0+1}^{n} \binom{n}{k} p^k (1-p)^{n-k}$$

Нажалост, поред смањења вјероватноће грешке долази до смањења брзине преноса информација, јер се сада за пренос количине информација, за код са понављањем од 1 шенона, умјесто једног користе три бита. Односно, при непромјењивом протоку информација мора се повећати битска брзина у каналу. Ово може да утиче на пропусни опсег и повећање снаге шума на улазу у пријемник.

50. Код са провјером на парност.

Код ових врста кодова се једноставно на *k* информационих бита дода само један контролни бит (*n=k+1*) провјере на парност, тако да укупан број јединица у кодној ријечи дужине *n* буде паран. Овим кодом се може открити непаран број грешака настао током преноса кодне ријечи. Међутим, паран број грешака у истом блоку је немогуће открити на овај начин, јер је и након тога укупан број јединица у блоку паран. У овом случају кодни количник је $R = \frac{n-1}{n}$.

Међутим, информациони бити се не морају посматрати као једнодимензионални низ. Информациони бити се могу сортирати у матричну форму (дводимензионално), па се у овом случају провјера на парност може обавити по врстама и колонама, како је приказано на слици:



Ако се у структури дводимензионалног кода са слике деси само једна грешка на блоку информационих бита, тада ће одговарајуће провјере на парност по врсти и колони тачно одредити позицију погрешног бита, па се грешка може исправити. У случају да се догоди више грешака, једнозначно одређивање њихове позиције је могуће само у случају да не припадају истим врстама и истим колонама. Надаље, примјењујући исту логику можемо говорити о кубним, то јест о кодовима са провјерама у три па и више димензија. Овакви кодови ће имати све већи кодни количник. Недостатак ових кодова представља временско кашњење, јер се на предаји мора сачекати формирање цијелог вишедимензионалног блока, а на пријему да се прикупи цијели блок да би се могао започети процес декодовања. Ако се користе кодови који служе само за откривање грешака, тада пријемник повратним каналом шаље захтјев предајнику за поновним емитовањем порешно примњене кодне ријечи. Наравно, недостатак овог приступа је потреба за повратним каналом и повећање укупног кашњења при декодовању.

51. Хемингов код.

У неким ситуацијама нема могућности за понављање погрешно пренесених дијелова поруке. Да би се могле исправљати грешке у примљеној поруци, идеја је да се умјесто једног уведе више контролних бита – контрола парности за неке подскупове бита у поруци. Наравно, претпоставља се да су све контроле парности линеарно независне. Хеминг је приказао фамилију кодова за откривање двоструких и исправљање једноструких грешака. Синдром, добијен као резултат провјера на парност извршених на пријему, у бинарној нотацији показује на позицију погрешног бита. Хеминг најприје одређује број различитих вриједности синдрома и закључује да број провјера *n-k* треба да задовољава израз:

$$2^{n-k} \geq n + 1,$$

јер постоји *n* позиција у кодној ријечи гдје би се могла десити грешка, као и случај када до грешке није ни дошло. Контролни бити не подлијежу провјери на парност и у принципу могли би се додати на крај кодне ријечи. Један информациони бит се може наћи у више провјера на парност. Пошто је Хеминг пошао од идеје да бинарно прочитана вриједност синдрома треба да покаже позицију погрешног бита, то позиције контролних бита у кодној ријечи треба да буду 2^0, 2^1, 2^2, …, 2^{n-k-1}. Другим ријечима, свака група бита почиње са бројем степена 2, на примјер 1, 2, 4, 8, итд. Ови бројеви су такође позиције паритетних бита. Хемингов код се може користити за кодну ријеч произвољне дужине. Сваки бит провјере успоставља непарну парност са групом бита података. Одређену провјеру на парност треба узети по свим оним позицијама чији запис у бинарном систему садржи ''1'' на том мјесту. На примјер, прва провјера би обухватила све непарне позиције чији је најнижи бит једнак јединици. Дакле, једну провјеру на парност треба узети по свим позицијама које на посљедњем мјесту у свом бинарном запису имају јединицу. Пошто ће на позицији један (2^0=1) стајати први контролни бит, провјера на парност која одређује тај контролни бит ће бити на позицијама 3, 5, 7, итд. Сљедећу провјеру треба узети по свим позицијама које имају једницу на претпосљедњем мјесту у

бинарном запису (3, 6, 7, 10, 11, ...), а одговарајући контролни бит се уписује на позицију 2^1=2. Користећи табелу са записом бројева од 0 до 15 у бинарној форми, лако се долази до позиција провјере на парност за одговарајући контролни бит (у овом случају 4 контролна бита). Тако, контролни бит на позицији 2^2=4 ће обухватити бите на позицијама (5, 6, 7, 12, 13, 14 и 15).

Позиција	Бинарни запис			
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
10	1	0	1	0
11	1	0	1	1
12	1	1	0	0
13	1	1	0	1
14	1	1	1	0
15	1	1	1	1