1. Дискретизация непрерывных сигналов. Квантование по времени и уровню.
Непрерывный сигнал представляет собой нечетное мн-во значений, т.е. эти значения нельзя пронумеровать натуральными числами. А дискретный сигнал имеет конечное мн-во значений, кот-е ограничено значением числа двоич. р-дов. Используется дискретизация сигнала по времени и его квантование по уровню. Квантование по уровню заключ. в том, что все знач. Сигнала, попавшие в ΔU_i считаются одинаковыми и = значению, которое приписывается этому интервалу квантования. Поскольку число уровней квантования конечно, то их можно закодировать доичным числом и т. о.мы получим дискретный цифровой сигнал. Возникает погрешность дискретизации, т.к. мы не учитываем знач-я исходного сигнала внутри интервалов дискретизации.

2. Восстановление непрерывного сигнала. Оценка погрешности восстановления.
1. Ступенчатая апроксимация 2. Линейная апроксимация 3. Сплайновая апроксимация (Лагранж, Чебышев). При преобразовании дискретного в неперывный мы получаем U*(t), которы отличается от исходного, т. е. имеет ошибку дискретизации $\delta = U(t) - U^*(t)$.
Оценки ошибки дикретизации:

1. по абсолютному значению $\delta_g \geq |\delta(t)|$ $t \in \Delta T$
2. среднеквадратическая оценка $\delta_g \geq \sqrt{\frac{1}{\Delta T}\int\limits_{\Delta T}[\delta(t)^2]dt} \quad t \in \Delta T$
3. Средняя погрешность $E_g \geq \frac{1}{\Delta T}\int\limits_{\Delta T}|\delta(t)|\,dt$

Интервал квантования по времени и по уровню выбирается т.о., чтобы обеспечить нужную точность квантования.

3. Теорема Котельникова.
Некоторые сведения из рядов: разложение периодической ф-ции в ряд Фурье: $F_0=1/T$; $\omega_0=2\pi F_0=2\pi/T$; $T=x_2-x_1$.
Любую непрерыв. периодич. ф-цию можно представить рядом Фурье. $U(x)=\frac{1}{2}\sum_{n=-\infty}^{\infty}A_n e^{jn\omega_0 x}$, $j=\sqrt{-1}$, $\lim\limits_{n\to\infty}\sum_{-n}^{n}A_n$

A_n – коэффициенты ряда Фурье. Мн-во всех $\{A_n\}$ назыв. спектром периодического сигнала. $A_n=\frac{2}{T}\int\limits_{x_1}^{x_2}U(x)e^{-jn\omega_0 x}dx$

Интеграл Фурье: если сигнал непериодич., то вместо ряда Фурье использ. интеграл Фурье:
$S(j\omega)=\int\limits_{-\infty}^{\infty}U(x)e^{-j\,\omega\,x}dx$ (*). Если такой сигнал сущ-т, то S(jω) – спектр непрерыв. сигнала. Спектр полностью определяет наш сигнал. С помощью обратного преобразования Фурье мы можем получить исходный сигнал:
$S(j\omega)=\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}S(j\omega)e^{jx\omega}d\omega$ (**).

Теорема Котельникова: если для сигнала U(t) существует прямое и обратное преобразование Фурье, и спектр сигнала ограничен $[-\omega_c;\omega_c]$, и на этом промежутке спектр сигнала либо непрерывен, либо имеет конечное число разрывов 1-го рода, то тогда сигнал U(t) можно полностью восстановить по его дискреным отсчетам, взятым с интервалом $\Delta T=\frac{\pi}{\omega_c}=\frac{1}{2F_e} \quad 2\pi F_c=\omega_c$

Док-во:
$U(t)=\frac{1}{2\pi}\int\limits_{-\omega_c}^{\omega_c}S(j\omega)e^{j\omega t}d\omega$ Точки дискретизации - (nΔt).
$U(n\Delta t)=\frac{1}{2\pi}\int\limits_{-\omega_c}^{\omega_c}S(j\omega)e^{-jn\Delta t\omega}d\omega$ (*). Т.к. область определения спектра ограничена, то мы можем периодически его повторить по всей оси. Периодическую функцию, которая совпадает с нашим спектром мы можем представить в виде ряда Фурье.

$$S(j\omega)=\frac{1}{2}\sum_{n=-\infty}^{\infty}A(j\omega_0 n)e^{jn\omega_0\omega}$$

$$\omega_0=\frac{2\pi}{2\omega_c}=T=\frac{\pi}{\omega_c}$$

$$S(j\omega)=\frac{1}{2}\sum_{n=-\infty}^{\infty}A(jn\frac{\pi}{\omega_c})e^{jn\frac{\pi}{\omega_c}\omega}$$

ω_0-частота повторения ф-ии спектра

$$A(jn\frac{\pi}{\omega_c})=\frac{2}{2\omega_c}\int_{-\omega_c}^{\omega_c}S(j\omega)e^{-jn\frac{\pi}{\omega_c}\omega}d\omega \quad (**)$$

Интегралы (*) и (**) совпадают с точностью до знака в показатели степени е, поэтому:

$$U(-n\Delta t)=\frac{1}{2\pi}\int_{-\omega_c}^{\omega_c}S(j\omega)e^{-n\frac{\pi}{\omega_c}\omega}d\omega$$

$$A(jn\frac{\pi}{\omega_c})=\frac{2\pi U(-n\Delta t)}{\omega_c}$$

Имея значение коэффициента ряда Фурье, мы можем написать значение нашего спектра.

$$S(j\omega)=\frac{1}{2}\sum_{n=-\infty}^{\infty}\frac{2\pi U(-n\Delta t)}{\omega_c}e^{jn\frac{\pi}{\omega_c}\omega}$$ Поскольку n пробегает все целые числа от -∞ до ∞, то мы можем заменить n на –n

$$S(j\omega)=\frac{\pi}{\omega_c}\sum_{n=-\infty}^{\infty}U(n\Delta t)e^{-jn\frac{\pi}{\omega_c}\omega}$$ Используя обратное преобразование Фурье, по спектру сигнала мы можем найти сам сигнал

$$U(t)=\frac{1}{2\pi}\int_{-\omega_c}^{\omega_c}\left[\frac{\pi}{\omega_c}\sum_{n=-\infty}^{\infty}U(n\Delta t)e^{-jn\Delta t\omega}\right]e^{j\omega t}d\omega$$ почленно интегрируем

$$U(t)=\frac{1}{2\omega_c}\sum_{n=-\infty}^{\infty}\left[U(n\Delta t)\int_{-\omega_c}^{\omega_c}e^{j(t-n\Delta t)\omega}d\omega\right]=\frac{1}{\omega_c}\sum_{n=-\infty}^{\infty}U(n\Delta t)\left.\frac{e^{j(t-n\Delta t)\omega}}{j(t-n\Delta t)}\right|_{-\omega_c}^{\omega_c}=$$

$$\frac{1}{2\omega_c}\sum_{n=-\infty}^{\infty}U(n\Delta t)\frac{1}{j(t-n\Delta t)}\left[e^{j(t-n\Delta t)\omega_c}-e^{-j(t-n\Delta t)\omega_c}\right]=\sum_{n=-\infty}^{\infty}U(n\Delta t)\frac{\sin[(t-\Delta tn)\omega_c]}{(t-\Delta tn)\omega_c}=U(t)$$

В левой части сигнал в дискретный момент времени, а в правой – в любой.

Замечания к использованию теоремы Котельникова:

1. Возможность определения значения точки по ее дискретному значению объясняется тем, что сигнал имеет конечный спектр
2. Чтобы воспользоваться т. Котельникова для сигнала с бесконечным спектром, бесконечный спектр заменяют на конечный, выбирая пороговую частоту ω_n. При этом основная часть энергии сигнала должна быть сосредоточена в $[-\omega_n;\omega_n]$

4. Квантование сигналов по уровню. Максимальные и среднеквадратические ошибки квантования.

$U(t)\in[U_{min},U_{max}]$,n,$U(t)\in[U_{i-1},U_i]\Rightarrow U^*(t)=U'_i$. 1 способ: U'_i совпадает с нижней границей интервала квантования. 2 способ: U'_i выбирается по середине соответствующего интервала квантования. Ошибка квантования: $\delta=\max_i|U_i(t)-U'_i|$. Обычно берутся одинаковые интервалы квантования: $\Delta U'_i=\Delta$. В этом случае, мы получим следующие значения ошибок: для 1 способа - $\delta=\Delta$; для 2 способа - $\delta=\Delta/2$. На практике учитыв., что сигнал U(t) имеет случ. характер => используется оценка среднеквадратической погрешности (это корень от дисперсии ошибки; δ^2-дичперсия;$\sigma_{ско}$).

$$\sigma^2=\int_{U_0}^{U_n}(U(t)-U')^2\rho_n(U)dU=\sum_{i=1}^{n}\int_{U_i}^{U_{i+1}}(U(t)-U')^2\rho_n(U)dU$$

. Предположим, что уровень квантования находится в середине интервала квантования – Δ_i. На практике интервалы квантования малы -> с достаточной точностью предполагается, что $\rho_i(U)$ внутри интервала квантования поястоянно. Сделаем замену переменных: пусть $U-U'_i=x$, тогда:

$$\sigma_i^2 = \int_{U_{i-1}}^{U_i} (U - U_i^{'})^2 \rho_i(U) dU = \rho_i(U) \int_{-\Delta_i/2}^{\Delta_i/2} x^2 dx = \rho_i(U) \frac{x^3}{3} \Big|_{-\Delta_i/2}^{\Delta_i/2} = \rho_i(U) \frac{\Delta_i^3}{12}. \ \sigma^2 = \sum^n \rho_i(U)' \frac{\Delta_i^3}{12}.$$

$\sigma^2 = \frac{\Delta^2}{12} \sum_{i=1}^n \rho_i(U)\Delta$ (ρ_i(U) – плотность распределения амплитуд внутри интервала, Δ – длина интервала).

Рассмотрим $\rho_i(U)\Delta$: т.к. мы полагали, что внутри интервала ρ_i(U) постоянно ввиду малости интервала, то $\rho_i(U)\Delta$ = вероятности попадания нашего сигнала в i-й интервал = P_i. $\sigma^2 = \frac{\Delta^2}{12} \sum_{i=1}^n \rho_i(U)\Delta = \frac{\Delta^2}{12} \sum_{i=1}^n P_i$. Поскольку сигнал попадает только в один и только в один интервал, то $\sum_{i=1}^n P_i = 1$ => $\sigma^2 = \Delta^2/12$ => $\sigma = \Delta/(2\sqrt{3}) = (U_{max} - U_{min})/(n2\sqrt{3})$ => $n = (U_{max} - U_{min})/(2\sigma\sqrt{3})$.

5. Аналого-цифровые преобразователи, их характеристики.

АЦП – преобразование аналогового сигнала в цифровую форму. Пар-ры: 1. относительная погрешность преобразования 2. разрешающая способность – ширина интервала квантования 3. быстродействие – характеризует время, кот-е требуется для преобразователя, чтобы получить сигнал в цифровой форме. Δt - в современных АЦП быстродействие достигает 1 нсек.

6. Энтропия. Свойства энтропии. Энтропия объединения нескольких статистически независимых источников информации.

Имеется дискретный источник информации, на выходе кот-го в дискретн. моменты времени появляются знаки (буквы). ИИ хар-ся состояниями: $\begin{pmatrix} U_1,..., & U_i,..., & U_N \\ P_1,..., & P_i,..., & P_N \end{pmatrix}$. $P_i = P(U_i)$ – вероятность того, что в дискретный момент времени на выходе появится буква U_i, она и называется текущим состоянием ИИ. *Энтропией* дискр. ИИ назыв. следующее выражение: $H(U) = -\sum_{i=1}^N P_i^{'} \log_2 P_i$.

Св-ва энтропии: 1. H(U)>=0, $P_i \in [0,1]$ – энтропия неотрицательна. 2. э. конечна. Если $P_i \in [0,1]$, то $\lim_{P_i \to 0}(-P_i \log_2 P_i) = \lim((\log_2 1/P_i)/(1/P_i))$=<$(1/P_i=\alpha)$>=$\lim[(\log_2\alpha)/\alpha]$=<использ. правило Лапиталя>=$\lim[(\log_2 e/2)/1]=0$. 3. если $P_i=1$, то H(U)=0: 4. э. достигает max, когда все состояния ИИ равновероятны: H(U)= $\log_2 N$ - max значение э.

э. объединения статич. независ. ИИ = сумме их энтропий: объединение ИИ:

Док-во: $P(U_i,V_j)$ – вер-ть появления пары (U_i,V_j) на выходе. H(UV) – э. объединения 2х ИИ. (*) $P(U_i,V_j)=P(U_i)P(V_j)$ – из теории вер-ти (если ИИ статистич. независимы!). H(UV)= $-\sum_{i=1}^N \sum_{j=1}^K P(U_i,V_j) \log_2 P(U_i,V_j)$ - по определению э.

по св-ву (*) => $H(UV) = -\sum_{i=1}^N \sum_{j=1}^K P(U_i)P(V_j) \log_2 [P(U_i)P(V_j)]$ =<используя правило log>=

$$\sum_{i=1}^N \sum_{j=1}^K P(U_i) \log_2 P(U_i) P(V_j) - \sum_{i=1}^N \sum_{j=1}^K P(V_j) \log_2 P(V_j) P(U_i) =$$

$$= -\sum_{i=1}^N P(U_i) \log_2 P(U_i) \sum_{j=1}^K P(V_j) - \sum_{j=1}^K P(V_j) \log_2 P(V_j) \sum_{i=1}^N P(U_i) =$$

$$= H(U) + H(V) = H(UV)$$

Используя метод мат. индукции можно док-ть, что: H(U,V,...,S)=H(U)+H(V)+...+H(S) – для нескольких ИИ.

7. Условная энтропия и ее св-ва.

В данном случае ИИ могут быть статистич. зависимыми. Из теории вер-ти: $P(U_i,V_j)=P(U_i/V_j)P(V_j)=P(V_j/U_i)P(U_i)$. Условная вер-ть – это вер-ть события U_i при условии, что произошло событие V_j. По опред-ю э.:

$H(UV) = -\sum_{i=1}^N \sum_{j=1}^K P(U_i,V_j) \log_2 P(U_i,V_j)$ =<используя $P(U_i,V_j)=P(V_j/U_i)P(U_i)$ получим> =

$$H_u(V)-H(V)=-\sum_{i=0}^{N}P(U_i)\sum_{j=1}^{k}P(V_j/U_i)\log_2 P(V_j/U_i)+\sum_{i=0}^{N}\sum_{j=1}^{k}P(U_i)\log_2 P(U_i)P(V_j/U_i)=$$

$$=\sum_{i=0}^{N}\sum_{j=1}^{k}P(V_j/U_i)\log\frac{1}{(V_j/U_i)}+\sum_{i=0}^{N}\sum_{j=1}^{k}P(V_j/U_i)\log_2 P(U_i)=$$

$$=\sum_{i=0}^{N}\sum_{j=1}^{k}P(V_j/U_i)\log_2\frac{P(U_i)}{P(V_j/U_i)}=\sum_{i=0}^{N}\sum_{j=1}^{k}P(V_j/U_i)\log_2\frac{P(U_i)P(U_i)}{P(V_j/U_i)P(U_i)}=$$

$$=\sum_{i=0}^{N}\sum_{j=1}^{k}P(V_j/U_i)\log_2\frac{P(U_i)P(U_i)}{P(V_j/U_i)}\le\sum_{i=0}^{N}\sum_{j=1}^{k}P(V_j/U_i)\left(\frac{P(U_i)P(U_i)}{P(V_j/U_i)}-1\right)=$$

$$=\sum_{i=0}^{N}\sum_{j=1}^{k}P(U_i)-\sum_{i=0}^{N}\sum_{j=1}^{k}P(U_i/V_j)=1-1=0;$$

$$H(U,V)=H(U)+H_u(V)\le H(U)+H(V)$$

Т.к. происходит 1 и только 1 событие V_j и их сумма =1 => $\sum_{j=1}^{K}P(V_j/U_i)=1$. $H_{U_i}(V)=-\sum_{j=1}^{K}P(V_j/U_i)\log_2 P(V_j/U_i)$ - условная частная э. источника V относительно события U_i.

$H(UV)=H(U)+\sum_{i=1}^{N}P(U_i)H_{U_i}(V)$, где $\sum_{i=1}^{N}P(U_i)H_{U_i}(V)$ = $H_U(V)$ – условная э. источника V относительно ИИ U и она = мат ожиданию условной частной э. <Мат ожид. дискретн. случ. величины: $M(a)=\sum_{i=1}^{N}P_i a_i$, a_i – значение случ. величины>. $H(UV)=H(U)+\sum_{i=1}^{N}P(U_i)H_{U_i}(V)=H(U)+H_U(V)$. Ввиду симметричности ИИ и V можно написать следующее: $H(UV)=H(V)+H_V(U)$.

Св-во условной э.:

потребуются следующие формулы: 1. $\log_2 x=\log_2 e\ \ln x$ (док-во: $\log_2 e\ \ln x=\log_2(e^{\ln x})=\log_2 x$). 2. $\ln x<=x-1$.

св-во: условная э. всегда меньше или равна безусловной э.: $H_U(V)<=H(V)$;$H_V(U)=H(U)$.

Док-во: $H_U(V)<=H(V)$ => $H_U(V)-H(V)<=0$.

$$H_u(V)-H(V)=-\sum_{i=0}^{N}P(U_i)\sum_{j=1}^{k}P(V_j/U_i)\log_2 P(V_j/U_i)+\sum_{i=0}^{N}\sum_{j=1}^{k}P(U_i)\log_2 P(U_i)P(V_j/U_i)=$$

$$=\sum_{i=0}^{N}\sum_{j=1}^{k}P(V_j/U_i)\log\frac{1}{(V_j/U_i)}+\sum_{i=0}^{N}\sum_{j=1}^{k}P(V_j/U_i)\log_2 P(U_i)=$$

$$=\sum_{i=0}^{N}\sum_{j=1}^{k}P(V_j/U_i)\log_2\frac{P(U_i)}{P(V_j/U_i)}=\sum_{i=0}^{N}\sum_{j=1}^{k}P(V_j/U_i)\log_2\frac{P(U_i)P(U_i)}{P(V_j/U_i)P(U_i)}=$$

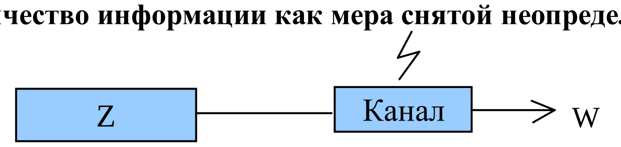
$$=\sum_{i=0}^{N}\sum_{j=1}^{k}P(V_j/U_i)\log_2\frac{P(U_i)P(U_i)}{P(V_j/U_i)}\le\sum_{i=0}^{N}\sum_{j=1}^{k}P(V_j/U_i)\left(\frac{P(U_i)P(U_i)}{P(V_j/U_i)}-1\right)=$$

$$=\sum_{i=0}^{N}\sum_{j=1}^{k}P(U_i)-\sum_{i=0}^{N}\sum_{j=1}^{k}P(U_i/V_j)=1-1=0;$$

$$H(U,V)=H(U)+H_u(V)\le H(U)+H(V)$$

Из доказанного нер-ва следует, что сумма энтропии 2х ИИ всегда меньше или равна сумме энтропий источников

8. Количество информации как мера снятой неопределенности. Основные свойства количества информации.



Определение:

Априорной неопределенностью источника информации называется:

$$I(Z_i)=-\log_2 P(Z_i).$$

В результате анализа работы канала информации и помех воздействующих на него нам известны вероятности следующих событий.

$P(Z_i/W_j)$- вероятность того,что при получении сигнала W_j был послан сигнал Z_i

Определение:

Условной апостериорной неопределенностью символа Z_i относительно принятого символа W_j называется выражение:

$$I_{wj}(Z_i)=-\log_2 P(Z_i/W_j)$$

Количество информации приходящейся на символ Z при условии приёма символа W, называется разность между априорной и аппостериорной неопределенностью.

$$I_{w_j}(z_i) = -\log_2 P(z_i) + \log_2 P(z_i / w_j) = \log_2 \frac{P(z_i / w_j)}{P(z_i)}$$

Это кол-во инф. явл. условным и касается символа Z_i при условии принятия символа W_j. Т.к. Z_i и W_j – это случ. величины, то и условное кол-во инф. будет случ. величиной. На практике нас интересует среднее кол-во инф. приходящейся на один символ. Нас интересует мат ожид. величины $I_{Wj}(Z_i)$. $M[y] = \sum_{i=1}^{N} y_i P_i$ => (на один символ)

$I_W(Z)=\sum_{i=1}^{N}\sum_{j=1}^{N} P(Z_i;W_j)\log_2 \frac{P(Z_i/W_j)}{P(Z_i)}$ =<умножим числ. и знамен. на вер-ть $P(W_j)$>=

$\sum_{i=1}^{N}\sum_{j=1}^{N} P(Z_i;W_j)\log_2 \frac{P(Z_i/W_j)P(W_j)}{P(Z_i)P(W_j)} = \sum_{i=1}^{N}\sum_{j=1}^{N} P(Z_i;W_j)\log_2 \frac{P(Z_iW_j)}{P(Z_i)P(W_j)} = I_W(Z)$ - среднее кол-во инф, приходящ. на 1 символ. Выразим кол-во инф. через энтропию (**):

$$I_W(Z) = -\sum_{i=1}^{N}\sum_{j=1}^{N} P(Z_iW_i)\log_2 P(Z_i) + \sum_{i=1}^{N}\sum_{j=1}^{N} P(Z_iW_j)\log_2 P(Z_i/W_j) =$$

$$= -\sum_{i=1}^{N}\sum_{j=1}^{N} P(Z_i)P(W_j/Z_i)\log_2 P(Z_i) + \sum_{i=1}^{N}\sum_{j=1}^{N} P(W_j)P(Z_i/W_j)\log_2 P(Z_i/W_j) =$$

$$= H(Z) - H_W(Z) = I_W(Z)$$

Среднее кол-во инф., приходящ. на 1 символ будет равно разности безусловной и условной энтропий.

Свойства количества информации:

1. Количество информации неотрицательно.
2. Если нет статистичекой связи между источником информации и получателем, то количество информации равно 0.

$I_W(Z)=\sum_{i=1}^{N}\sum_{j=1}^{N} P(Z_i;W_j)\log_2 \frac{P(Z_i)P(W_j)}{P(Z_i)P(W_j)} = 0$

3. Ввиду симметричности Z_i и W_j входящих в формулу: $I_W(z)=I_z(w)$

4. Если помехи отсутствуют, то $I_W(z)=H(z)$.

Единица измерения кол-ва инф: бит/символ или бит.

9. Информационные хар-ки источника дискретных сообщений. Эргодический источник сообщений. Теорема об эргодических последовательностях знаков. Мера избыточности источника. Производительность ИИ.

Источник информации может работать в 2ух режимах: стационарном и не стационарном. Если характеристики источника информации зависят от времени, то он работает в нестационарном режиме, иначе в стационарном режиме.

На выходе ИИ имеется бесконечная последовательность знаков(букв), среди этих последовательностей выделяются эргодические последовательности.

Эргодическая последовательность знаков это такая последовательность, которая является стационарной и в которой вероятностные характеристики появления тех или иных знаков можно определить посредством усреднения по ансамблю, так и посредством усреднения по времени.

Под стационарностью потока знаков(букв) понимается, то что вероятность появления знаков в последовательности не зависит от времени.

Вероятность появления знака Z_i может зависеть от предыдущих N знаков,такие источники информации называются источниками с памятью. Состояние источника с памятью определяется последовательностью из N предыдущих знаков. Если N=0, то это источник без памяти.

Состояние И перед появлением $Z_i = S_q$ (q – номер состояния, кот-й определяется номером послед-ти N символов, кот-я предшествует появлению символа Z_i). R – общее кол-во состояний И. Если послед-ть n, l – кол-во букв в алфивите, то max значение кол-ва состояний: l^n, $R<=l^n$. $P(Z_i/S_q)$ – вер-ть появления на выходе И символа Z_i

при условии, что И находился в состоянии S_q. $H_{S_q}(Z_i) = -\sum_{i=1}^{l} P(Z_i / S_q)\log_2 P(Z_i / S_q)$ - условная э. И Z_i при условии, что он находился в состоянии S_q. Полная э.: $H(Z) = -\sum_{q=1}^{R} P(S_q)\sum_{i=1}^{l} P(Z_i / S_q)\log_2 (Z_i / S_q)$. Частные случаи: когда сущ-т зависимость между соседними символами: R=l.

$$H(Z) = -\sum_{j=1}^{l} P(Z_j)\sum_{i=1}^{l} P(Z_i / Z_j)\log_2 [P(Z_i / Z_j)].$$

Теорема об эргодических последовательностях знаков.

Типичной последовательностью знаков называется такая последовательность, в которой вероятности появления тех или иных знаков подчиняются закону больших чисел.

N – длина последовательности знаков.

$\forall \mu > 0, \delta > 0 при N \to \infty$, то P- будет одинакова для всех типичных последовательностей и будет выполняться равенство:

$\left| \frac{1}{N}\log_2(\frac{1}{P}) - H(z) \right| < \mu$, вероятность появления нетипичной последовательности: $P_{нп} = \delta$

Доказательство теоремы для источника без памяти.

Типичная последовательность из N символов:

N i=1...L $P(Z_i)$

Поскольку типичная последовательность подчиняется закону больших чисел, то количество символов Z_i в конечной последовательности будет равна: $Z_i = N*P(i)$

Поскольку вероятность появления символов не завистит друг от друга, то используем формулу умножения,получим: $P = P_1^{P_1 N} \cdot P_2^{P_2 N} \cdot \ldots \cdot P_i^{P_i N} \cdot \ldots \cdot P_l^{P_l N}$.Возьмем log от послед-ти:

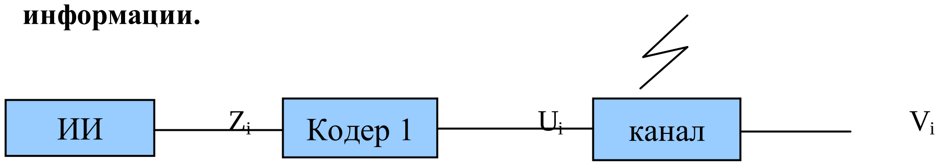
$$\log_2 P = \sum_{i=1}^{l} \log_2 P_i^{P_i N} = N\sum_{i=1}^{l} P_i \log_2 P_i = [\log_2 (1/P)]/N = -\sum_{i=1}^{l} P_i \log_2 P_i = H(Z)$$

Избыточностью ИИ назыв. следующее выражение: $D=(H_{max}(Z)-H(Z))/H_{max}(Z)$. Надо стремиться, чтобы D была min. Современные языки имеют D=50%.

Замечания к теореме об эргодическом ИИ: 1. типичные послед-ти символов явл-ся эргодическими и стационарными, а след-но подчиняются з-ну больших чисел; 2. т.к. в-ть P появления каждой эргодической послед-ти одинакова, то их кол-во будет: $n_T=1/P$. Распишем: $(1/N)\log_2(1/P) \approx H(Z)$; $n_T=1/P=2^{NH(Z)}$.

Производительностью ИИ назыв. кол-во инф., выдаваемой И в единицу времени: $\bar{I}(Z) = I(Z)/\tau_ч$, где $\tau_ч$ – средняя длительность знака на выходе ИИ: $\tau_ч = \sum_{q=1}^{R} P(S_q)\sum_{i=1}^{l} P(Z_i / S_q)\tau_{q,z}$, где P – возможное кол-во состояний И перед выходом символа Z_i; l – кол-во букв в алфавите; S_q – состояния И с памятью; $P(S_q)$ – в-ть того, что И находится в состоянии S_q; $\tau_{q,z}$ – длительность символа Z_i при условии, что И находится в состоянии с номером q. Считаем, что на выходе помех нет, тюею все они сосредоточены в канале передачи инф. => $\bar{I}(Z) = H(Z)/\tau_ч$. Чтобы повысить произв-ть ИИ, мы должны уменьшать $\tau_ч$. Для этого использ. методы эффективного кодирования, при кот-х наиболее встречающиеся на выходе ИИ знаки, должны иметь min длительность.

10. Информационные хар-ки каналов связи. Техническая скорость передачи. Скорость передачи инф. Пропускная способность канала при помехах. Коэффициент использования канала передачи информации.



Кодер 1 устраняет избыточность ИИ и осуществляет перекодировку знаков в символы.

$P(U_i/V_j)$ — вероятность того, что при приёме V_j послан U_i

Техническая скорость передачи информации — количество символов, передаваемых по каналу в единицу времени.

$\bar{I}(U,V) = VI(U,V)$

Пропускной способностью канала передачи информации называется максимально возможная скорость передачи информации: $C_q = \max \bar{I}(U,V)$.

1. При отсутствии помех и сбоев в канале связи, количество информации приходящейся на 1 символ будет равно энтропии источника:

$$C_q=V_T\log_2 m.$$

2. При помехах:

$$C_q=V_T\max(I(U,V))$$

Для того чтобы достичь максимума нужно использовать такое кодирование для символов U,которое этот максимум обеспечивает. Эту функцию обеспечивает кодер 2.

Коэффициент использования КПИ – это отношение скорости передачи инф. к пропускной способности канала: $\lambda = \bar{I}/C_q$, $0 <= \lambda <= 1$.

11. Согласование хар-к ИИ и канала передачи данных.

При передаче информации необходимо руководствоваться следующим:

1. Достоверность передачи информации (характеризуется вероятностью ошибки)

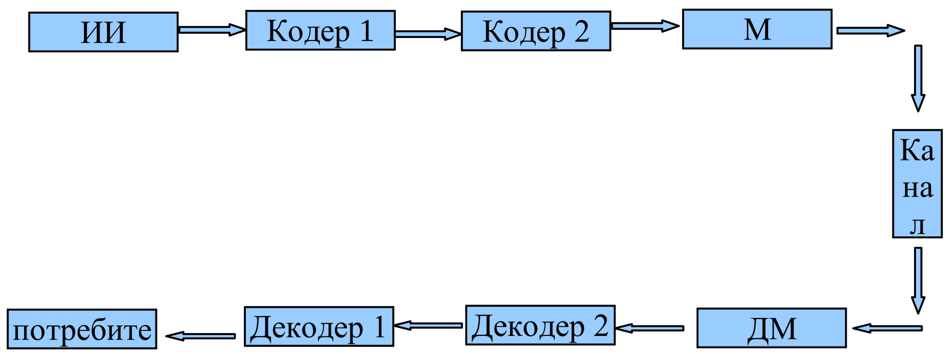
Достигается путём использования кодов исправляющих ошибки, а также использование технических средств, в которых вероятность сбоя будет минимальна.

2. Должна быть обеспечена, как можно большая скорость передачи информации

Для повышения скорости передачи информации и приближения её к пропускной способности канала связи, необходимо осуществить полное преобразование исходной информации, которое устраняет избыточность в исходной информации. Одним из способов является такое кодирование знаков(символов), при котором наиболее вероятные знаки кодируются меньшим числом символов, а знаки маловероятные кодируются большим числом знаков. Т.е. энтропия на выходе кодера 1 — max

3. Надёжность и экономичность оборудования

Как правило,статистические характеристики ИИ и характеристики помех и сбоев являются независимыми величинами, поэтому процесс кодирования можно осуществить с помощью двух кодеров.



12. Основная теорема Шеннона о кодировании для канала без помех. Пояснение к док-ву теоремы. Альтернативная формулировка теоремы Шеннона.

Кодер 1 осущ-т оптимальное кодир-е знаков, т.е. среднее кол-во символов, приходящихся на 1 знак должно быть min'м (это даст увеличение скорости передачи инф. по каналу связи, кроме того методы оптим. кодир-я использ-ся для сжатия инф. при ее хранении на маг. дисках).

Теорема Шеннона: 1. если пропускная способность КПИ больше, чем производительность ИИ, то сущ-т такой оптимальный способ кодир-я, кот-й позволяет передать инф. по каналу: $C_q > \bar{I}(Z)$. 2. если производительность ИИ больше пропускной способности канала, то не сущ-т способа кодир-я, кот-й бы позволил передать эту инф. по каналу: $C_q < \bar{I}(Z)$. В этом случае образуется неогранич. возрастающие очереди на входе канала.

Док-во:

В основе доказательства лежит идея о кодировании не отдельного знака, а достаточно большой последовательности знаков N.

По теореме об эргодическом ИИ вероятность появления последовательности равнопостоянно. При этом будем рассматривать типичные последовательности.

$$n_T=2^{NH(Z)}$$

$T=N*\tau$ – длительность

Чтобы не было очередей,необходимо,чтобы кодер работа так,чтобы закодированное сообщение имело ту же длину.

τ - длительность символа на выхожде кодера.

$\tau_и=1/V_T$.

Можно найти количество символов,которое необходимо для кодирования N – знаков.

$N=TV$

$n_k=m^k=m^{TV_T}=2^{TV_T\log_2 m}=2^{TC_q}$

$$n_{mn}=2^{NH(z)}=2^{T\frac{nz}{\tau}}=2^{T\bar{I}(z)}$$

$$n_{кодера}=2^{TC_g}>2^{T\bar{I}(z)}=n_{m.n.}, если C_g>\bar{I}(z)$$

Отсюда видно,что если пропускная способность < производительности, то количество способов,которыми можно закодировать будет больше,чем количество всех типичных последовательностей.

$$n_{кодера}=2^{TC_g}<2^{T\bar{I}(z)}=n_{m.n.}, если C_g<\bar{I}(z)$$

Для кодировки одного занака:

$$l_{cp}=\frac{\tau_n}{\tau}=\frac{T}{N}V_T=\frac{T}{N}V_T\frac{\log_2 m}{\log_2 m}=\frac{T}{N}C_g\frac{1}{\log_2 m}>\frac{T}{N}\bar{I}(z)\frac{1}{\log_2 m}=$$

$$=\frac{T}{N}\frac{H(z)}{\tau_n}\frac{1}{\log_2 m}=\frac{H(z)}{\log_2 m}$$

$$l_{cp}>\frac{H(z)}{\log_2 m}$$

$$l_{cp}>H(z)$$

Среднее количество символов требуемое для кодирования одного знака > энтропии ИИ.

Замечания:

Теорема Шенона относится к теоремам существования, она утверждает, что существует или не сучествует способ кодирования.

13. Методы эффективного кодирования. Код Шеннона-Фэно.

Эффективное кодирование: наиболее часто встречающиеся буквы кодируются меньшим числом символов; двоичные символы на выходе кодера 1 должны быть приблизит. равновероятны. Для уменьшения ошибки при передаче инф., использ. кодер 2, кот-й осущ. спец. помехоустойчивое кодирование таким образом, что имеется возможность обнаружить и исправить ошибку в принятом сообщении. Это осущ-т декодер 2. Декодер 1 превращает принятое сообщение в форму удобную для потребителя. Использование раздельных кодеров (1 и 2) возможно по причине, что как правило отсутствует статистическая связь между источником инф. и помехами, кот-е воздействуют на КПИ.

Алгоритмы оптим. кодир-я некоррелир. послед-ти знаков: некоррелир = независимая послед-ть знаков.

Алгоритм Шеннона-Фэно: для построения оптимального кода создается табл. из 3х столбцов: 1. запис-ся знаки (буквы) в порядке убывания вер-ти их появления; 2. запис-ся соответствующие в-ти появления этих знаков; 3. использ-ся для оптимального двоичного кода. 1ШАГ: табл. разбивается по горизонтали на 2 части таким образом, чтобы сумма в-тей верхней и нижней частей таблицы была примерно одинаковой; 2 ШАГ: для знаков, находящихся в верхней части запис. в 3м столбце 1, а для нижней части – 0. Процесс деления продолжается и аналогично формир-ся следующий разряд. в коде. Процесс деления продолжается до тех пор пока не закончится. Считается средняя длина кода: $l_{cp}=\sum_{i=1}^{N}P(Z_i)n(Z_i)$, где N – кол-во знаков, а $n(Z_i)$ – кол-во двоичных разрядов в коде.

Недостаток метода: неоднозначность, т.к. разбивка табл. происходит приближенно.

14. Код Хаффмена. Префиксность эффективных кодов.

Код Хаффмена. Для кодирования составляется табл.: 1ом столбце-кодируемые знаки(буквы) в порядке уменьшения вер-ти их появления. 2ом столбце-верти сооответ этим знакам.Остальн столбцы вспомогат. Он формир так: берется сумма2 последн вер-тей из предыд столбца и заносится в текущ столбец,туда же помещ остальные вер-ти. Эти вер-ти сортируются по убыванию. Процесс происх до тех пор пока в послед вспомогат столбце не будетсумма всех вер-тей=1.→2способа образ кода Хаффмана**: 1способ**)путем анализа переходов сумм последн 2х вер-тей в послед столбец.(если сумма занамает в текущ столбце послед позицию, то очередн раз-ду присв знач=0; если предпоследн позицию, то=1; если не предпосл не последн, то раз-д кода пропускается). Формируемые разряды записываются справа на лево. **2 способ**)путем построения на основе табл бинарного дерева-на ветви наносится значение соответ вер-ти: большему знач ставится в соотв-ие =1, меньшему=0.Результир код считывается с вершины дерева. Метод Хаффмана широко использ не только для оптимальн кодировании, но и при сжатии инф при хранении ее на магнит носителе, при этом никакой потери инф не происходит. **Префиксность эффективных кодов.** При оптим кодиров возник ? как отделять один код от другого. Разделители не допустимы т.к. код будет не оптимальным→префиксность оптим кодов заключ в след: ни один код имеющ меньшую длину не явл-ся началом более длинного кода.

15. Методы эффективного кодирования коррелированных послед-тей знаков.

В явном виде ал-мы Шеннона и Хаффмана к коррелированным (зависимым) последовательностям применять нельзя.

$Z_1 \ldots Z_n$ }n; $Z_{n+1} \ldots Z_{2n}$}n Для того чтобы указанные алгоритмы можно было применить к коррелированным последовательностям использ кодиров не отдельн букв, а последовательностей из n букв. Если n достаточно велико, то эти последоват-ти можно считать не коррелированными м собой и тогда к ним можно применять методы Хаффмана и Шеннона-Фено. Достаточно n>3

16. Основная теорема Шеннона о кодировании для канал с помехами. Источники помех. Формулировка теоремы Шеннона. Замечания к теореме Шеннона.

Помехи: 1.) Сбои в технич сред-вах.- связ в искажении разрядов. Для обнаруж и исправления соответ-ого разряда использ спец-ые помухоустойчив кодир инф. Кодер2-обнаруж ошибки, Декодер2-испрвление ошибки. **2.)**внешние помехи 2 вида: а)естественные-космич излучение, промышл помехи, внутр шумы радио приемных устр-в, к-ые оказались соизмеримыми со значением самого сигнала. (рис) .б) искусственные.- отдельн цифр раз-ды могут быть искажены, декодер2 может обнаружить их и исправить.(рис). **Формулировка теоремы Шеннона: 1)**Если пропускная способность канала перед инф больше чем производ-ть источника инф-ции, то сущ-ет такой способ кодирования кот-ый позволяет передать всю инф-цию по каналу со сколь угодно малой вер-тью ошибки. 2) если пропускн способ-ть канала меньше чем произ-ть источника информ, то не сущ-ет такого способа кодировния кот-ый позволил бы передать инф-ию со сколь угодно малой вер-тью ошибки. **Замечания к теореме Шеннона.1)** теорема Шеннона относ к теоремам существо-ния, она говорит о том, что сущ-ет такой способ кодирования, но ничего не говорит о самом способе кодир-ия. **2)** Д. того чтобы вер-ть ошибки стремилась к нулю нужно увелич длить-ть кодируемой посл-ти. Поскольку время T конечно, то вер-ть ошибки не равна 0.

17. Блоковые коды.

Способ помехоустойчив кодирования заключ в ведении доп информации. (рис). Блоковый код состоит из пос-ти n двоичн символов из них k –информационные символы, а n- k симв. -проверочными символами д. того чтобы можно было исправить ошибку. На выходе источ инф- блок k, на выходе кодера –блок n, добавл →появл допустимый код. На выходе канала связи могут быть как допустим так и не допустимый код, из-за наличия помех. Число возможн комбинаций на вых Ист Инф – $2^к$. Число возм. Допуст кодов на вых кодера- $2^к$. На выходе Канала передачи инф число комбин- 2^n. Способы перед инф: 1)допуст-допус-$2^к$. 2)допуст- друг допуст $2^к(2^к-1)$. 3) доп-недопуст $2^к(2^n-2^к)$. Общее число кодов передачи-$2^к*2^n$. Определим % обнаружаемых передач по каналу связи: $(2^к(2^n-2^к))/ 2^к*2^n=1-2^к/2^n$-% обнаруж неправильн передач.

Кроме обнаруж ошибки помехоуст коды позвол ее исправить. Идея исправл ошибки: 1 допуст код↔недоп коды $\check{n}_1$(кол-во недопуст кодов в кажд подм-ве), 2 доп код↔недоп коды $\check{n}_2 \ldots$,$2^к$ допуст кодов↔недоп коды $\check{n}_{2^к}$. Кол-во недопустимых кодов =$2^n-2^к$. Если доп коду поставить в однознач соответ-ие некотор подм-во не допустимых кодов, при этом подм-во недоп кодов не должно пересекаться др с др-ом и включ в себя все эти подмн-ва, все возможн недопуст коды. В этом случае по принятому непопуст коду можно найти соответ допустимый код. Число возможн передач по каналу связи когда образов-сь недопуст коды будет равно сумме эл-ов этих подм-в= $2^n-2^к$(можно исправить). Обнаружить ошибки: $2^к(2^n-2^к)$. →записыв отношение: $(2^n-2^к)/ (2^к(2^n-2^к))= 1/2^к$-кол-во исправленных меньше кол-ву кодов котор можно обнаружить→Чем больше информацион раз-ов тем меньше отношение исправлен ошибок к обнаруженным. 2 вар-та искажений радов в 2ом коде:1)искжение происходит независимо и обознач вер-т искаж p.2)искажение происх в пачке длиной b. **Кратность ошибки в коде**- кол-во искаженных разрядов r в коде длинною n . Если искаж. независ раз-ов-вер-ть появления ошибки кратностью r будет равна: $p_r= C_n^r p^r (1-p)^{n-r}$(где p_r-вер-ть того что будет искажено r-раз-ов, p-одного раз-да). **Избыточность в кодах.** Избыт-тью назыв отношение: $R=(n-k)/k$, $R \in [0,\infty)$. Тот код котор имеет min избыт-ть при заданной разреш способ-ти ошибок назыв ***Оптимальным кодом***. Код котор обеспечив наибольш кол-во допуст кодов при задан разреш способ-ти назыв ***плотноупакованным***

18. Связь корректирующей способности кода с кодовым расстоянием. Декодирование по методу максимального правдоподобия. Требования к кодовому расстоянию при обнаружении и исправлении ошибок.

Кодовым расстоянием м 2мя кодами называется кол-во 2ых разрядов в которых их значение не совпадает. Для того чтобы опред кодов. Расстояние достаточно сложить эти коды по mod2 и сосчитать кол-во едениц в рез-те. ***Мин кодов расстоян-ие***- миним расстояние м всеми допуст кодами. ***Метод max правдоподоб***-принятому недопуст коду ставится в соответ-ие тот допуст код кот-ый имеет с данным не допуст кодом min кодов расстоян-ие.(рис). **Связь корректирующей способности кода с кодовым расстоянием.** Имеется кратность ошибки –r. B_i ,B_j-допустим коды.d-кодов расстояние м ними.. Д обнаружения ошибки кратности r, расстоян м допуст кодами d должно быть таким чтобы один доп код не мог перейти в друг доп код: d>=r+1. сли использ метод max правдоподобия и при этом нужно исправить ошибки крат-ти s, то кажд допуст коду став в соответ-ие подм-во недопуст кодов,котор получ из данного допуст кода с кратностями ошиб-ок 1,2…s (рис). Если 1 раз-д исказился, то C_n^1=n, если s раз-ов то C_n^s=число недоп кодов наход на кодов расст от данного допуст кода. (рис).Из рис видно что min кодов расстоян-ие должно быть: d>=2s+1. В этом случае можно исправить ошибку кратности s.(ко-во искаж раз-ов в коде).

Оценка кол-ва допуст кодов при использ метода max правдоподоб: Общее кол-во недоп кодов соотв 1ому допуст коду→будет =:сумме всех кодов на орбите. $\Sigma^s_{i=1} C^i_n$, $\Sigma^s_{i=1} C^i_n+1 = \Sigma^s_{i=0} C^i_n$-общее кол-во кодов во мн-ве. Общее число кодов 2^n, а вкажд планет сист $\Sigma^s_{i=0} C^i_n$→кол-во допуст кодов q : $q>=2^n/(\Sigma^s_{i=0} C^i_n)$, если = то код будет плотноупакованным.

19. Показатели качества корректирующего кода. Понятие о линейных кодах.

n- общее число раз-ов, k-инф раз-ды, n-k- проверочн раз-ды- они позвол обнаруж и исправить ошибку в коде. В лин-ых кодах проверочные раз-ды формир-ся как линейная комбинация заданных инф раз-ов. Т.О. чтобы сумма по мод2 провероч раз-да и тех инф раз-ов кот-ые ему соответ-ют была =0. Пример: контроль на четность: к-инф, 1-провер раз-д. В общем случае провер раз-д формир так: $x_i \oplus\Sigma^k_{j=1}\alpha_j x_j=0$ (x_i-i- проверочн раз-д, α_j= {0 1}-указ какие инф раз-ды участв в формиров проверочн раз-да., x_j-инф раз-ды.) Если $\alpha_j=0$, то данный инф раз-д не участв в формиров данного проверочн раз-да. α_j=1-то участв. $x_i=\Sigma^k_{j=1}\alpha_j x_j$

20. Построение двоичного группового кода. Опознаватели (синдромы). Определение проверочных равенств. Примеры.

Вектор ошибки ξ– n раз-ый 2ый код в котором единицы записываются в тех разрядах, в которых были ошибки. Недопуст код= допуст код⊕ξ. Зная вектор можно восстановить правильн допуст код: допуст код= Недопуст код⊕ξ . Если взять все доп коды и конкрет вектор ошибки и образовать с помощью этого ветора все возможн недоп коды, тогда приняв недоп код и можем сопоставить ему вектор ош, то можно установить дапуст код: недоп коды для ξ_1….недоп коды для $\xi_{\Sigma^s_{i=1} C_i^n}$.Если мы смож однознач сопост кажд вектору ош-ки n-k(опозноват ош-к , синдром ош) разрядный код, то опять в этом случае можно найти вектор ош-ки. Для формиров опознователей использ проверочн разряды в коде. Опред размера помехоуст кода: к-колво инф разр, n-длина блока. Пусть в алфавите Q букв, для закодиров-ия нужно иметь k-инф-ых разрядов и должно выполн след нер-во: $2^к$-1>=Q=>k, n-k-провер раз-ов должно быть достаточно чтобы пронумеровать все вектора ошибки. **1)**Если однократ ош S=1, то число ошибок $2^{n-к}-1>=C_n^1=n$→n , отсюда нер-во: $2^n-2^к>= n=C_n^1$.В случае рав-ва не всегда явл ДОС-м для того чтобы пронумеровать все вектора ош. d>=2s+1. **2)** Ошибка кратности s. Тогда вып нер-во: $2^n-2^к>=C_n^1+ C_n^2 +…+C_n^s$=>n. Исходя из нер-ва наход длину блока(кода) n. ***Пример обнаруж однократ ош-ки***: Пусть Q=15, s=1,Опред размер кода: $2^к$-1>=15=>к=4, Длина блока: $2^n-2^к$>= n=> n=7(раз-ов) составл табл опознават и вектор-в ош-к:

Вектор ош-ки	**Сидром он-ки**
0000001	001
0000010	010
0000100	011
0001000	100
0010000	101
0100000	110
1000000	111
7654321-нумерац	(нумер по пор-ку, n-k=3разр)

Сформир провер раз-ды, так чтобы $\oplus\Sigma\alpha_i x_i=0$. 1)когда в послд раз-де опозновата будут 1,будут тогда козда была ош в 1ом,3,5,7 раз-де 1, сфортир рав-во: $a_1\oplus a_3\oplus a_5\oplus a_7=0$. если все раз-ды правильны, то ра-во будет соблюдаться. Если однократ ошибка и в сущ ош-ка в к-либо раз-де рав-во выполн не будет. 2) в синдроме во 2м раз-де. $a_2\oplus a_3\oplus a_6\oplus a_7=0$. 3) 2) в синдроме во 1м раз-де. $a_4\oplus a_5\oplus a_6\oplus a_7=0$. (опред декодером). Т.К число провер ра-ов =3,то этих рав-в будет достаточно чтобы сформир проверочн раз-ды. Из кажд ра-ва выдел те рзр-ды котор не встреч в друг ра-вах, тогда выдел проверочн раз-ды: $a_1= a_3\oplus a_5\oplus a_7$, $a_2= a_3\oplus a_6\oplus a_7$, $a_4= a_5\oplus a_6\oplus a_7$(делает кодер). Кодер формир провер раз-ды, а декодер провер эти нер-ва. Если рав-ва не соблюд, то в соответ раз-де сдрома наход 1, т.о. опред все раз-ды опозноват. ***обнаруж многократ ош-ки***: s>1, не всегда удается пронумеровать вектора ош подряд. Поэтому сост спец табл опознават. Сост табл опознават д одиночн ошибок, а опознават д 2х кратн ошибок получаются суммированием по мод2 опознават соответ однократн ошибок.

21. Матричное представление линейных кодов. Примеры.

Рассматрив поле Галуа GF(2) {0;1}. Над полем сущ-ют векторн пр-ва→V=(0,1,0,1,1) n=5-размерность→матрица-в кач-ве строки матрицы явл вектор [$v_1 v_2 … v_k$] .Можно производ все дей-ия: умножение: $A_{l,m} *B_{n,m}=C_{l,m}$. Эл-т мотрицы опред так: $C_{ij}=\oplus\Sigma^n_{q=1}a_{iq}*b_{qj}$.Лин незав-ть векторов: $v_1 v_2 … v_n$, $\alpha_1 v_1+…\alpha_n v_n=0$, вектора будут лин независ том случае если $\alpha_i=0$, i=1,n.**Образующая матрица д формиров лин кода**: Пусть имеется код сост из к инф рз-ов: $A_к$. Получ образующ матрицу $M_{k,n}$.Допуст код получ так: $A_n= A_к* M_{k,n}$.Матрица явл лин оператором, поэтому получ лин код. Получим матрицу $M_{k,n}$: $M_{k,n}=[v_1 v_2 … v_k]$, $A_к=(a_1, a_2,…,a_i,…, a_k)$. Умножим $M_{k,n}$на $A_к$:A

$_n=\Sigma^{к}_{i=1}a_i{*}\,v_i$. Т.О помехоуст код А $_n$ предст собой лин комбинацию векторов кот-ые записаны в соответ строки матрицы. Кол-во таких векторов А $_n$-число $2^к$-1. Для формиров всех векторов А $_n$ необход что бы все строки матрицы $v_1\,v_2\ldots\,v_k$ должны быть бызисом векторного прост-ва.Берем стандартн базис: 100…0,010…0,000…1. Остальные n-k раз-ов или компонент в векторе v_i. явл проверочными разр-ми к-ые в свою очердь явл лин-ой комбинац инф раз-ов, поэтому матр имеет вид:

Наличие метр I_k обеспечив лин нез-ть $M_{k,n}\rightarrow$можем закодир $2^к$-1 допуст кода. Матрица Р должна быть сформир так чтобы можно было исправить s

$a_j=\Sigma^{k}_{i=1}a_ip_{ij}$.(1). Первые k раз-ов рез-ого кода совпад с исходн инф-м кодом. Найдем эл-ты матрицы Р. Вес вектора=кол-во едениц в векторе. (*в)*. Лемма: мин кодов расстояние длин кодов рано мин весу д этих кодов. Эл-ты матрицы Р выбир исходя из ошибки кратности s=>. d>=2s +1, должны обеспечивать мин треб кодовое расстоян (см Лемму), т.е. кол-во едениц в кажд коде должно быть не менее чем d. $A_n=A_kM_{k,n}=(a_1,..,a_k){*}[v_1,\ldots,V_i]=$ $=\Sigma^{к}_{i=1}a_i{*}\,v_i$. Т.О. д образ кода складыв те строчки образ матрицы д кот-ых соответ раз-д исходн кода=1. ⇒эл-ты матр P_{ij}, выбир так, чтобы д люб исходн кода число еден в рез-щем коде было <d. ***Проверочная матрица*** .-использ для исправл ош в принятом коде. $H^т=[P\ I]$. Раз-ть столбцов = n-k, строк- n. $\tilde{A}_n{*}\,H^т=(S_{k+1},\ldots,s_j,\ldots,s_n)$-вектор s – синдром ош-ки, и =0 если выполн провероч нав-во(1). $s_j=\Sigma^{k}_{i=1}a_ip_{ij}\oplus a_j$, если рав-во (1) выполн то a_j=0. Предполож что из-за помех была ошибка: $\tilde{A}_n{*}\,H^т=(A_n+\xi){*}\,H^т=A_n\,H^т$(прав код =0)+ $\xi\,H^т=\xi\,H^т$. Т.О. сидром зависит от вектора ошибки и не завис от исходн кода. Д исправл ош-ки вычисл все возм синдромы ош д всех возмож векторов ош-к: $S=\xi\,H^т$. При обнар ош-ки Декодер2 сравнив вычисл заранее синдромом ош принятого кода с тем синдр кот у него есть→опред вектор ос помощ егго исправл эти ошибки.

22. Общее понятие и определения для циклических кодов. Математический аппарат для циклических кодов. Требования к образующему многочлену.

В циклич кодах использ мн-ны над полем Галуа: $a_{n-1}x^{n-1}\oplus a_{n-2}\,x^{n-2}\oplus\ldots\oplus a_1x^1\oplus a_0x^0$. Коэф мн-ов могут быть 0 или 1. Под слож поним сумма по мод2. Соотв-ий двоичн код представл в виде мног-на, где цифры этого кода явл коэфиц этого кода. Циклич коды явл подм-вом лин кодов и они формируются путем циклич сдвига, так назыв образ мн-на кода. 0101(←)⇒1010(0101÷(0x3+1x2+0x+1)*x(для осущ цикл сдвига)=0x4+1x3+0x2+1x+0=1010. Если в старшем раз-де ($1x^{n-1}$)=1, то д циклич сдвига надо умножить на x и добавить к руз-ту x ⊕ ($x^n\oplus1$).Идея циклич кодов закл в том что он образ путем циклич сдвига образующ-го многочлена. (слож иумнож по мод2 легко реализ в регистрах сдвига-широк распростр технике. **Требования к образующему многочлену.** Преобраз циклич кодов в строки образ-ей матрицы запис не вектора, а мн-ны. Строки образ мотрицы получ путем послед-ого циклич сдвига образ мног-на при этом допуст циклич коды должны делиться без остатка на образ мног-н: $g_i(x)$-мног-н в I строке: а)степень = n-1-мах возм, б) степень < n-1. Осущ циклич сдвиг мы $g_i(x){*}$ x.Мн-н образ в ре-те циклич сдвига опред след образом: $(g_ix)\mathrm{mod}(x^n+1)$.-даст необх циклич сдвиг.a=b mod c-b - a делится на с без остатка, a-явл остатком от деления b на c⇒ a)(x^n+…+) / $x^n+1=(x^n+1)$+…+1(цикл сдв) / (x^n+1)=1+остаток/ x^n+1. б)deg(g_ix) ≤n-1. В обоих случаях цикл сдвиг будет давать остаток мн-на n-1. Допуст коды можно предст в виде: f(x)*g(x) (g(x)-образ мн-н. Подмн-в таких мн-ов в алгебре наз идеал над мног-ом g(x). $g_2(x)=g_1(x){*}x+\alpha(x^n+1)$ ($g_2(x)$-вторая строка матр). deg g_i (x)<n-1=> α =0, deg g_i (x) =n-1=>α =1. g_2-должно дел-ся на g(x), $g_1(x)$-дел-ся на g(x)→ x^n+1 должно дел-ся на g(x).Если прин код приделении даст остаток $r_i(x)$не=0 , то $r_i(x)$-синдром ошибки. Пусть m=deg (g(x))-степень образ-его мног-на. Наиб кол-во остатков 2^m-1 получ если g(x) явл неприводимым многочленом(делится на самого себя и на 1). Мах степень мног-на : мах deg= n-1, степень образ мн-на deg (g(x))= m, мах deg f(x)= n-1- m. 2^{n-m}-1-кол-во допуст кодов-оно должно быть равно кол-ву различн кодов соответ-х информацион кодов: $2^к-1=2^{n-m}-1$=> m= n-к(степень образ раз-ов =числу провер раз-ов).Требования к образ мн-нам: 1) g(x)-делитель x^n+1 2) g(x)-простое не привод 3) deg (g(x))= n-к(к-кол-во разр, n-длина кода)

23. Выбор образующего многочлена по заданному объему кода и заданной корректирующей способности. Обнаружение одиночных ошибок.

$a_к(x)$-исходн инф код(мн-н), $a_n(x)$-правильн или допустимый код, $\tilde{a}_n(x)$-искаженный код, $\tilde{a}_n(x)=a_n(x)+\xi(x)$, $\xi(x)=x^{l\text{-номер раз-да где ошибка}}$ l=(0,1,…, n-1) , g(x)-образ-ий код, $a_n(x)$-делится на g(x) без остатка => остаток($\tilde{a}_n(x)$/ g(x))=остаток (ξ (x)/ g(x)). Предполог использ мн- н g(x)= x +1, явл ли этот мн-н делителем x^n+1; $x^n+1=(x+1)(x^{n-1}+x^{n-2}+\ldots+1)=x^n+x^{n-1}+\ldots+x+x^{n-1}+\ldots+x+1=x^n+1$-прост мн-н делится на 1 и на самого себя. =>(x^l/ x+1)= $(x^l+1/\,x+1)_{(\text{ост от дел}=0)}+(1_{(\text{остаток})}/\,x+1)$. Т.О. мы действит обнаруж одиночн ошибку. Фактически он сводится к добавл проверочн раз-да при контроле на четность. Такой контроль на четность и так образ мн-н позвол обнаружив ошибки произошедш в нечетном кол-ве раз-ов.ξ(x)= $x^{l1}+x^{l2}+\ldots+x^{lp,(\text{кол-во раз-ов где произош ошибка})}$ $(x^{l1}+1)+(x^{l2}+1)+\ldots+(x^{lp}+1)+\Sigma^{p}_{i=1}1$ <кажд (x^{l1}+1), (x^{l2}+1) делится без остатка на x+1, p-нечтно то $\Sigma^{p}_{i=1}1$ =1 >=ост(ξ (x)/x+1)=1 не=0

24. Исправление одиночных ошибок и обнаружение двойных с помощью циклического кода. Примеры.

S=1, к-число инф раз-ов. $2^к$-1>=Q(кол-во букв в алфавите)=>k , $2^{n-к}-1>=C_n^1$=n=>n-длина кода. Зная величины n и к можно нйти степень образующ-ого многочлена: m= n-к (в таблице можно посмотреть простые мн-ны нал полем Галуа. Теорема Паттереона: Пусть имеется мн-н вида: $x^{2q-1}+1=x^n+1$(q-целое число). Мн-н может быть представлен виде произвед простейших мн-ов со степенями кот-ые явл делителями q, т.е. 1,.., q. С помощью этой теоремы можно д-ть что мн-н x^n+1 можно разложить на просые мн-ны. Пример: Есть код: n=14, к=11, m= n-к=4, 1) $x^n+1=x^{15}+1=x^{2(4)-1}+1$. q=4, по теор Паттереона x^n+1 может быть предст в виде прост мн-на: 1,2,4=делим

на q. 2) $2^{n-к}-1>= n$, $2^4-1>=n$, 15=15. 3) чему будет равно: $x^n+1=$
$x^{15}+1=[(x+1)(x2+x+1)][(x4+x+1)(x4+x3+1)](x4+x3+x2+x+1)=\ldots= x^{15}+1$. образ мн-н g(x)= (x4+x3+x2+x+1) можно взять как образ-щий,т.к. он делится на x^{15} и x^1, но можно взять люб другой.

25. Обнаружение ошибок кратности 3 и ниже с помощью циклических кодов. Обнаружение и исправление независимых ошибок произвольной кратности. Обнаружение и исправление пачек ошибок.
1)Код Хэмингад, обнаружение ош –ки s+1. g(x)-мн-н котор позвол обнаружить ошибку кратности s. Хэмминг показал что: мн-н g(x)(x+1)-позвол обнаруж ошибки s+1, т.е. добавл еще 1 раз-д д контроля на четность.
2)Циклические коды Боуз, Чоундхури, Хоквингем позвол исправить ош-ки кратности s, обнаруж ошибку крат-ти 2s, длина кода при этом мож предст в виде $n=2^q-1$, $s<n/2$, число провер раз-ов: n-к< s *q. Относится к независ ошибкам в раз-дах.. 3) Коды исправл ошибки в пачке раз-ов. ***в***-длина пачки раз-ов-есть циклич код длиной n и к инф раз-ов. Для исправл ошибки в пачке раз-ов должно выполн условие: n-к<2 ***в***. Эти коды назыв: коды Бартон, Файар, Рид-Соломон.

26. Методы образования циклического кода. Матричная запись циклического кода.
Имеется образующий мн-н g(x)и имеется мн-н a(x) соответ-ий исходн коду A_k, $a(x)\div A_k$. Допустим циклич код должен делиться без остатка на образ-ий мн-н g(x). Если код не допустимый, то остаток от деления будет опознавателем(синдромом ош-ки). $f(x)\div A_n$-правильн допуст помехоуст код., $n(x)\div \tilde{A}_n$-соответ принятому коду. Простой способ формирования цикл кода: 1) f(x)= a(x) *g(x), f(x)-делится без остатка на g(x). Так способ облад недостатком: инф и проверочн раз-ды будет перемешаны др с другом, для избавдения от недостатка польз след приемом: 2) deg (g(x))= m= n-к (deg-степень образ мн-на), а) $a(x)*x^m$; б) находим остаток от деления: r(x)= ост($(a(x)*x^m)$ / g(x)) ; deg (r(x))<m-степень от деления должн быть меньше чем m, $f(x)= a(x)*x^m\oplus r(x)$. Поскольку степень остатка меньше чем m, то все инф раз-ды будут наход в начале блока. Докажем что f(x) делится на g(x)(код допустимый). Из определ делимого, делителя,частного и остатка имеем такое рав-во: $a(x)*x^m{}_{(делимое)}=$ $q(x)_{(частное)}*\ g(x)_{\ (делитель)}\oplus r(x)_{\ (остаток)}$ => $f(x)= a(x)*x^m\oplus r(x)= q(x) * g(x)$=>видно что f(x) делится на g(x) без остатка. **Формиров образ матрицы для циклич кодов**. В образ матрице строками явл не вектора, а мн-ны над полем Галуа и она имеет вид: $M_{k,n}= [I_k(x)\ C_{k,n-k}(x)]$, $I_k(x)$-позвол формировать систематич-ки помехоуст код, где инф раз-ды наход в начале кода. $C_{k,n-k}(x)$-служит для формирв проверочн раз-ов. Поскольку код циклический, то кажд строка матрицы должна без остатка делиться на образ мн-н g(x). Образование строки матрицы: $b_i(x)$ – i –ая строка матрицы. Берется соответ-ая строка ед-ой матрицы: $b_i(x)= I_{i,k}(x)*x \oplus r_i(x)$- остаток формир так: $r_i(x)$=ост $(I_{i,k}(x)*\ x^m)/\ g(x)$. Докажем что i –ая строка матрицы ($b_i(x)$) делится без остатка на g(x). $I_{i,k}(x)*\ x^m= q_i(x)_{(частное)}*$ $g(x)_{\ (делитель)}\oplus r_i(x)_{\ (остаток)}$ $\Rightarrow$переносим остаток в лев часть: $b_i(x)= I_{i,k}(x)*\ x^m\oplus r_i(x)= q_i(x)_{(частное)}*\ g(x)_{\ (делитель)}$.
Видно что делится.