Formler INCO

Self information:

Enhed = bits

$$I_i \equiv -log_b P_i = log_b(\frac{1}{P_i})$$

Hvi s man har to uafhængige symboler (hver deres sandsynlighed P_i og P_j)

$$I_{i,j} = log_b \frac{1}{P_i P_j} = log_b \frac{1}{P_i} + log_b \frac{1}{P_j} = I_i + I_j$$

Entropi:

Enhed = bits/symbol

$$H_b(X) = \sum_{i=1}^{M} P_i I_i = \sum_{i=1}^{M} P_i log_b(\frac{1}{P_i})$$

Information rate:

$$R = \frac{nH(X)}{(n/r)} = rH(X) bps$$

Extended discrete memoryless source:

$$H(X^n) = nH(X)$$

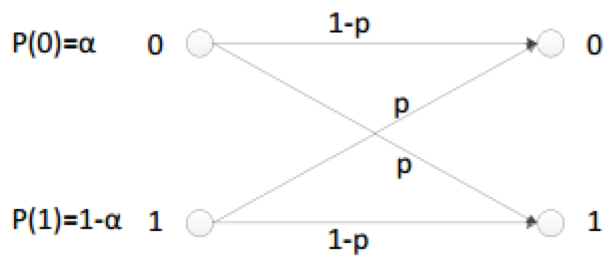
Transition probability matrix;

$$P_{ch} = \begin{bmatrix} P(y_1/x_1) & P(y_2/x_1) & \dots & P(y_V/x_1) \\ P(y_1/x_2) & P(y_2/x_2) & \dots & P(y_V/x_2) \\ \vdots & \vdots & & \vdots \\ P(y_1/x_U) & P(y_2/x_U) & \dots & P(y_V/x_U) \end{bmatrix}$$

summen af en række = 1

Binary symetric channel (BSC)

$$H(X) = \Omega(\alpha) = \alpha log_2\left(\frac{1}{\alpha}\right) + (1-\alpha)log_2\left(\frac{1}{1-\alpha}\right)$$

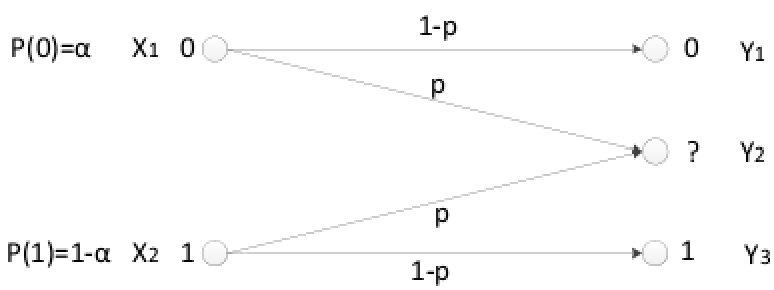


$$P_{ch} = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$$

$$I(X,Y) = H(Y) - H(Y/X) = \Omega(\alpha + p - 2\alpha p) - \Omega(p)$$

$$C_s = 1 - \Omega(p)$$

Binary erasure channel (BEC):



$$H(Y/X) = \sum_{i,j} P(y_j/x_i)P(x_i)\log_2\frac{1}{P(y_j/x_i)} = p\log_2\frac{1}{p} + (1-p)\log_2\frac{1}{(1-p)} = \Omega(p)$$

$$I(X,Y) = H(Y) - H(Y/X) = (1-p)\Omega(\alpha)$$

$$C_s = 1 - p$$

Output probability:

$$P(y_j) = \sum_{i=1}^{U} P(y_j/x_i)P(x_i)$$

Forward probability:

$$P(y_j/x_i)$$

$$\boxed{\begin{aligned} P(x_i, y_j) &= P(x_i/y_j)P(y_j) = P(y_j/x_i)P(x_i) \\ P(y_j) &= \sum_i P(y_j/x_i)P(x_i) \\ P(x_i) &= \sum_j P(x_i/y_j)P(y_j) \end{aligned}}$$

Backward probability:

$$P(x_i/y_j) = \frac{P(y_j/x_i)P(x_i)}{\sum_{i=1}^{U} P(y_j/x_i)P(x_i)}$$

Mutal information:

$$I(X, Y) = H(X) - H(X/Y) = H(Y) - H(Y/X)$$

Equivocation:

$$\sum_{i,j} P(x_i, y_j) log_2 \left[\frac{1}{P(x_i/y_j)}\right] = H(X/Y)$$

Priori entropy:

$$H(X) = \sum_i P(x_i) log_2 \left[\frac{1}{P(x_i)}\right]$$

Posteriori entropy:

$$H(X/y_j) = \sum_i P(x_i/y_j) log_2 \left[\frac{1}{P(x_i/y_j)}\right], i = 1, 2, \ldots, U$$

Channel capacity:

$$C_s = \max_{P(x_i)} I(X, Y)$$

Shannon

- Even though there are the total M^{n_f} possible sequences which can be emitted by information source alphabet $A = \{x_1,\ x_2, \dots,\ \ x_M\}$, ONLY $2^{n_f H(X)}$ sequences have a significant probability of occurrence.

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

- where B is the bandwidth, S is the signal power, N_0 is the power density of the noise;

Rewrite the above equation using E_b average energy per bit:

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

Linear Block Codes:

Code length = n

Number of message bits = k

Number valid code words = 2^k

Coding rate: R = k / n

Redundant bits: r = n - k

Generator matrix:

$$\mathbf{c} = \mathbf{m} \circ \mathbf{G} \quad = \quad (m_0, m_1, \ldots, m_{k-1}) \circ \begin{bmatrix} g_{00} & g_{01} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & \cdots & g_{1,n-1} \\ \vdots & \vdots & & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

- A systematic linear block code $C_b(n, k)$ is uniquely specified by a generator matrix of the form:

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} = \begin{bmatrix} p_{00} & p_{01} & \cdots & p_{0,n-k-1} & 1 & 0 & 0 & \cdots & 0 \\ p_{10} & p_{11} & \cdots & p_{1,n-k-1} & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$
$$= \begin{bmatrix} P & I_k \end{bmatrix}$$

- Submatrix P is of size $k \times (n-k)$;
- Submatrix I_k is of size $k \times k$.
- Generator matrix $\mathbf{G}$ is of size $k \times n$.

Parity check matrix:

$$\mathbf{H} = \begin{bmatrix} I_{n-k} & P^T \end{bmatrix}$$

Rows: n-k, Coloums: n

Syndrome error detection:

$$\begin{aligned} \mathbf{s} &= \mathbf{r} \circ \mathbf{H}^T \\ &= (\mathbf{c} \oplus \mathbf{e}) \circ \mathbf{H}^T \\ &= \mathbf{c} \circ \mathbf{H}^T \oplus \mathbf{e} \circ \mathbf{H}^T = \mathbf{e} \circ \mathbf{H}^T \end{aligned}$$

Probability of undetected error:

$$P_{\mathrm{U}}(E) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}$$

Probability of uncorrected error:

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

Error Capabilities:

dmin = Minimum number of ones in any row of G (Minimum number of ones in any columns of H + 1)

Error correction capability: t = (dmin-1) / 2

Error detection capability: dmin-1

Cyclic code verification:

- if $g(X)$ is a generator polynomial of a given linear cyclic code $C_{cyc}(n, k)$, then $g(X)$ is a factor of $X^n + 1$.
- if a polynomial of degree $r = n - k$ is a factor of $X^n + 1$, then this polynomial generates a linear cyclic code $C_{cyc}(n, k)$.

Encoding of cyclic code in systematic form:

- **Summary** Encoding of a cyclic codes $C_{cyc}(n, k)$ in systematic form consists three steps:
  1. Multiplying the message polynomial $m(X)$ by X^{n-k}, forming $X^{n-k}m(X)$;
  2. Diving $X^{n-k}m(X)$ by $g(X)$, obtaining the remained polynomial $p(X)$;
  3. Forming the code polynomial $c(X) = p(X) + X^{n-k}m(X)$.

Cyclic code syndrome polynomial:

- We know $r(X) = q(X)g(X) + S(X)$

r / g = q*g + S

When r(X) is divided by g(X) syndrome is the remainder

Conjugated roots:

- The element β^{2^l} is called the conjugate of β.

Minimal polynomial:

Theorem B.6: Let $\phi(X)$ be the minimal polynomial of the element β of the Galois Field GF(2^m), the let e be the smallest non -zero integer number for $\beta^{2^e} = \beta$, then the minimal polynomial of β is

$$\phi(X) = \prod_{l=0}^{e-1}(X + \beta^{2^l})$$

BCH Code:

	BCH code
Code length	$n = 2^m - 1$
Number of parity bits	$n - k \leq mt$
Minimum Hamming distance	$d_{min} \geq 2t + 1$
Error correction capability	t

$$g(X) = \mathrm{LCM}\{\phi_1(X), \phi_3(X), \ldots, \phi_{2t-1}(X)\}$$

The degree of the generator polynomial is r = n-k