Linear Codes

Linear code form parity bits from linear combinations of source bits. } Hamming codes are linear

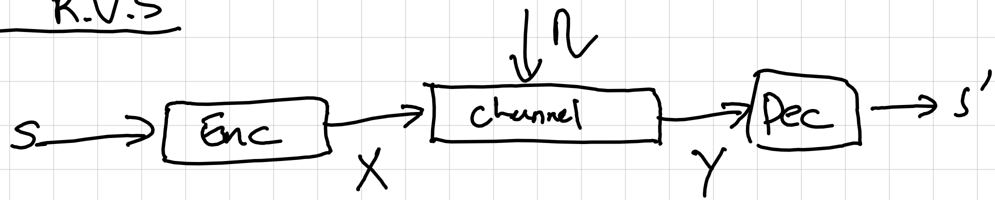
$$\underline{t} = \underline{s}\,\underline{\underline{G}} \qquad \underline{\underline{G}} = \begin{bmatrix} 1000101 \\ 0100110 \\ 0010111 \\ 0001011 \end{bmatrix}$$

Encode syndromes

$$\underline{\underline{H}} = \begin{array}{c} \begin{bmatrix} 101 \\ 110 \\ 111 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix} \end{array} \begin{array}{l} \leftarrow \text{if bit 1 should be flipped} \\ \leftarrow \text{bit 2} \\ \vdots \\ \\ \\ \\ \\ \end{array}$$

$$\boxed{\text{Uglier than circles but it generalises}}$$

Correlated R.V.S



No Noise $\Rightarrow$ $X = Y$ One R.V.

Noise $\Rightarrow$ $Y \neq X$ Two correlated R.V.S

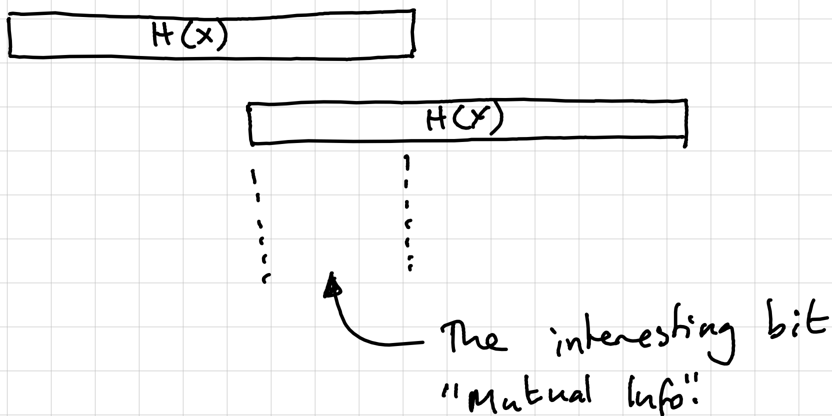
If not correlated then no info is passing $X \to Y$

Key question $\Rightarrow$ How much of the info in X gets to Y?

$\Rightarrow$ We want the $\boxed{\text{Mutual Information}}$ between X and Y

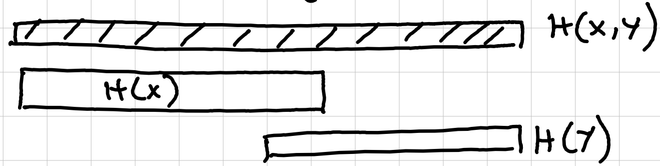
$\Rightarrow$ But how does this relate to Entropy??

<u>Visually</u>



Joint Entropy $H(X,Y)$

Total entropy of two R.V.s together



$$\boxed{H(X,Y) = E\left(\log_2 \frac{1}{P(x,y)}\right) = \sum_{x \in A_X} \sum_{y \in A_Y} P(x,y) \log_2 \frac{1}{P(x,y)}}$$

X,Y independent $\Rightarrow$ $H(X,Y) = \sum_x \sum_y P(x)P(y) \log_2 \frac{1}{P(x)P(y)}$

$$= \sum_x \sum_y P(x)P(y) \log \frac{1}{P(x)} + P(x)P(y) \log \frac{1}{P(y)}$$

$$= \quad H(X) \quad + \quad H(Y)$$

Not independent $\Rightarrow$ $H(X,Y) < H(X) + H(Y)$

E.g. 8.1

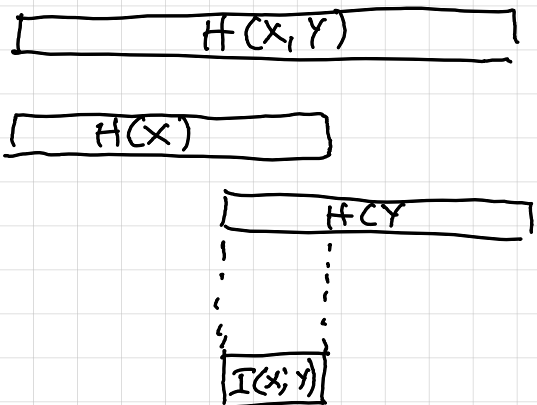
Select an integer 1-8 inclusive

Let $X \rightarrow$ number is even
$Y \rightarrow$ number is prime

$H(X, Y) = ?$

Mutual Information $I(X;Y)$

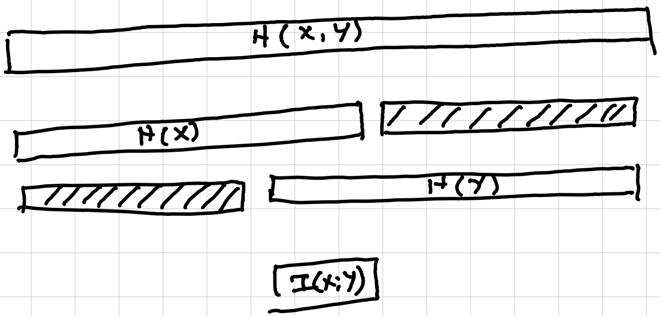
"The ave info. gained about y when we know x"



$$\boxed{I(X;Y) = H(X) + H(Y) - H(X,Y)}$$

$$\boxed{I(X;Y) = I(Y;X)}$$

Visualisation



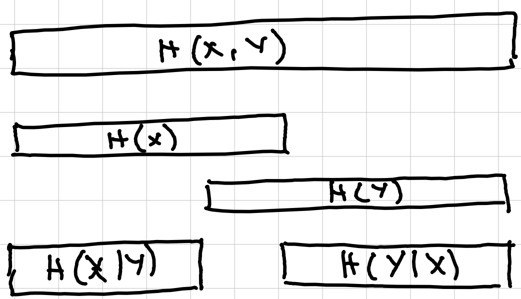
Also useful to link to conditional entropy

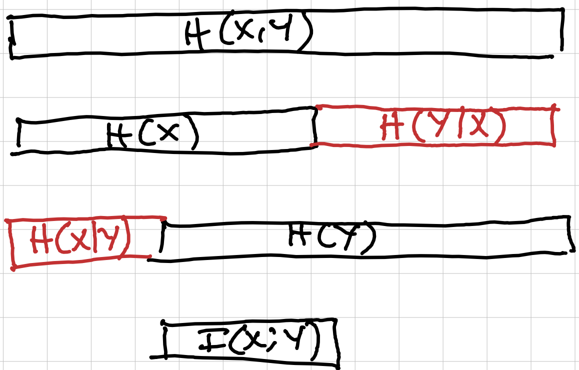
Conditional Entropy $H(X|Y)$

The uncertainty left in X when you know $Y=y$

$$H(X|Y) = E\big(H(x|y)\big)$$

$$\boxed{H(X|Y) = \sum_{y \in A_y} P(y) \sum_{x \in A_x} P(x|y) \log_2 \frac{1}{P(x|y)}}$$

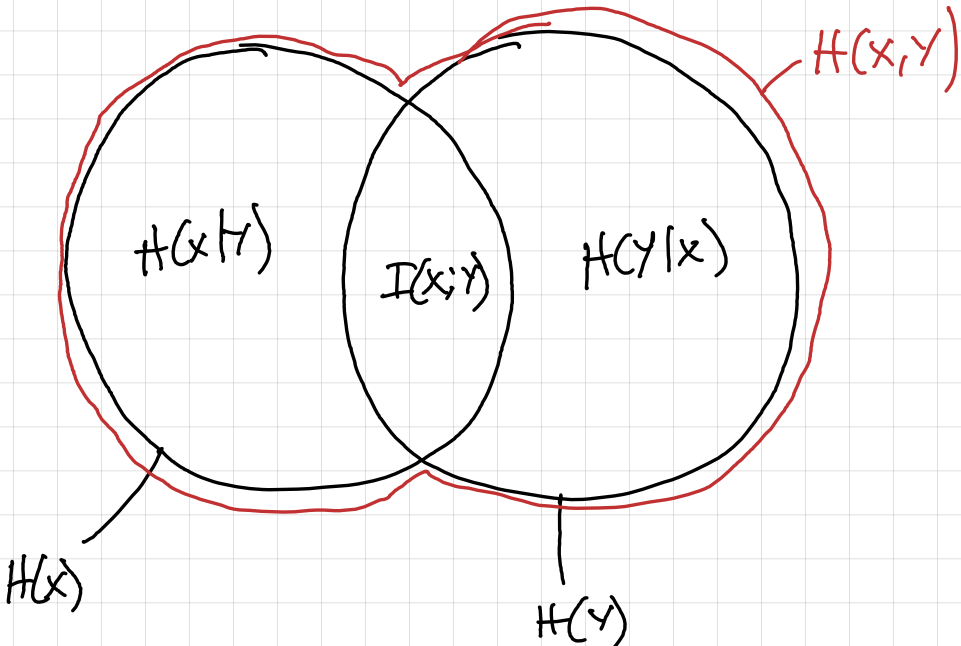




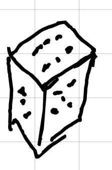
Memorise this

$$
\boxed{
\begin{aligned}
I(X;Y) &= H(X) + H(Y) - H(X,Y) \\
&= H(X) - H(X|Y) \\
&= H(Y) - H(Y|X)
\end{aligned}
}
$$

Alternative View



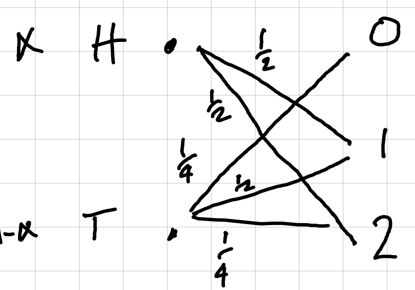
Example



Roll a die $\quad 1,2,3,4 \Rightarrow$ Flip a coin

$\qquad\qquad\quad\; 5,6 \Rightarrow$ Flip a coin twice

How much info about the die face is revealed by the no. of heads I get?



$$P(y=0) = \frac{(1-\alpha)}{4}$$

$$P(y=1) = \frac{\alpha}{2} + \frac{(1-\alpha)}{2} = \frac{1}{2}$$

THH 1/8
HHH 1/8
HTH 1/8
HHT 1/8

$$P(y=2) = \frac{\alpha}{2} + \frac{(1-\alpha)}{4} = \frac{2\alpha+1-\alpha}{4} = \frac{1+\alpha}{4}$$

$$H(Y) = -\frac{1-\alpha}{4}\log\frac{1-\alpha}{4} - \frac{1}{2}\log\frac{1}{2} - \frac{1-\alpha}{4}\log\frac{1-\alpha}{4} = .$$

$$= -\frac{1-\alpha}{4}\log\frac{1-\alpha}{4} - \frac{1}{2}\log\frac{1}{2} - \frac{1+\alpha}{4}\log\frac{1+\alpha}{4}$$

$P(y=0 \mid x=H) = 0 \qquad P(y=0 \mid x=T) = \frac{1}{4}$

$P(y=1 \mid x=H) = \frac{1}{2} \qquad P(y=1 \mid x=T) = \frac{1}{2}$

$P(y=2 \mid x=H) = \frac{1}{2} \qquad P(y=2 \mid x=T) = \frac{1}{4}$

$\frac{3}{8} + \frac{1}{2} - \frac{3}{8}\log\frac{3}{8}$

$\frac{7}{8} - \frac{3}{8}\log\frac{3}{8}$

1.344

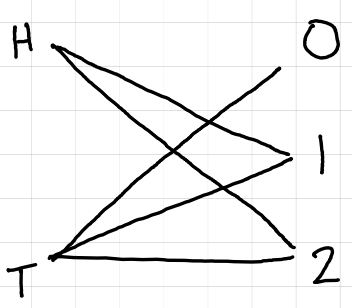
$$H(Y|X) = \alpha H\left(\tfrac{1}{2},\tfrac{1}{2}\right) + (1-\alpha)H\left(\tfrac{1}{4},\tfrac{1}{4},\tfrac{1}{2}\right)$$

$$= \alpha\left(-\log\tfrac{1}{2}\right) + (1-\alpha)\left(-\tfrac{1}{2}\log\tfrac{1}{2} - \tfrac{1}{2}\log\tfrac{1}{4}\right)$$

$$= \alpha + (1-\alpha)\left(\tfrac{1}{2}+1\right)$$

$$= \alpha + \frac{3}{2} - \frac{3\alpha}{2} = \frac{3}{2} - \frac{\alpha}{2}$$

$$I = -\frac{1-\alpha}{4}\log\frac{1-\alpha}{4} - \frac{1}{2}\log\frac{1}{2} - \frac{1+\alpha}{4}\log\frac{1+\alpha}{4} - \frac{3}{2} + \frac{\alpha}{2}$$



$P(0|H) = 0 \qquad P(0|T) = 1/4$

$P(1|H) = 1/2 \qquad P(1|T) = 1/2$

$P(2|H) = 1/2 \qquad P(2|T) = 1/4$

$$P(0) = \tfrac{1}{2}\times\tfrac{1}{4} = \tfrac{1}{8}$$

$$P(1) = \tfrac{1}{2}\times\tfrac{1}{2} + \tfrac{1}{2}\times\tfrac{1}{2} = \tfrac{1}{2}$$

$$P(2) = \tfrac{1}{2}\times\tfrac{1}{2} + \tfrac{1}{4}\times\tfrac{1}{2} = \tfrac{3}{8}$$

$$H(Y) = \tfrac{1}{8}\log 8 + \tfrac{1}{2}\log 2 + \tfrac{3}{8}\log\tfrac{8}{3}$$

$$= \tfrac{3}{8} + \tfrac{1}{2} + \tfrac{3}{8}(3 - \log 3) = 2 - \tfrac{3}{8}\log 3 = 1.40564$$

$$H(Y|X) = -\tfrac{1}{2}\left(\tfrac{1}{2}\log\tfrac{1}{2} + \tfrac{1}{2}\log\tfrac{1}{2}\right) - \tfrac{1}{2}\left(\tfrac{1}{4}\log\tfrac{1}{4} + \tfrac{1}{2}\log\tfrac{1}{2} + \tfrac{1}{4}\log\tfrac{1}{4}\right)$$

$$= +1 + \tfrac{1}{2}\left(\tfrac{1}{2} + \tfrac{1}{2} + \tfrac{1}{2}\right) = 1.25$$

$$I(X;Y) = 1.40564 - 1.25 = \underline{0.15564}$$

Noise

For our system $Y = X + \eta$

$$I(X;Y) = H(Y) - H(X+\eta \mid X)$$

$$\boxed{I(X;Y) = H(Y) - H(\eta \mid X)}$$

$$H(\eta \mid X) = \sum_{x \in A_X} P(x)\, H(\eta \mid x)$$

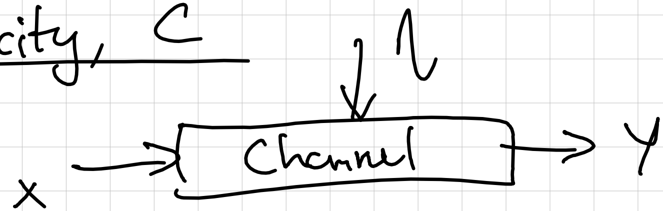
$$= P(x=0)\, H(\eta \mid x=0) + P(x=1)\, H(\eta \mid x=1) \quad \text{for binary.}$$

If channel symmetric $\Rightarrow$ $H(\eta \mid x=0) = H(\eta \mid x=1)$

$\therefore \Rightarrow H(Y \mid X) = H(\eta)$

$$\boxed{I(X;Y) = H(Y) - H(\eta)}$$ for symmetric channel.

Capacity, C



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

bits per symbol.

Binary Entropy : useful shorthand

We often have to deal with binary problems where

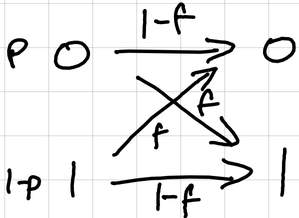
$$P(x=0) = p$$
$$P(x=1) = 1-p.$$

In such a case we define:

$$\boxed{H_2(p) = -p\log p - (1-p)\log(1-p)}$$

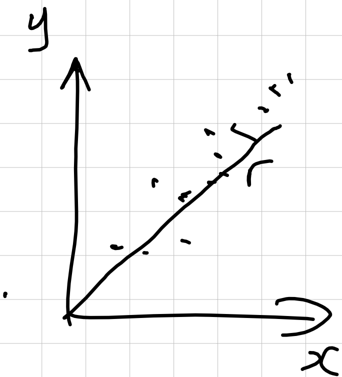
Binary Entropy function.

BSC Capacity   Eg. 8.3



Bonus: Correlation and Mutual Info

$$r = \frac{\mathrm{cov}(x,y)}{\mathrm{var}(x)\,\mathrm{var}(y)} = \left(E(x,y) - E(x)E(y)\right)\frac{1}{\sigma_x \sigma_y}$$



$\Rightarrow$ Measuring strength of linear relationship.

$y = mx + c$	$r = 1$	$I(X;Y) \neq 0$
$y = mx^2 + c$	$r = 0$	$I(X;Y) \neq 0$

Mutual Info. is a more general way to quantify the relationship.