$$N_{a,b}^{(i,j)} = M\, p_{a,b}^{(i,j)}$$

Calculate

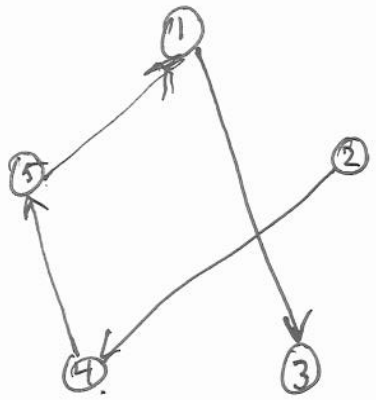
$$M^{ij} = \sum_{a,b=A}^{Z} p_{ab} \cdot \log p_{ab}^{(ij)}$$

If M^{ij} is "big"

then i follows j in rectangular transposition key

If M^{ij} is "small"

then it i doesn't follow j



41523 ← permutation to encrypt

↕ inverse of each permutation

1 2 3 4 5

24513 ← permutation to decrypt

1 is in position 4
2 is in position 1
3 is in position 5
4 is in position 2
5 is in position 3

The Entropy of An Event

Definition: The *entropy of an event* A is:

1. the measure of uncertainty we *feel* about the occurrence of A.
2. the amount of *information*, measured in bits, contained by A.

Events that occur with equal probability have the same amount of uncertainty and contain the same amount of information

$\Downarrow$

The entropy of an event should be a function of the probability of that event occurring

The entropy of event $A = h(P(A))$

What properties should the entropy function, h, have to numerically express the measure of our uncertainty about the occurrence of an event in a manner which is compatible with our intuitive notion of uncertainty?

Basic Requirements

1. The more probable the event the smaller the uncertainty

   $h(x)$ should be a decreasing function

2. The uncertainty about the simultaneous occurrence of two independent events is equal to the sum of the individual uncertainties

   $P(A \& B) = P(A) \cdot P(B)$ if A & B are independent

   $h(xy) = h(x) + h(y)$ ✓

3. Small changes in the probability should correspond to small changes in the uncertainty

   $h(x)$ should be a continuous function ✓ if $x \neq 0$

4. Recording the outcome of a 50/50 situation requires one binary register.

   $h(1/2) = 1$ (bit) ✓

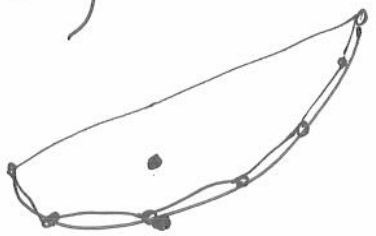
Therefore $h(x \cdot y) = \log_2(1/xy) = \log_2(1/x) + \log_2(1/y)$

$h(x) = \log_2 1/x$

$h(1/2) = \log_2(1/(1/2)) = \log_2 2 = 1$

$F(x)$ concave up $(F''(x) \geq 0)$

$$\sum_{i=1}^{n} m_i F(x_i) \geq F\left(\sum_{i=1}^{m} m_i x_i\right)$$



$\frac{1}{n}\left(\sqrt{1} + \sqrt{2} + \cdots + \sqrt{n}\right)$ is related to $\sqrt{n+1}$

$F(x) = \sqrt{x}$ is concave down

$$\frac{1}{n}\left(\sqrt{1}+\sqrt{2}+\cdots+\sqrt{n}\right) = \sum_{i=1}^{n} m_i F(x_i) \leq F\left(\sum_{i=1}^{n} m_i x_i\right) = \frac{1}{\sqrt{2}}\sqrt{n+1}$$

$m_i = 1/n \quad x_i = i$

$$\sum_{i=1}^{n} m_i F(x_i) = \frac{1}{n}\cdot\sqrt{1} + \frac{1}{n}\sqrt{2} + \cdots + \frac{1}{n}\sqrt{n}$$

$$F\left(\sum_{i=1}^{n} m_i x_i\right) = \sqrt{\frac{1}{n}\cdot 1 + \frac{1}{n}\cdot 2 + \frac{1}{n}\cdot 3 + \cdots + \frac{1}{n}\cdot n}$$

$$= \sqrt{\frac{1}{n}(1+2+3+\cdots+n)}$$

$$= \sqrt{\frac{1}{n}\,\frac{n(n+1)}{2}} = \frac{1}{\sqrt{2}}\cdot\sqrt{n+1}$$