Shannon Theory

- Birthday attacks
    1. For positive integer m, n with $m \geq n$, the number $m^{(n)}$ is defined as followed:

    $$m^{(n)} = m(m-1)(m-2)...(m-n+1)$$

    2. Let $m, n \geq 1$ with $m \geq n$. (*This is called Sterling number of the second kind*):

    $$\begin{Bmatrix} m \\ n \end{Bmatrix} = \frac{1}{n!}\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^m$$, with the exception is $\binom{0}{0} = 1$

- Example: A bowl with m balls numbered from 1 to m. Suppose that n balls are drawn from the bowl on at a time with ***replacement***, and the numbers are listed.
1. The probability that exactly t different balls have been drawn is

$$P_1(m,n,t) = \begin{Bmatrix} n \\ t \end{Bmatrix}\frac{m^t}{m^n},\ 1 \leq t \leq n$$

2. The probability of at least once coincidences (the ball being drawn twice) is:

$$P_2(m,n) = 1 - P_1(m,n,n) = 1 - \frac{m^n}{m^n},\ 1 \leq n \leq m.$$

from number theory $n = O\sqrt{m}$ and $m \to \infty$, then

$$P_2(m,n) \to 1 - \exp(-\frac{n(n-1)}{2m} + O\left(\frac{1}{\sqrt{m}}\right) \approx 1 - \exp\left(-\frac{n^2}{2m}\right)$$

as $m \to \infty$, the expected number of draws before coincident is $\sqrt{\frac{\pi m}{2}}$.

Suppose there are two bowls containing m red balls numbered 1 to m and the other containing m white balls numbered 1 to m.

1. n_1 balls are selected from the first bowl and their numbers listed.
2. n_2 balls are selected from the second bowl and their numbers listed.
3. Finally the coincidences between the two lists are counted.

- If the balls from both bowls are drawn one at a time, with replacement, then the probability of at least one coincidences is:

  $P_3(m,n_1,n_2) = 1 - \frac{1}{m^{n_1+n_2}} \sum_{t_1,t_2} m^{(t_1+t_2)} \begin{Bmatrix} n_1 \\ t_1 \end{Bmatrix} \begin{Bmatrix} n_2 \\ t_2 \end{Bmatrix}$, where $0 \le t_1 \le n_1, 0 \le t_2 \le n_2$. If $n = n_1 = n_2, n = O(\sqrt{m})$ and $m \to \infty$, then

  $$P_3(m,n_1,n_2) \to 1 - \exp\left(-\frac{n^2}{m}\left[1 + O\left(\frac{1}{\sqrt{m}}\right)\right]\right) \approx 1 - \exp\left(-\frac{n^2}{m}\right)$$

- If the balls from both bowls are drawn without replacement, the probability of at least one coincidence is:

  $P_4(m,n_1,n_2) = 1 - \frac{m^{(n_1+n_2)}}{m^{(n_1)}m^{(n_2)}}$, If $n = n_1 = n_2, n = O(\sqrt{m})$ and $m \to \infty$, then

  $$P_4(m,n_1,n_2) \to 1 - \exp\left(-\frac{n_1 n_2}{m}\left[1 + \frac{n_1+n_2-1}{2m} + O\left(\frac{1}{m}\right)\right]\right)$$

- If the n_1 white balls are drawn one at a time, with replacement, and n_2 red balls are drawn without the replacement, the probability of at least one coincidence is:

  $P_5(m,n_1,n_2) = 1 - \left(1 - \frac{n_2}{m}\right)^{n_1}$, If $n = n_1 = n_2, n = O(\sqrt{m})$ and $m \to \infty$, then

  $$P_5(m,n_1,n_2) \to 1 - \exp\left(-\frac{n_1 n_2}{m}\left[1 + O\left(\frac{1}{\sqrt{m}}\right)\right]\right) \approx 1 - \exp\left(-\frac{n_1 n_2}{m}\right)$$

Entropy

Definition: The *entropy* or *uncertainty* of X is defined to be
$H(X) = -\sum_{i=1}^{n} p_i \log p_i = \sum_{i=1}^{n} p_i \log\left(\frac{1}{p_i}\right)$, where $p_i \cdot \log p_i = p_i \cdot \log\left(\frac{1}{p^i}\right) = 0$ if $p_i = 0$

X is a random variable which takes on a finite set values $x_1, x_2, x_3 ... x_n$, with probability $P(X = x_i) = p_i$, where $0 \le p_i \le 1$ for each i, $1 \le i \le n$, and where $\sum_{i=1}^{n} p_i = 1$. Also, let Y and Z be random variables, which take on finite sets of values. (…in English… entropy is a *mathematical* measure of the amount of information provide by an observation of X. A useful entity for approximating the average number of bits require to encode the element of X.)

Properties of Entropy:

a) $0 \le H(X) \le \log n$
b) $H(X) = 0$ iff $p_i = 1$ for some i, and $p_j = 0$ for all $j \ne i$ (no uncertainty in the outcome).
c) $H(X) = \log n$ iff $p_i = 1/n$ for each i, $i \le i \le n$ (all outcome are equally likely)

Joint entropy:

$$H(X,Y) = -\sum_{x,y} P(X = x, Y = y) \log(P(X = x, Y = y))$$

If X and Y are random variables, then $H(X,Y) \le H(X) + H(Y)$,
$H(X,Y) = H(X) + H(Y)$ iff X and Y are independent.

If X and Y are random variables, the *conditional properties of* X given $Y = y$ is

$$H(X \mid Y) = \sum_{y} P(Y = y) H(X \mid Y = y)$$

Some *properties of conditional entropy*: Let X and Y be random variables.

a) The quantity $H(X\,|Y)$ measures the amount of uncertainty remaining about X after Y has been observed.
b) $H(X\,|Y)\geq 0$ and $H(X\,|\,X)=0$
c) $H(X\,|Y)=H(X)+H(Y\,|\,X)=H(Y)+H(X\,|Y)$
d) $H(X\,|Y)\leq H(X)$, with equality iff X and Y are equal.

Mutual Information (*transinformation*) between random variable X and Y is:

$I(X;Y)=H(X)-H(X\,|Y)$, similarly the, the transinformation ox X and the pair Y,Z is defined to be: $I(X;Y,Z)=H(X)-H(X\,|Y,Z)$.

Properties:

a) The quantity $I(X;Y)$ is the amount of information that Y reveals about X. Similarly, $I(X;Y,Z)$ is the information that Y and Z together reveals about X.
b) $I(X;Y)\geq 0$
c) $I(X;Y)=0$ iff X and Y are independent. Y contributes no information about X.
d) $I(X;Y)=I(Y;X)$

The *conditional transinformation* of the pair X,Y given Z is defined to be:

$I_Z(X:Y)=H(X\,|\,Z)-H(X\,|Y,Z)$, having the following properties

a) $I_Z(X;Y)$ is the amount of information that Y provides about X, given that Z has already been observed.
b) $I(X:Y,Z)=I(X:Y)+I_Y(X;Z)$
c) $I_Z(X;Y)=I_Z(Y;X)$

References

Apache-SSL: http://www.apache-ssl.org/
You will need the following package as well:

http://www.openssl.org/ (version 0.9.4 or better)
ftp://ftp.psy.uq.oz.au/pub/Crypto/SSL/ (SSLeay Source version 0.5.1b+ or better).

You will need to do a lot of work to get this package working properly.

Modssl: If you are using RedHat, the RPM can be download here:
http://www.modssl.org/contrib/

This will take you 5 minutes to install.

Documentations:
Apache 1.3 Documentation: http://cold.litech.com/manual/index.html
mod-SSL Documentation: http://cold.litech.com/manual/mod/mod_ssl/

A working installation of mod-ssl – http://cold.litech.com