SHANNON'S THEOREM AND THE BINOMIAL RANDOM VARIABLE

Martin Erickson

Northeast Missouri State University

Claude E. Shannon's 1948 theorem on coding over a noisy channel states that information can be transmitted with arbitrarily high accuracy at any rate below the channel capacity. Channel and capacity are defined in the references below. The proof requires a combinatorial or probabilistic lemma about binomial coefficients $C(n, j)$.

Lemma. If $0 < x < \frac{1}{2}$ and

$$H(x) = -x \log x - (1-x) \log(1-x),$$

then

$$\sum_{j=0}^{[nx]} C(n, j) < 2^{nH(x)}.$$

The logarithms are base two and the quantity $H(x)$ is the entropy of the channel, measured in bits. All previously published proofs of the lemma use subtle approximation methods (often Stirling's approximation to the factorial function). The following new proof presumes only the binomial theorem.

Proof. With $x + y = 1$ the binomial theorem and two simple inequalities yield

$$1 = \sum_{j=0}^{n} C(n, j) x^j y^{n-j} > \sum_{j=0}^{[nx]} C(n, j) x^j y^{n-j}$$

$$> \sum_{j=0}^{[nx]} C(n, j) x^j y^{n-j} (x/y)^{nx-j} = \sum_{j=0}^{[nx]} C(n, j) x^{nx} y^{ny}.$$

Hence

$$\sum_{j=0}^{[nx]} C(n,j) < x^{-nx} y^{-ny} = 2^{nH(x)}.$$

For an application of the lemma to probability theory, let Y be the binomial random variable with distribution $B(n, \frac{1}{2})$. Multiplying the inequality of the lemma by 2^{-n} yields an upper bound for the area under the left tail of the distribution curve of Y.

$$P(0 \leq Y \leq nx) = \sum_{j=0}^{[nx]} C(n,j) 2^{-n} < 2^{n(H(x)-1)}.$$

Since $H(x) - 1$ is negative (elementary calculus), $P(0 \leq Y \leq nx)$ decreases exponentially with n. For example, when n fair coins are tossed the expected number of heads is $n/2$. The probability P that at most 10% are heads is estimated by computing

$$2^{H(.10)-1} \doteq .6921\ .$$

Therefore $P < (.6922)^n$.

References

1. R. W. Hamming, *Coding and Information Theory,* (second edition), Prentice-Hall, Englewood Cliffs, NJ, 1986.

2. F. Ingels, *Information and Coding Theory,* International Textbook Company, San Francisco, 1971.

3. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977.

4. R. J. McEliece, *The Theory of Information and Coding,* Addison-Wesley, Reading, 1977.