Guessing and Entropy

James L. Massey
Signal & Info. Proc. Lab., Swiss Federal Inst. Tech, CH-8092 Zurich, Switzerland

Abstract — **It is shown that the average number of successive guesses, $E[G]$, required with an optimum strategy until one correctly guesses the value of a discrete random X, is underbounded by the entropy $H(X)$ in the manner $E[G] \geq (1/4)2^{H(X)}+1$ provided that $H(X) \geq 2$ bits. This bound is tight within a factor of $(4/e)$ when X is geometrically distributed. It is further shown that $E[G]$ may be arbitrarily large when $H(X)$ is an arbitrarily small positive number so that there is no interesting upper bound on $E[G]$ in terms of $H(X)$.**

I. Introduction

Consider the problem of guessing the value taken on by a discrete random variable X in one trial of a random experiment by asking questions of the form "Did X take on its i-th possible value?" until the answer is "Yes!". This problem arises for instance when a cryptanalyst must try out possible secret keys one at a time after narrowing the possibilities by some cryptanalysis. Let G be the number of guesses used in the guessing strategy that minimizes $E[G]$, which is obviously to guess the possible values of X in order of decreasing probability. With no loss of essential generality, we may suppose that these are the first, second, third, etc., possible values of X so that the probability distribution for X, say $\mathbf{p} = (p_1, p_2, p_3, \ldots)$ satisfies $p_1 \geq p_2 \geq p_3 \geq \ldots$ and we will call such a $\mathbf{p}$ a *monotone* distribution. With this convention, $E[G] = \sum i \cdot p_i$, where in this and in all later sums the summation is on i from 1 to infinity. The purpose of this paper is to answer the question of whether the entropy $H(X)$ determines interesting upper or lower bounds on $E[G]$.

II. A Lower Bound on $E[G]$

For any $A > 1$, the set of (not necessarily montone) probability distributions $\mathbf{p}$ such that $\sum i \cdot p_i = A$ is a convex set and the entropy $h(\mathbf{p}) = -\sum p_i \cdot log(p_i)$ is a concave function on this set. (Here and hereafter, all logarithms are to the base 2.) A standard calculus of variations argument [which is precisely the argument used by Jaynes [1] to show that the Boltzmann (or geometric) distribution maximizes entropy for an average quantum-level energy] shows that the entropy is maximized uniquely by the geometric distribution

$$p_i = (1/(A-1))(1-1/A)^i$$

. Because the geometric distribution is monotone, it is *a fortiori* the unique monotone distribution maximizing $H(X)$ and its entropy is readily calculated to be

$$h(\mathbf{p}_{geom}) = log(A-1) + log(1-1/A)^{-A}.$$

Because the second term on the right decreases monotonically to $log(e)$ with increasing A and equals 2 when $h(\mathbf{p}_{geom}) = 2$ bits, it follows that

$$h(\mathbf{p}_{geom}) \leq log(A-1) + 2$$

when

$$h(\mathbf{p}_{geom}) \geq 2.$$

It follows, for an arbitrary monotone distribution with mean A and entropy $h(\mathbf{p}) \geq 2$ bits, that $h(\mathbf{p}) \leq log(A-1)+2$ or, equivalently, that

$$A \geq (1/4)2^{H(X)} + 1.$$

Because the second term on the right in our expression for $h(\mathbf{p}_{geom})$ is at least $log(e)$, it follows that

$$h(\mathbf{p}_{geom}) \geq log(A-1) + log(e)$$

or, equivalently, that

$$A \leq (1/e)2^{h(\mathbf{p}_{geom})} + 1,$$

which shows that our lower bound on A in terms of $H(X)$ is conservative by at most a factor of $4/e$ when X is geometrically distributed.

III. Lack of an Entropic Upper Bound on $E[G]$

For every $A > 1$ and every integer $L > 2A-1$, the distribution $\mathbf{p}$ with $p_1 = (L-2(A-1))/L$, $p_i = 2(A-1)/(L^2-L)$, and $p_i = 0$ for $i > L$ is monotone with mean A. The entropy of this distribution is

$$h(\mathbf{p}) = h_{bin}(2(A-1)/L) + (2(A-1)/L)log(L-1)$$

where $h_{bin}(.)$ is the binary entropy function. Because $h(\mathbf{p})$ tends to zero as L tends to infinity, it follows that A cannot be overbounded in a nontrivial way in terms of $h(\mathbf{p})$ alone.

IV. Remark

A concise statement of what has been proved is contained in the abstract above.

References

[1] E. T. Jaynes, "Information Theory and Statistical Mechanics," *Physical Review*, vol. 106, no. 4, pp. 620-630, May 15, 1957.

0 - 7803-2015-8/94/$4.00