Sum of Two Independent Random Variables

September 16, 2012

Bounds on entropy of sum

Suppose we have two independent random variables X and Y. Their sum is $Z = X + Y$. When X and Y are independent, we can prove the following bounds

$$\max\{H(X), H(Y)\} \leq H(Z) \leq H(X) + H(Y).$$

Proof. (i) First prove $H(Z|X) = H(Y|X)$:

$$\begin{aligned} H(Z|X) &= -\sum_x p(X=x) \sum_z p(Z=z|X=x) \log p(Z=z|X=x) \\ &= -\sum_x p(X=x) \sum_z p(Y=z-x|X=x) \log p(Y=z-x|X=x) \\ &= -\sum_x p(X=x) \sum_{y'} p(Y=y'|X=x) \log p(Y=y'|X=x) \\ &= H(Y|X). \end{aligned}$$

After observing X, the remaining uncertainty in Z is due to Y. Since we also know X and Y are independent, so $H(Y|X) = H(Y)$. Combining with "conditioning reduces entropy":

$$H(Z) \geq H(Z|X) = H(Y|X) = H(Y).$$

(ii) By symmetry, we can also prove

$$H(Z) \geq H(Z|Y) = H(X|Y) = H(X).$$

So we have shown the left-hand-side of the inequality:

$$\max\{H(X), H(Y)\} \leq H(Z).$$

(iii) Because Z is a function of X and Y, $Z = g(X, Y) = X+Y$, using the fact we have shown that entropy of a function of random variable is smaller than the random variable (treat (X, Y) as a random vector), we have

$$H(Z) \leq H(X, Y) = H(X) + H(Y).$$

The last equality is because X and Y are independent: $H(X, Y) = H(X) + H(Y|X) = H(X) + H(Y)$.

□

The upper bound and lower bound in general do not meet, unless $H(X) = 0$ or $H(Y) = 0$. For example, when X or Y only takes one value.

Next we will show that $H(Z) = H(X) + H(Y)$ if the vector (X, Y) is a function of Z, and X and Y are independent.

Proof. Since $Z = g(X, Y)$, we know that

$$H(Z) = H(g(X, Y)) \leq H(X, Y).$$

If (X, Y) is also a function of Z as well: $X = f(Z)$ and $Y = h(Z)$, then we have

$$H(X, Y) = H(f(Z), h(Z)) \leq H(Z).$$

□

We will show that we need both independence and the fact that (X, Y) is a function of Z.

Example 1 Given two independent random variables X and Y, with pdfs as

$$p(X) = \begin{cases} 1/2 & X = 0; \\ 1/2 & X = 1. \end{cases}$$

and

$$p(Y) = \begin{cases} 1/2 & Y = 0; \\ 1/2 & Y = 1. \end{cases}$$

Hence $H(X) = H(Y) = 1$. One can derive that the pdf of $Z = X + Y$ is given by

$$p(Z) = \begin{cases} 1/4 & Z = 0; \\ 1/2 & Z = 1; \\ 1/4 & Z = 2. \end{cases}$$

Hence $H(Z) = 3/2$, which satisfies the inequality:

$$1 = \max\{H(X), H(Y)\} < H(Z) < H(X) + H(Y) = 2.$$

Note that although X and Y are independent, the entropy of their sum is not equal to the sum of their entropy, because we cannot recover X or Y from Z.

Example 2 Given a random variables X with pdf

$$p(X) = \begin{cases} 1/2 & X = 0; \\ 1/2 & X = 1. \end{cases}$$

Let $Y = X$. So Y is completely dependent of X, and $Z = 2X$. So we can recover X and Y from Z. However, $H(Z) = H(2X) = 1$, which is less than $H(X) + H(Y) = 2H(X) = 2$. So when X and Y are dependent, even if X and Y can be recovered from Z, $H(Z) < H(X) + H(Y)$.

Example 3 Again consider the earlier example. Given two independent random variables X and Y, but this time with disjoint support and their pdfs are

$$p(X) = \begin{cases} 1/2 & X = 0; \\ 1/2 & X = 1. \end{cases}$$

and

$$p(Y) = \begin{cases} 1/2 & Y = 2; \\ 1/2 & Y = 4. \end{cases}$$

Hence $H(X) = H(Y) = 1$. One can derive that the pdf of $Z = X + Y$ is given by

$$p(Z) = \begin{cases} 1/4 & Z = 2; \\ 1/4 & Z = 3; \\ 1/4 & Z = 4; \\ 1/4 & Z = 5; \end{cases}$$

Hence $H(Z) = 2$, which satisfies the inequality:

$$1 = \max\{H(X), H(Y)\} \leq H(Z) = H(X) + H(Y) = 2.$$

Note that we can recover X and Y from Z as

$$X = \begin{cases} 0, & Z = 2 \text{ or } 4; \\ 1, & Z = 3 \text{ or } 5. \end{cases}$$

$$Y = \begin{cases} 2, & Z = 2 \text{ or } 3; \\ 4, & Z = 4 \text{ or } 5. \end{cases}$$