EE606: Lecture 5

Supplemental Material

Oct. 19, 2004

As an example and preview of the *Shannon's Channel Coding Theorem*, we shall consider the binary symmetric channel as illustrated in the figure. Next time, we will give rigorous

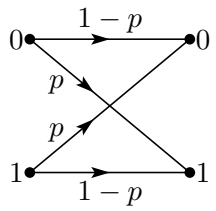


Figure 1: Binary symmetric channel with crossover probability p.

and general proofs. Suppose that $p = 0.1$. How can we improve the reliability of the system. We could send each bit three times (repetition code), and use majority rule to decode. The probability of incorrect decoding is then $p^3 + 3p^2(1-p) = 0.028$. The gain is made at the expense of the information transmission rate, which has been reduced three times. If we send each bit five times, we can further reduce the probability of incorrect decoding to 0.00856.

As the length of a repetition code increases, the the probability of incorrect decoding approaches 0, but so does the transmission rate. Shannon showed that there are codes with the rate of transmission approaching a positive constant (dependent on p) with probability of incorrect transmission approaching 0, as the length of the code increases.

If binary strings of length k are mapped into binary strings of length n for transmission, we say that the rate of the code is

$$R = \frac{k}{n}.$$

Such code consists of a choice of $2^k = 2^{nR}$ strings among the 2^n possible strings of n bits. For any input string of length n bits, errors will typically cause about np of the bits to flip. Therefore, an n bit input string typically diffuses to one of about $2^{nH(p)}$ output strings within a Hamming distance of np apart of the input string. To decode reliably, we will want to choose our input strings (codewords) so that the error spheres of two different codewords are unlikely to overlap. To avoid overlaps, the total number of strings contained in all nR error spheres must not exceed the total number 2^n possible strings:

$$2^{nH(p)} \cdot 2^{nR} \leq 2^n,$$

giving

$$R \leq 1 - H(p).$$

If transmission is highly reliable, we cannot expect the rate of the code to exceed $1 - H(p)$, but is the rate $R \leq 1 - H(p)$ actually attainable (asymptotically)? Shannon's idea: Choose the 2^{nR} codewords uniformly at random out of the 2^n possible strings of length n. Find the average probability of incorrect decoding over all such choices.

Thheorem 1 *Let $p < 0.5$ be fixed. For $\epsilon > 0$ arbitrarily small, there exists a coding scheme with rate of transmission greater than $1 - H(p) - \epsilon$ and probability of incorrect transmission less than ϵ.*

Suppose that 2^{nR} codewords are chosen at random by sampling the ensemble $\{0,1\}^n$, and one of the codewords is sent. To decode the received message, we look at $2^{n(H(p)+\epsilon)}$ words at the Hamming distance $n(H(p)+\epsilon)$ from the received string. To decode correctly, there should be a unique codeword among those words. If no such codeword exists or the codeword is not unique, there will be a decoding error. How likely is a decoding error? We have chosen the decoding sphere large enough so that failure of a valid codeword to appear in the sphere is atypical so we need only worry about its uniqueness. Since there are altogether 2^n possible strings, the Hamming sphere around the received message contains a fraction

$$\frac{2^{n(H(p)+\epsilon)}}{2^n} = 2^{-n(1-H(p)-\epsilon)}$$

of all strings. Thus the probability that one of the 2^{nR} randomly chosen codewords lands in this sphere is

$$2^{-n(1-H(p)-R-\epsilon)},$$

which goes to zero exponentially fast as long as $R < 1 - H(p) - \epsilon$. Note that ϵ can be chosen to be arbitrarily small, and thus R can be chosen to be arbitrarily close to $1 - H(p)$.