University of Illinois **Spring 2011**

ECE 361: Lecture 11: Rate-Efficient Communication – Part II

In Lecture 10, we considered coded communication systems using codes of block length n and rate R and found that the error probability $P(E)$ of any specific coded communication system is given by a complicated formula that is difficult to evaluate. We found an upper bound (10.6) on $P(E)$ but even this is not easy to evaluate. In this Lecture, we will consider the *average value* of $P(E)$ for the codes in very large collections of codes (called *ensembles* of codes) of block length n and rate R. Here, average means averaged over all codes in the ensemble: we add up the values of $P(E)$ for all the codes in the ensemble and divide by the number of codes in the ensemble. Equivalently, if we think of an experiment in which we pick a code at random (with equal probability) from the ensemble, and think of its error probability $P(E)$ as a random variable (since the value of $P(E)$ depends on the outcome of the experiment, *viz.*, the code we picked), then the *expected value* of $P(E)$ is what we are considering. Let $\overline{P(E)}$ denote the average error probability of the codes in the ensemble. We can similarly compute the upper bound (10.6) for each code in the ensemble and find the average upper bound over all codes in the ensemble. We will develop an argument that the *average value* of the upper bound (10.6) on $P(E)$ is smaller than $2^{n(R-R^*)}$ where R^* is a number whose value is given in (11.6) below. Since $P(E)$ for each code is smaller than the corresponding upper bound (10.6) on $P(E)$ for that code, $\overline{P(E)}$ must be smaller than the average value of the upper bound (10.6), and thus we have that

$$\overline{P(E)} < 2^{n(R-R^*)} \tag{11.1}$$

If $R < R^*$, the right side of (11.1) is smaller than 1, and indeed can be made as small as we like by choosing the ensemble to have suitably large block length n. Thus, for *at least one* code in an ensemble of codes of block length n and rate $R < R^*$, the error probability $P(E)$ is no larger than $2^{n(R-R^*)} < 1$. In fact, since the ensemble includes some demonstrably poor codes that no one would ever consider using because they have very high error probabilities, it is reasonable to believe that not just one but *many* codes in the ensemble will have $P(E)$ smaller than $2^{n(R-R^*)}$. Thus, unlike M-ary orthogonal signaling schemes which are energy-efficient but not rate-efficient, general coded communication systems with rates $R < R^*$ can be both energy-efficient and rate-efficient, transmitting data at nonzero rates with arbitrarily small error probabilities with a fixed amount of energy per data bit.

11.1. Code Ensembles

11.1.1. The Ensemble of All Binary Codes

In Lecture 10, we developed the notion of an (n, k) code of rate $R = k/n$ as a set $\mathcal{C} = \{\mathbf{x}^{(0)}, \mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(2^k-1)}\}$ of 2^k binary vectors of length n with which $\mathbf{x}^{(i)} = [x_1^{(i)}, x_2^{(i)}, \ldots, x_n^{(i)}]$ is used to transmit the k-bit representation of the integer i, $0 \le i \le 2^k - 1$. Since we will need to talk of the i-th codeword in different codes, let us change notation slightly and denote the i-th codeword of $\mathcal{C}$ by $\mathbf{x}^{(i)}(\mathcal{C})$. We placed no restrictions on which of the 2^n binary vectors of length n is chosen for the i-th codeword in a code; indeed, the same choice could be made for i-th and the j-th codeword if we so desired. Thus, since there are 2^n choices for each codeword, and $2^k = 2^{nR}$ different codewords, there are a total of $(2^n)^{2^{nR}} = 2^{2^{nR}n}$ different binary codes $\mathcal{C}$ of block length n and rate R. We denote this *ensemble of all binary* (n, nR) *codes* by $\mathfrak{C}$. Thus, $|\mathfrak{C}| = 2^{2^{nR}n}$. This enormously large ensemble contains some notably bad codes — for example, the 2^n different codes with the property that $\mathbf{x}^{(0)}(\mathcal{C}) = \mathbf{x}^{(1)}(\mathcal{C}) = \ldots = \mathbf{x}^{(2^k-1)}(\mathcal{C})$ have error probability $1 - 2^{-k} \approx 1$ — but nonetheless, $\overline{P(E)}$ for this ensemble satisfies (11.1). The key property needed to prove that $\overline{P(E)} < 2^{n(R-R^*)}$ is as follows.

Let i and j, $0 \le i, j \le 2^k - 1$, be two distinct integers, and suppose that binary n-bit vectors $\mathbf{x}^{(i)}$ and $\mathbf{x}^{(j)}$ each are equally likely to be any of the 2^n n-bit binary vectors. Now, $d_H(\mathbf{x}^{(i)}, \mathbf{x}^{(j)})$, the Hamming distance between $\mathbf{x}^{(i)}$ and $\mathbf{x}^{(j)}$, equals the *Hamming weight* of their bit-by-bit Exclusive-OR sum $\mathbf{z} = \mathbf{x}^{(i)} \oplus \mathbf{x}^{(j)}$, where the Hamming weight of a vector is the number of 1s in the vector. A little thought shows that $\mathbf{z}$ is also equally likely to be any of the 2^n n-bit binary vectors, that is, as $(\mathbf{x}^{(i)}, \mathbf{x}^{(j)})$ ranges over the $2^n \times 2^n$

possible values, each of the 2^n binary n-bit vectors occurs 2^n times as the sum $\mathbf{z}$. Since $\binom{n}{\ell}$ binary vectors of length n have Hamming weight ℓ, we have that

$$P\{d_H(\mathbf{x}^{(i)}, \mathbf{x}^{(j)}) = \ell\} = \binom{n}{\ell}\frac{1}{2^n}, \quad 0 \le \ell \le n, \tag{11.2}$$

that is, $d_H(\mathbf{x}^{(i)}, \mathbf{x}^{(j)})$ is a *binomial* random variable with parameters $\left(n, \frac{1}{2}\right)$. Another way of thinking about this result is that $\binom{n}{\ell}\frac{1}{2^n}|\mathfrak{C}| = \binom{n}{\ell}\frac{1}{2^n}2^{2^{nR}n}$ of the $|\mathfrak{C}| = 2^{2^{nR}n}$ codes in $\mathfrak{C}$ enjoy the property that $d_H(\mathbf{x}^{(i)}(\mathcal{C}), \mathbf{x}^{(j)}(\mathcal{C})) = \ell$, $0 \le \ell \le n$.

The set $\mathfrak{C}$ of all binary codes is very large, and most of the codes in the collection cannot be decoded easily. A much smaller subset of $\mathfrak{C}$ also enjoys the property (11.2), and contains many codes that can be decoded relatively easily. This set is $\mathfrak{C}_L$, the set of all *linear codes* which concept we discuss next,

11.1.2. The Ensemble of All Linear Binary Codes

A *linear* binary code of block length n and rate R is a set $\mathcal{C}$ of $2^k = 2^{nR}$ n-bit binary vectors with the property that if $\mathbf{x}$ and $\mathbf{y}$ are codewords in $\mathcal{C}$, then their sum $\mathbf{x} \oplus \mathbf{y}$ is also a codeword in $\mathcal{C}$. As in Lecture 10, let the k data bits to be transmitted comprise a k-bit vector $\mathbf{u}$. There are 2^k such vectors and we denote them individually as $\mathbf{u}^{(0)}$, $\mathbf{u}^{(1)}$, $\ldots$, $\mathbf{u}^{(2^k-1)}$ where $\mathbf{u}^{(i)}$ is the k-bit binary representation of the integer i, $0 \le i \le 2^k - 1$. Then, a linear code encodes the data vector $\mathbf{u}$ into a n-bit vector $\mathbf{x} = \mathbf{u}G$ where G is a $k \times n = nR \times n$ matrix of 0's and 1's called the *generator matrix* of the code. Note that the additions involved in the vector-matrix multiplication are all Exclusive-OR additions. Thus, the 2^k codewords $\mathbf{x}^{(0)}, \mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(2^k-1)}$ comprising the code $\mathcal{C}$ are $\mathbf{x}^{(i)} = \mathbf{u}^{(i)}G$, $0 \le i \le 2^k - 1$.

There are many properties of linear binary codes that are easy to verify. We simply list them without proof.

- The mapping $\mathbf{u}^{(i)} \to \mathbf{x}^{(i)}$ is a *linear transformation*: $\mathbf{u}^{(i)} \oplus \mathbf{u}^{(j)} \to \mathbf{x}^{(i)} \oplus \mathbf{x}^{(j)}$.
- Each row of the generator matrix G is a codeword in $\mathcal{C}$. In fact, if $\mathbf{g}_i$, $1 \le i \le k$ denotes the i-th row of G, then $\mathbf{g}_i = \mathbf{x}^{(2^{i-1})}$.
- **Either** *all* the codewords have a 0 in a given coordinate, **or** 2^{k-1} codewords have a 0 in that coordinate and the other 2^{k-1} codewords have a 1 in that coordinate.
- **Either** *all* the codewords in $\mathcal{C}$ have *even* Hamming weight **or** 2^{k-1} codewords have even Hamming weight and the other 2^{k-1} codewords have odd Hamming weight.
- $\mathcal{C}$ is a vector subspace of the n-dimensional vector space of all binary n-tuples. Note that the *field of scalars* for this vector space is the *finite field* $\{0, 1\}$ of two elements in which addition is the Exclusive-OR operation and multiplication is the AND operation (or ordinary integer multiplication if you prefer).
- $|\mathcal{C}| = 2^k$, that is, $\mathcal{C}$ is a k-dimensional subspace, if and only if G has *row rank* k. Otherwise, $\mathcal{C}$ is a *multiset* in which each element of some i-dimensional subspace occurs 2^{k-i} times, that is, 2^{k-i} data vectors get mapped onto the same codeword.

The set $\mathfrak{C}_L$ of all linear binary codes contains $2^{kn} = 2^{n^2R}$ codes corresponding to the 2^{kn} possible generator matrices G. Note that $\mathfrak{C}_L \subset \mathfrak{C}$ and $|\mathfrak{C}_L| \ll |\mathfrak{C}|$. There is no restriction placed on the rows of G. Each row can be any of the 2^n binary vectors, and there is no requirement that the rows of G be distinct. But, unless the row rank of G is k, the code will have large error probability. Nonetheless, just as with $\mathfrak{C}$, the ensemble $\mathfrak{C}_L$ has the property that $\overline{P(E)}$ for the ensemble satisfies (11.1) and this follows from the fact that (11.2) holds for $\mathfrak{C}_L$. The proof of (11.2) is similar to that presented in the previous subsection, but is more complicated because it is necessary to account for the fact that every linear code contains the all-zeroes codeword $\mathbf{0}$. The details will not be presented here and the reader is asked to accept on faith that over the ensemble $\mathfrak{C}_L$, $d_H(\mathbf{x}^{(i)}, \mathbf{x}^{(j)})$ is a *binomial* random variable with parameters $\left(n, \frac{1}{2}\right)$ with the pmf shown in (11.2). As before, an equivalent statement is that $\binom{n}{\ell}\frac{1}{2^n}|\mathfrak{C}_L|$ codes of the 2^{n^2R} codes in $\mathfrak{C}_L$ have the property that $d_H(\mathbf{x}^{(i)}(\mathcal{C}), \mathbf{x}^{(j)}(\mathcal{C})) = \ell$, $0 \le \ell \le n$.

11.2. Average Error Probability of a Code Ensemble

In Lecture 10, we derived the following upper bound on the error probability $P(E;\mathcal{C})$ for a given code $\mathcal{C}$:

$$P(E;\mathcal{C}) < \frac{1}{2^k}\sum_{i=0}^{2^k-1}\sum_{j=0,j\neq i}^{2^k-1} Q\left(\frac{\sqrt{d_H(\mathbf{x}^{(j)}(\mathcal{C}),\mathbf{x}^{(i)}(\mathcal{C}))\mathcal{E}}}{\sigma}\right). \tag{11.3}$$

where $\mathbf{x}^{(i)}(\mathcal{C})$ and $\mathbf{x}^{(j)}(\mathcal{C})$ denote the i-th and j-th codewords in $\mathcal{C}$. Now, the Chernoff bound gives us that $Q(x) < \exp(-x^2/2)$ for $x > 0$, and thus (11.3) can be loosened and simplified to

$$P(E;\mathcal{C}) < \frac{1}{2^k}\sum_{i=0}^{2^k-1}\sum_{j=0,j\neq i}^{2^k-1} \exp(-d_H(\mathbf{x}^{(j)}(\mathcal{C}),\mathbf{x}^{(i)}(\mathcal{C}))\mathcal{E}/2\sigma^2). \tag{11.4}$$

Let $\mathfrak{D}$ be any ensemble of codes for which (11.2) holds (e.g. $\mathfrak{C}$ or $\mathfrak{C}_L$). Then, the average error probability for the codes in the ensemble is

$$\begin{aligned}
\overline{P(E)} &= \frac{1}{|\mathfrak{D}|}\sum_{\mathcal{C}\in\mathfrak{D}} P(E;\mathcal{C}) \\
&< \frac{1}{|\mathfrak{D}|}\sum_{\mathcal{C}\in\mathfrak{D}}\frac{1}{2^k}\sum_{i=0}^{2^k-1}\sum_{j=0,j\neq i}^{2^k-1} \exp(-d_H(\mathbf{x}^{(j)}(\mathcal{C}),\mathbf{x}^{(i)}(\mathcal{C}))\mathcal{E}/2\sigma^2) \\
&= \frac{1}{2^k}\sum_{i=0}^{2^k-1}\sum_{j=0,j\neq i}^{2^k-1}\frac{1}{|\mathfrak{D}|}\sum_{\mathcal{C}\in\mathfrak{D}} \exp(-d_H(\mathbf{x}^{(j)}(\mathcal{C}),\mathbf{x}^{(i)}(\mathcal{C}))\mathcal{E}/2\sigma^2)
\end{aligned}$$

But in the innermost sum, $d_H(\mathbf{x}^{(j)}(\mathcal{C}),\mathbf{x}^{(i)}(\mathcal{C})) = \ell$ for $\binom{n}{\ell}\frac{1}{2^n}|\mathfrak{D}|$ codes, $0 \le \ell \le n$, and thus

$$\begin{aligned}
\overline{P(E)} &< \frac{1}{2^k}\sum_{i=0}^{2^k-1}\sum_{j=0,j\neq i}^{2^k-1}\frac{1}{|\mathfrak{D}|}\sum_{\mathcal{C}\in\mathfrak{D}} \exp(-d_H(\mathbf{x}^{(j)}(\mathcal{C}),\mathbf{x}^{(i)}(\mathcal{C}))\mathcal{E}/2\sigma^2) \\
&= \frac{1}{2^k}\sum_{i=0}^{2^k-1}\sum_{j=0,j\neq i}^{2^k-1}\sum_{\ell=0}^{n}\binom{n}{\ell}\frac{1}{2^n}\exp(-\ell\mathcal{E}/2\sigma^2) \\
&= \frac{1}{2^k}\sum_{i=0}^{2^k-1}\sum_{j=0,j\neq i}^{2^k-1}\left(\frac{1+\exp(-\mathcal{E}/2\sigma^2)}{2}\right)^n
\end{aligned}$$

from which we get that

$$\overline{P(E)} < 2^k\left(\frac{1+\exp(-\mathcal{E}/2\sigma^2)}{2}\right)^n \tag{11.5}$$

for any ensemble of codes for which (11.2) holds. Recall that $2^k = 2^{nR}$ and define the parameter R^* as

$$R^* = \log_2\left(\frac{2}{1+\exp(-\mathcal{E}/2\sigma^2)}\right) = 1 - \log_2(1+\exp(-\mathcal{E}/2\sigma^2)). \tag{11.6}$$

Then, (11.5) can be expressed as

$$\overline{P(E)} < 2^{n(R-R^*)} \tag{11.7}$$

which is just (11.1). If $R > R^*$, the right side of (11.7) exceeds 1 and the bound is useless. On the other hand, when $R < R^*$, the exponent on the right side of (11.7) is negative, and the bound is smaller than 1. More interestingly, the right side of (11.7) can be made as small as we desire by choosing a suitably large value of n. How large n must be is determined by how close the rate R is to R^*. If we wish to push the envelope and operate at rate R close to R^*, n must be larger than if we were more easy-going and chose to operate at rate R that is not so close to R^*. In any case, the probability of error, averaged over all codes in an ensemble such as $\mathfrak{C}$ or $\mathfrak{C}_L$, is small provided that $R < R^*$ and n is suitably large, and therefore there must be at least one code in the ensemble whose error probability is no larger than $\overline{P(E)}$, and thus no larger that $2^{n(R-R^*)}$.

11.3. Channel Capacity

Define the signal-to-noise ratio SNR of the discrete-time Gaussian channel with peak energy constraint $\mathcal{E}$ per channel use as $\mathsf{SNR} = \mathcal{E}/\sigma^2$. Notice that since the signal amplitudes used are $\pm\sqrt{\mathcal{E}}$ and thus matched filtering would give $\sigma^2 = N_0/2$, this definition of SNR is actually the quantity $(\mathsf{SNR}^*)^2 = 2\mathcal{E}/N_0$ that we used in Lectures 3 and 4 where we were considering the transmission of a single bit using antipodal signaling. With this revised definition of SNR, the *capacity* of the discrete-time Gaussian channel *with a peak power constraint and when the transmitter is restricted to using binary modulation* is

$$R^* = \log_2\left(\frac{2}{1+\exp(-\mathsf{SNR}/2)}\right) = 1 - \log_2(1+\exp(-\mathsf{SNR}/2)) \ \text{ bits per channel use.} \tag{11.8}$$

Alternatively, we can write

$$R^* = \log_2\left(\frac{2}{1+\exp(-\mathcal{E}/N_0)}\right) \ = 1 - \log_2(1+\exp(-\mathcal{E}/N_0)) \ \text{ bits per channel use.} \tag{11.9}$$

Notice that the capacity is nonzero for all $\mathsf{SNR} > 0$ and approaches 1 bit per channel use as $\mathsf{SNR} \to \infty$. The operational meaning of capacity is that at any $\mathsf{SNR} > 0$, it is possible to transmit data with *arbitrarily high reliability* over the channel at all rates $R < 1 - \log_2(1+\exp(-\mathsf{SNR}/2))$ using a suitable linear binary code of suitably large block length n, and binary modulation. Since $n\mathcal{E}$ is used to transmit nR bits so that the *energy per data bit* is $\mathcal{E}_b = \mathcal{E}/R > \mathcal{E}$, fixed and not dependent on n, we see that linear binary coding and binary modulation can be used to devise a rate-efficient (that is, fixed rate R bits per channel use regardless of how large n is) *and* energy-efficient (that is, fixed energy $\mathcal{E}_b$ per bit regardless of how large n is) *coding* scheme for communication over the discrete-time Gaussian channel. It is important to understand that *coding* is the key to data transmission with arbitrarily high reliability. Without coding, we could send data over the channel at rate of 1 bit per channel use using energy $\mathcal{E}$ per bit, but the error probability would be $Q(\sqrt{\mathsf{SNR}}) = Q(\sqrt{\mathcal{E}/\sigma^2})$ and could not be made any smaller. If we did not have a peak power constraint on the channel, we could use antipodal signaling with energy $\mathcal{E}_b = \mathcal{E}/R$ per data bit and improve this error probability to $Q(\sqrt{\mathcal{E}_b/\sigma^2}) < Q(\sqrt{\mathcal{E}/\sigma^2})$ but no smaller. This is a far cry from the *arbitrarily small* error probability promised by coding, though of course since there is no such thing as a free lunch, the data rate must be reduced from one data bit per channel use to R data bits per channel use where R is constrained to be smaller than R^* as specified in (11.8).

If we have an *average power constraint* on the channel, *viz.* the *total energy* over n channel uses must not exceed $n\mathcal{E}$ though there is not a peak power limitation on any particular channel use, and we do not restrict the transmitter to use only binary modulation, then the discrete-time Gaussian channel has a larger capacity

$$C = \frac{1}{2}\log_2(1+\mathsf{SNR}) \ \text{ bits per channel use.} \tag{11.10}$$

The proof of this important and famous result is unfortunately beyond the scope of this course, though the meaning is the same, *viz.* it is possible to communicate data with arbitrarily small error probability at all rates $R < C$ with average energy use of $\mathcal{E}/R$ per data bit by choosing a good coding scheme of rate R and sufficiently large block length n. One difference to note, though, is that as SNR increases, C in (11.10) *increases beyond one bit per channel use* instead of approaching the limiting value of one bit per channel use with binary modulation as happens with binary modulation and a peak power constraint.