Error Control Coding for Information Transmission and Storage

Shu Lin
Department of Electrical and Computer Engineering
University of California, Davis
Davis, CA 95616

Lecture 1

Introduction to Error Control Coding

1.1 A Block Diagram for a Data Transmission or Storage System

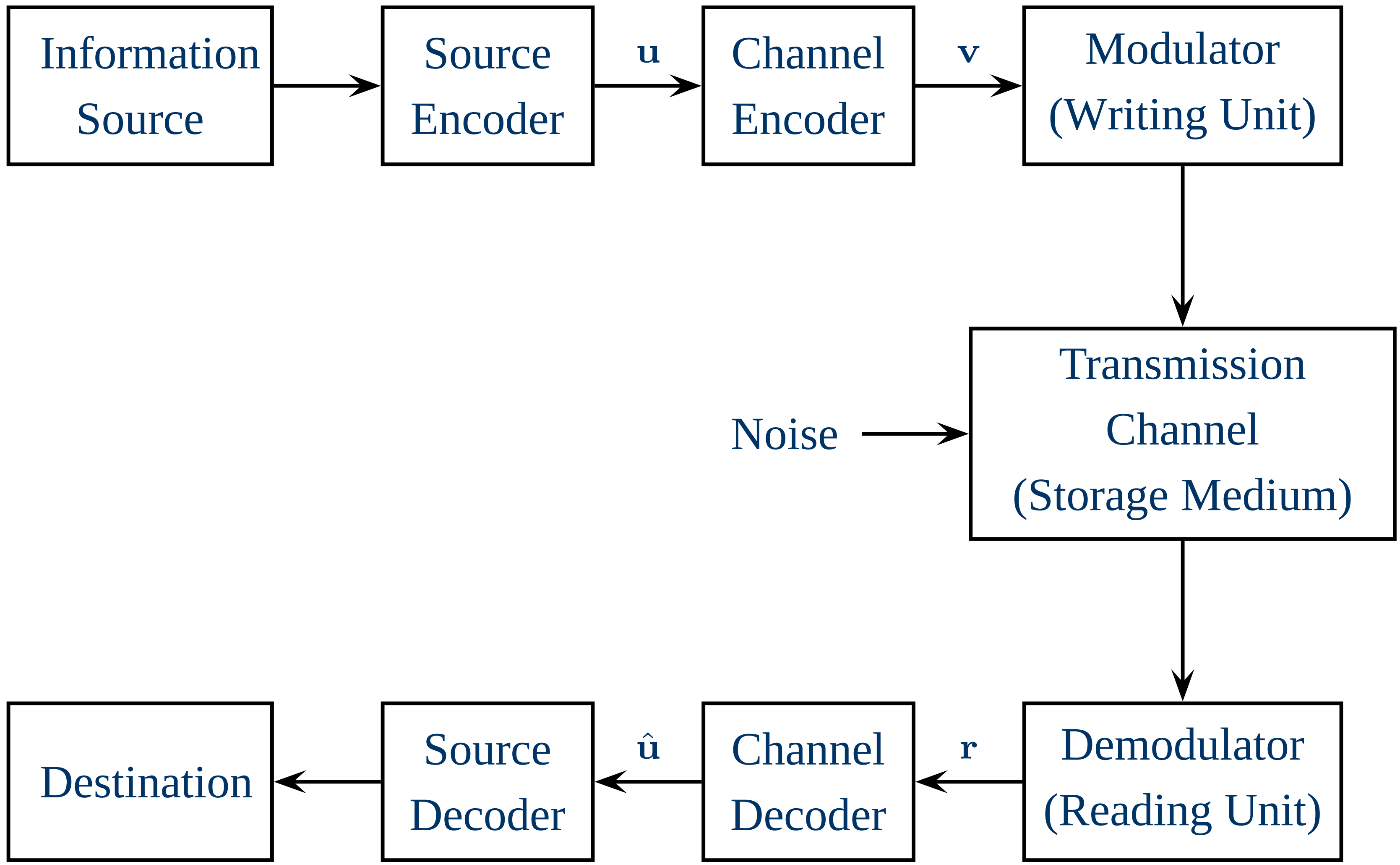

Figure 1.1: A block diagram of a typical data transmission or storage system.

1.2 Encoding

- In block coding, information sequence is divided into **messages** of k information bits (or symbols) each. Each message

$$\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$$

is mapped into a structured sequence of n bits (or symbols)

$$\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$$

based on certain rules where $n > k$. The sequence $\mathbf{v}$ is called the **code word** of the message $\mathbf{u}$.

- Corresponding to 2^k distinct messages, there are 2^n code words which form an (n,k) **block code**.

1.3 Decoding

- Suppose a code word $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ corresponding to a certain message is transmitted (or stored) over a noisy communication channel (or in a storage medium).

- Let $\mathbf{r} = (r_0, r_1, \ldots, r_{n-1})$ be the corresponding received (or read out) sequence. The receiver (or the decoder), based on $\mathbf{r}$, the encoding rules and noise characteristics of the channel (or storage medium), makes a decision which message was actually transmitted (or stored). This decision making operation is called **decoding**. The devise that performs the decoding operation is called a **decoder**.

- There are two types of decodings based on the inputs to the decoder (or the outputs of the demodulator).
- **Hard-Decision Decoding:** When binary coding is used, the modulator has only binary inputs. If the output of the demodulator is quantized into two levels, the decoder has only binary inputs. In this case, the demodulator is said to make **hard-decisions**. Decoding based on hard-decisions made by the demodulator is called **hard-decision decoding**.
- **Soft-Decision Decoding:** If the output of the demodulator consists of more than two quantization levels or is left unquantized, the demodulator is said to make **soft-decisions**. Decoding based on soft-decisions made by the demodulator is called **soft-decision decoding**.

- Hard-decision decoding is much easier to implement than soft-decision decoding. However, soft-decision decoding offers significant performance improvement over hard-decision decoding.

1.4 Some Channel Models

- In a binary coded communication or storage system, if the channel is an **additive white Gaussian noise** (AWGN) channel, hard-decision made by the demodulator results in a **binary symmetric channel** (BSC) shown in Figure 1.2.

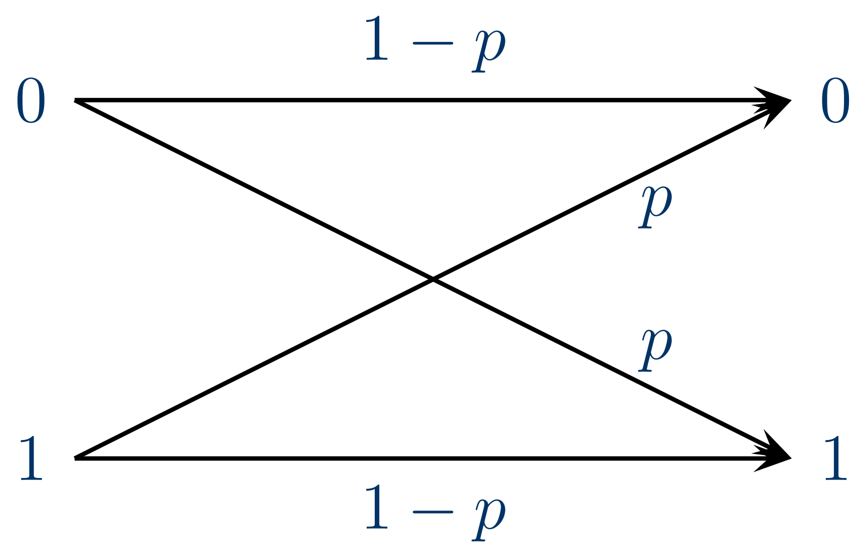

Figure 1.2: A binary symmetric channel.

- Suppose the demodulator makes soft-decision and has 8 output quantization levels. Then we have a binary-input, 8-ary output discrete channel as shown in Figure 1.3.

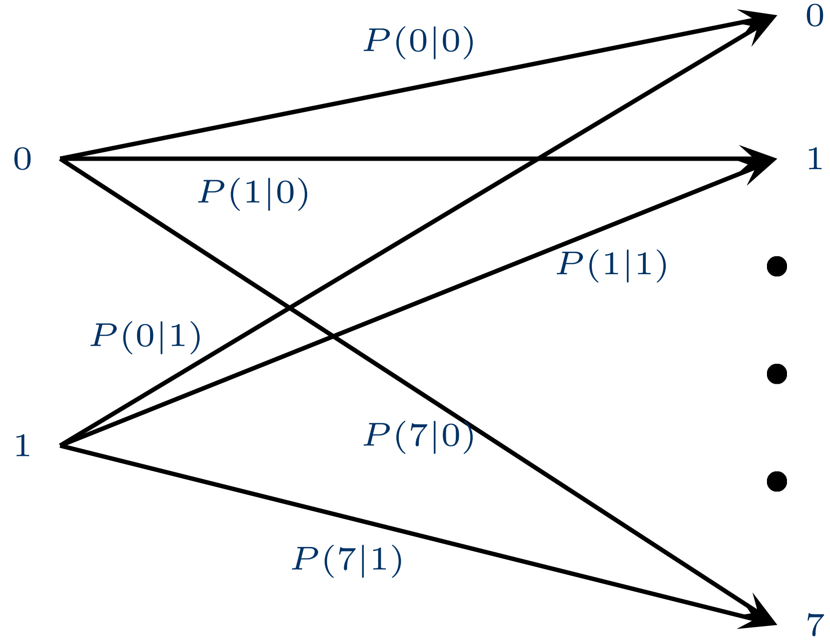

Figure 1.3: A binary-input, 8-ary output discrete channel.

1.5 Optimal Decoding

- Given a code, we want to devise a decoding scheme (or rule) to keep the **probability** of a **decoding error** as small as possible.

- Given that $\mathbf{r}$ is received, the conditional error probability of decoding is defined as

$$P(E|\mathbf{r}) \triangleq P(\hat{\mathbf{v}} \neq \mathbf{v}|\mathbf{r})$$

Then the error probability of the decoding is

$$P(E) \triangleq \sum_{\mathbf{r}} P(E|\mathbf{r})P(\mathbf{r})$$

- A decoding rule that minimizes $P(E)$ is referred to as an **optimum decoding rule**.
- Note that $P(\mathbf{r})$ is independent of the decoding rule used since $\mathbf{r}$ is produced before decoding.
- Hence an optimum decoding rule must minimize $P(E|\mathbf{r}) = P(\hat{\mathbf{v}} \neq \mathbf{v}|\mathbf{r})$ for all $\mathbf{r}$. Since minimizing $P(\hat{\mathbf{v}} \neq \mathbf{v}|\mathbf{r})$ is equivalent to maximizing $P(\hat{\mathbf{v}} = \mathbf{v}|\mathbf{r})$.
- $P(E|\mathbf{r})$ is minimized for a given $\mathbf{r}$ by choosing $\hat{\mathbf{v}}$ as the codeword that maximizes

$$P(\mathbf{v}|\mathbf{r}) = \frac{P(\mathbf{v})\mathbf{P}(\mathbf{r}|\mathbf{v})}{P(\mathbf{r})} \quad .$$

- Optimal Decoding

1. Compute the conditional probability $P(\mathbf{v}|\mathbf{r})$ for every codeword $\mathbf{v}$.
2. Decode the received sequence $\mathbf{r}$ into the codeword $\hat{\mathbf{v}}$ that has the largest **a posteriori probability** $P(\hat{\mathbf{v}}|\mathbf{r})$, i.e.,

$$P(\hat{\mathbf{v}}|\mathbf{r}) > \mathbf{P}(\mathbf{v}|\mathbf{r})$$

for $\mathbf{v} \neq \hat{\mathbf{v}}$.

1.6 Maximum Likelihood Decoding

- Suppose all the messages are **equally likely**.
- An optimal decoding can be done as follows:
  1. For every code word $\mathbf{v}_j$, compute the conditional probability $P(\mathbf{r}|\mathbf{v}_j)$.
  2. The code word $\mathbf{v}_k$ with the largest conditional probability is chosen as the estimated transmitted code word, called the decoded code word.
  3. Find the corresponding message $\mathbf{u}_k$ for the decoded code word $\mathbf{v}_k$.
- This decoding rule is called the **maximum likelihood decoding (MLD)**.

1.7 Error Performance Measure

- The error performance of a coded system is measured by the **error probability** of a decoding. There are two types of error probabilities which are used for performance measures: the **block (word or frame) error probability** and **bit (or symbol) error probability** (also known as **bit- (symbol-) error rate**, denoted BER or SER).
- The block-error probability is the probability that a decoded code word is in error, and the bit-error (or symbol-error) probability is the the probability that a decoded bit (or symbol) in error.

1.8 Coding Gain

- The usual figure of merit for a coded system is the ratio of energy per information bit (or symbol) to noise power spectral density, denoted E_b/N_0, which is required to achieve a given error probability. E_b/N_0 is referred to as the **signal-to-noise** ratio (SNR).
- **Coding gain** of a coded system over an uncoded system with the same modulation (or a reference system) is defined as the reduction, expressed in decibels, in the required E_b/N_0 to achieve a specified error probability, say bit-error rate.
- Coding gain is commonly used for evaluating the effectiveness of a coded system.

- Let $(E_b|N_0)_{uncoded}$ and $(E_b|N_0)_{coded}$ be the SNRs required by an uncoded and a coded systems to achieve a specified error probability P_b, respectively.

- In decibels, the SNRs are expressed as follows:

$$10\log_{10}(E_b|N_0)_{uncoded}, \quad (dB)$$
$$10\log_{10}(E_b|N_0)_{coded}$$

- Coding gain,

$$\begin{aligned}\eta &= 10\log_{10}(E_b|N_0)_{uncoded} - 10\log_{10}(E_b|N_0)_{coded} \\ &= 10\log_{10}\frac{(E_b|N_0)_{uncoded}}{(E_b|N_0)_{coded}} \ (dB)\end{aligned}$$

- If $\frac{(E_b|N_0)_{uncoded}}{(E_b|N_0)_{coded}} = 2$ at the BER $= 10^{-5}$ then

$$\eta = 10 \log_{10} 2 = 3 \; dB$$

- We say that the coded system achieves 3 dB coding gain over the uncoded system at the BER $= 10^{-5}$.

1.9 Shannon Limit

- In designing a coded system, it is desired to minimize the SNR required to a achieve a specific error rate.
- This is equivalent to maximizing the coding gain over an uncoded system.
- A theoretical limit on the minimum SNR required for coded system with code rate R to achieve error-free information transmission is called the **Shannon limit**. This theoretical limit simply says that for a coded system with rate R, error-free information transmission is achievable only if the SNR exceeds this limit.

- As long as the SNR exceeds this limit, Shannon's coding theorem guarantees the existence of a coded system, perhaps very complex, capable of achieving error-free information transmission.

- Figure 1.4 gives the Shannon limit as a function of code rate for a binary input continuous output AWGN channel with BPSK signalling.

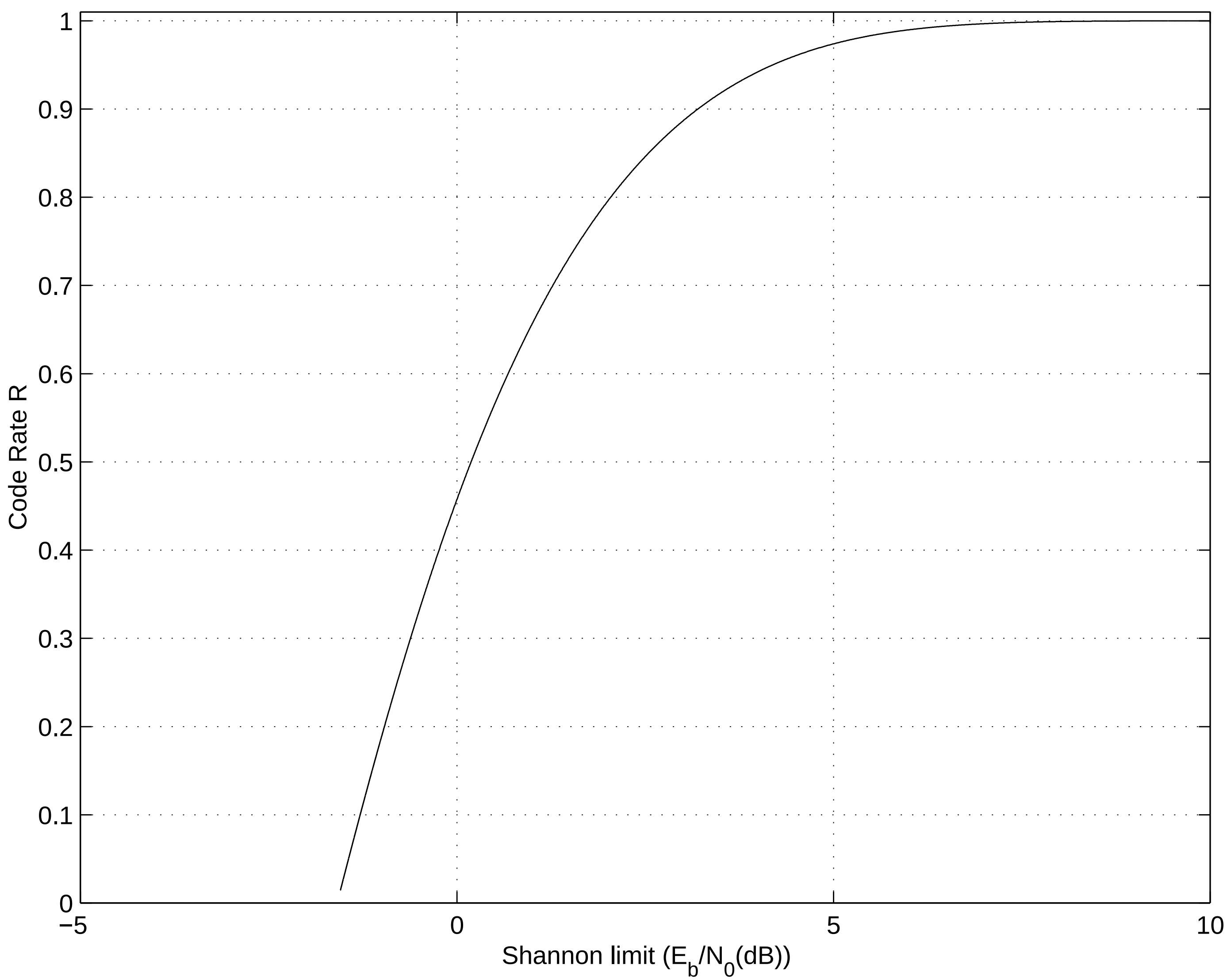

Figure 1.4: Shannon limit as a function of code R.