Channel Coding Theory (EELE 6338)

Lecture # 1

Chapter1: Coding for Reliable Digital Transmission and Storage

Link to the book:

http://en.bookfi.org/md5/4F09E9E85F28C6F06054F2EF8E7D236A

Outline

- Introduction.
- Types of the codes.
- Modulation and Coding.
- Maximum likelihood decoding.
- Error types.
- Error correcting strategies.
- Performance measures.

Error Control Coding?

- **What** is error control?
  Detecting/Correcting errors in digital data
- **How**?
  By adding redundancy to the information sequence (encoding) and utilize it to catch the errors (decoding)
- **Why**?
  Enhance the reliability of the system.

Introduction

- **Reliable communication** : Communication where messages are guaranteed to reach their destination complete and uncorrupted and in the order they were sent.
- Emergence of large scale and High speed data networks increase the demand for reliable and efficient communications.
- The system designer major concern is the control of errors so that the data can be reliably produced.

Introduction(2)

- Shannon 1948, "by proper encoding of the information, errors induced by a noisy channel or storage medium can be reduced to any desired level without scarifying the rate of information transmission or storage as long as the information rate is less than the capacity of the channel".
- Much effort has been done to design efficient coding and encoding schemes → achieve required reliability by current high-speed digital systems.

Introduction (3)

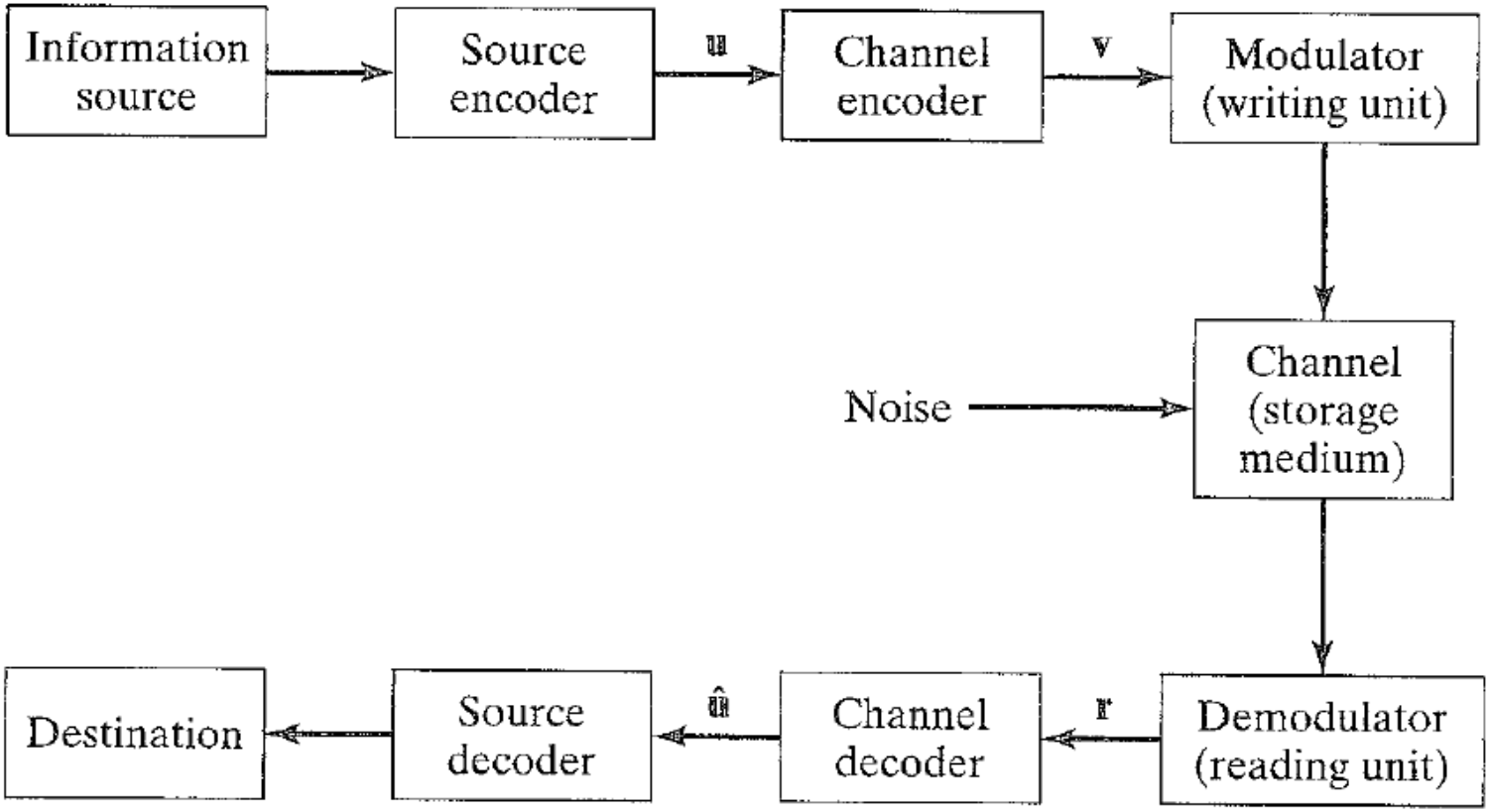


FIGURE 1.1: Block diagram of a typical data transmission or storage system.

Introduction (4)

- Information source : human or machine.
- Source encoder: transforms the source output into a sequence of binary digits called information sequence.
  - The number of bits per unit time required to represent the source output is minimized.
  - The source output can be unambiguously reconstructed from the information sequence.

Introduction (5)

- Channel encoder: transform the information sequence into discrete sequence called codeword. The encoder is designed to combat the noisy environment.
- Received Sequence : the sequence of the demodulator output.
- Estimated information sequence: the output of the channel encoder.
- The probability of the decoding errors should be minimized.

Introduction (6)

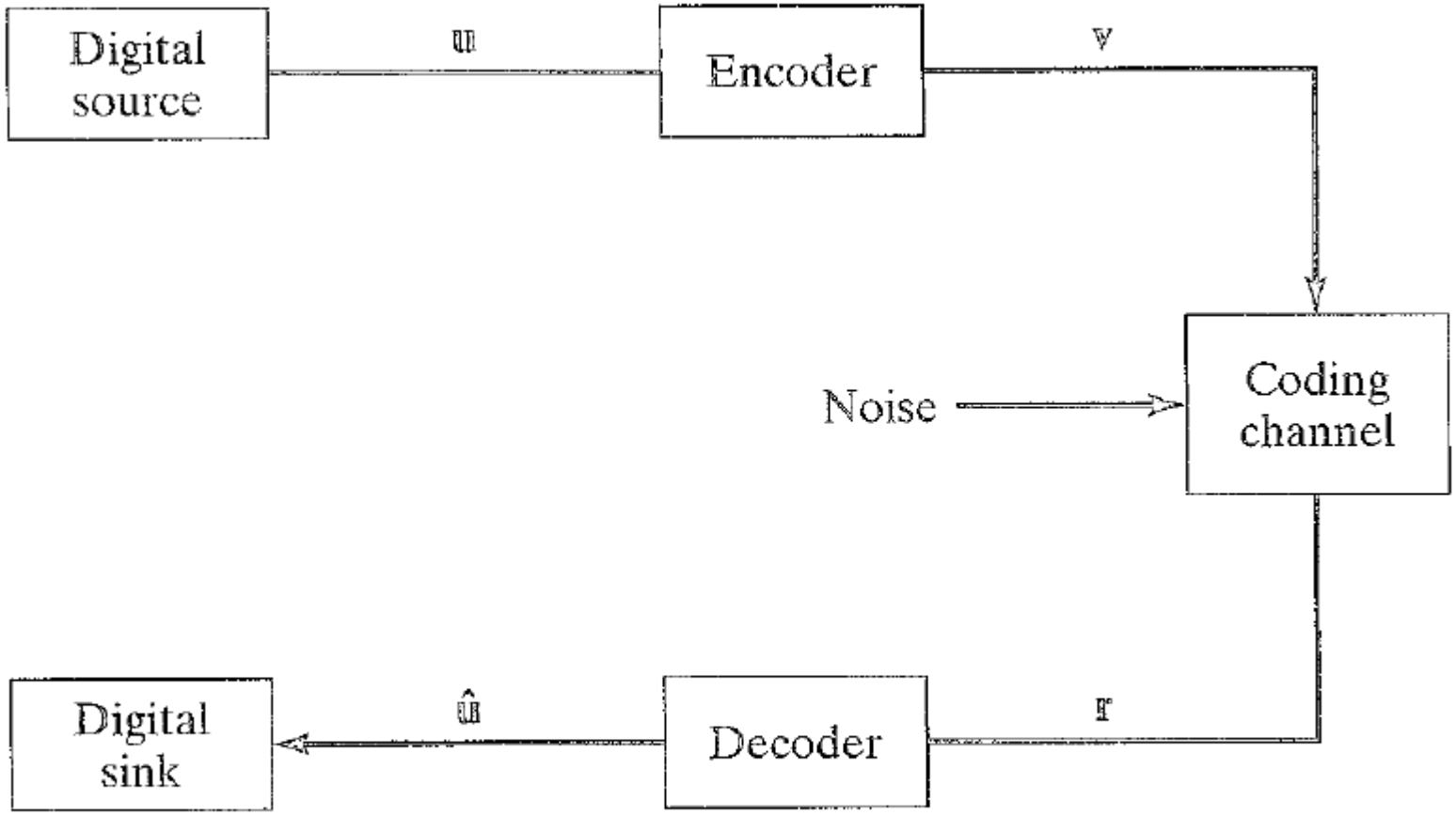


FIGURE 1.2: Simplified model of a coded system.

Introduction (7)

- The channel encoder/decoder pair should be designed such that
  1. Information can be transmitted in a noisy environment as fast as possible.
  2. The information can be reliably reproduced at the output of the channel decoder.
  3. The cost of the implementation falls within acceptable limits.

Types of Codes

- Generally the codes are classified into Block or Convolutional codes.
- Block Code:
  - The encoder divides the information sequence into message blocks of k information bits.
  - The message is represented by the binary k-tuple $U = (u_0, u_1, \dots, u_{\{k-1\}})$ → 2^k possible messages.
  - The encoder transform U into n-tuple $V = \left(v_0, v_1, \cdots, v_{\{n-1\}}\right)$ called codeword.
  - 2^k possible codewords.
  - Such a code called (n,k) block code.

Types of Codes (2)

- Code rate: $R = \frac{k}{n}$, the number of information bits entering the encoder per transmitted symbol.
- The encoder is memory less and can be implemented with combinational logic circuits.
- Binary Code : the codewords are binary.
- n-k redundant bits are added to each message to form the codeword.
- These redundant bits provide the code the capability to combat the channel.
- More redundant bits can be added for fixed rate R.

Types of Codes (3)

TABLE 1.1: A binary block code with $k = 4$ and $n = 7$.

Messages	Codewords
(0 0 0 0)	(0 0 0 0 0 0 0)
(1 0 0 0)	(1 1 0 1 0 0 0)
(0 1 0 0)	(0 1 1 0 1 0 0)
(1 1 0 0)	(1 0 1 1 1 0 0)
(0 0 1 0)	(1 1 1 0 0 1 0)
(1 0 1 0)	(0 0 1 1 0 1 0)
(0 1 1 0)	(1 0 0 0 1 1 0)
(1 1 1 0)	(0 1 0 1 1 1 0)
(0 0 0 1)	(1 0 1 0 0 0 1)
(1 0 0 1)	(0 1 1 1 0 0 1)
(0 1 0 1)	(1 1 0 0 1 0 1)
(1 1 0 1)	(0 0 0 1 1 0 1)
(0 0 1 1)	(0 1 0 0 0 1 1)
(1 0 1 1)	(1 0 0 1 0 1 1)
(0 1 1 1)	(0 0 1 0 1 1 1)
(1 1 1 1)	(1 1 1 1 1 1 1)

Types of codes (4)

- Convolutional Codes
  - Accept k-bits blocks of information sequence U and produce an encoded sequence V of n-symbol blocks.
  - Has memory : each encoded block depends not only on the corresponding k-bit message at the same time but also on m previous message blocks.
  - The encoder has memory of order m.
  - Code rate = k/n.
  - Implemented using sequential logic circuits.

Type of code (5)

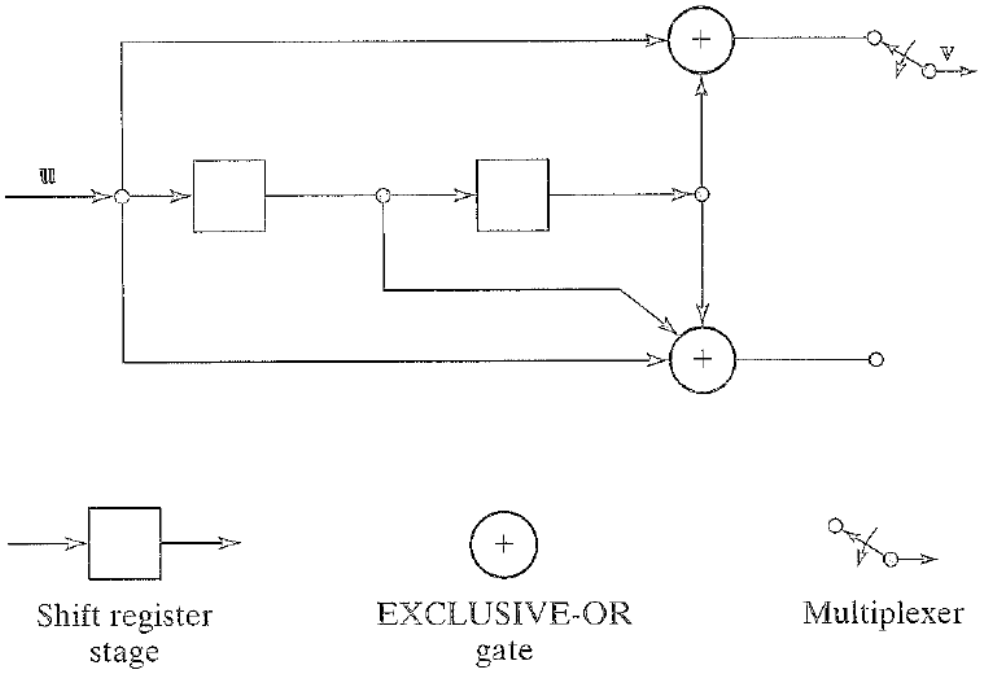


FIGURE 1.3: A binary feed-forward convolutional encoder with $k = 1$, $n = 2$, and $m = 2$.

U=(110100…) → v=(11,10,10,00,01,11,00,00,00,..)

Modulation and Coding

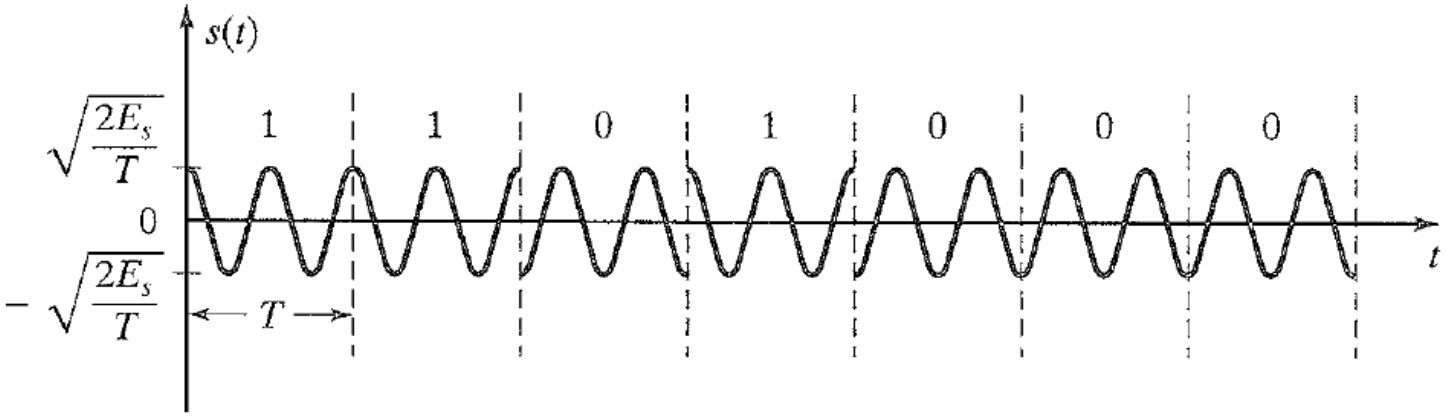


FIGURE 1.4: BPSK-modulated waveform corresponding to the codeword $\mathbf{v} = (1101000)$.

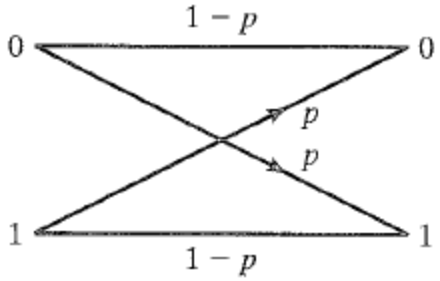
- Memory-less Channel : if the detector in a given interval depends only on the transmitted signal in that interval and not on any previous transmission.

Modulation and coding (2)

- Discrete memory-less channel (DMC): the combination of the modulator, physical memory-less channel and the demodulator.
- Its completely described by the transition probability $P(j/i)$.
- Binary symmetric channel (BSC) : the input and output are binary and the amplitude distribution of the noise is symmetric.

Modulation and Coding (3)

- The transition probability diagram of the BSC channel



(a)

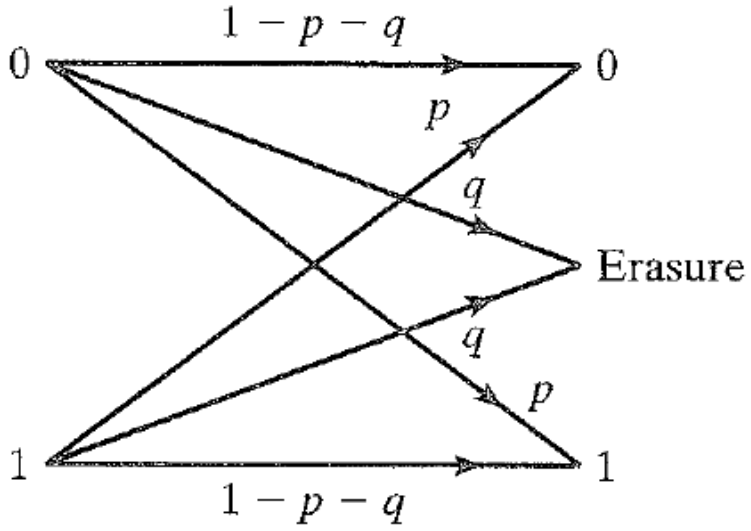
- Note that the transition probability completely describe the channel.

Modulation and Coding (4)

- The transition probability p calculated from
  - Knowledge of the signal used.
  - Probability distribution of the noise.
  - Output quantization threshold of the demodulator.
- Example : for BPSK $p = Q(\sqrt{2E_s/N_o})$, where Q(x) is the complementary error function.
- $Q(x) \leq \frac{1}{2} e^{\left\{-\frac{x^2}{2}\right\}}, x \geq 0$

Modulation and Coding (5)

- In binary systems with 2-level quantization, Hard-decision decoding is used.
- Binary symmetric erasure channel (BSEC)



(b)

Modulation and coding (6)

- Stream of data with symbol time T has rate 1/T.
- If we encode it with code of the rate R<1, the information rate is R/T.
- To achieve the same rate of the un-coded system, BW expansion is required by factor 1/R.

Maximum likelihood decoding

- Suppose that the codewords from the code {000,111} are being sent over a BSC with transition probability p=0.05. Suppose that the word 110 is received. What is the sent codeword?
- P(110 recieved|000sent)=P(1|0).P(1|0).P(0|0)
  =0,002375.
- P(110 recieved|111sent)=P(1|1).P(1|1).P(0|1)
  =0,045125.

Maximum likelihood decoding (2)

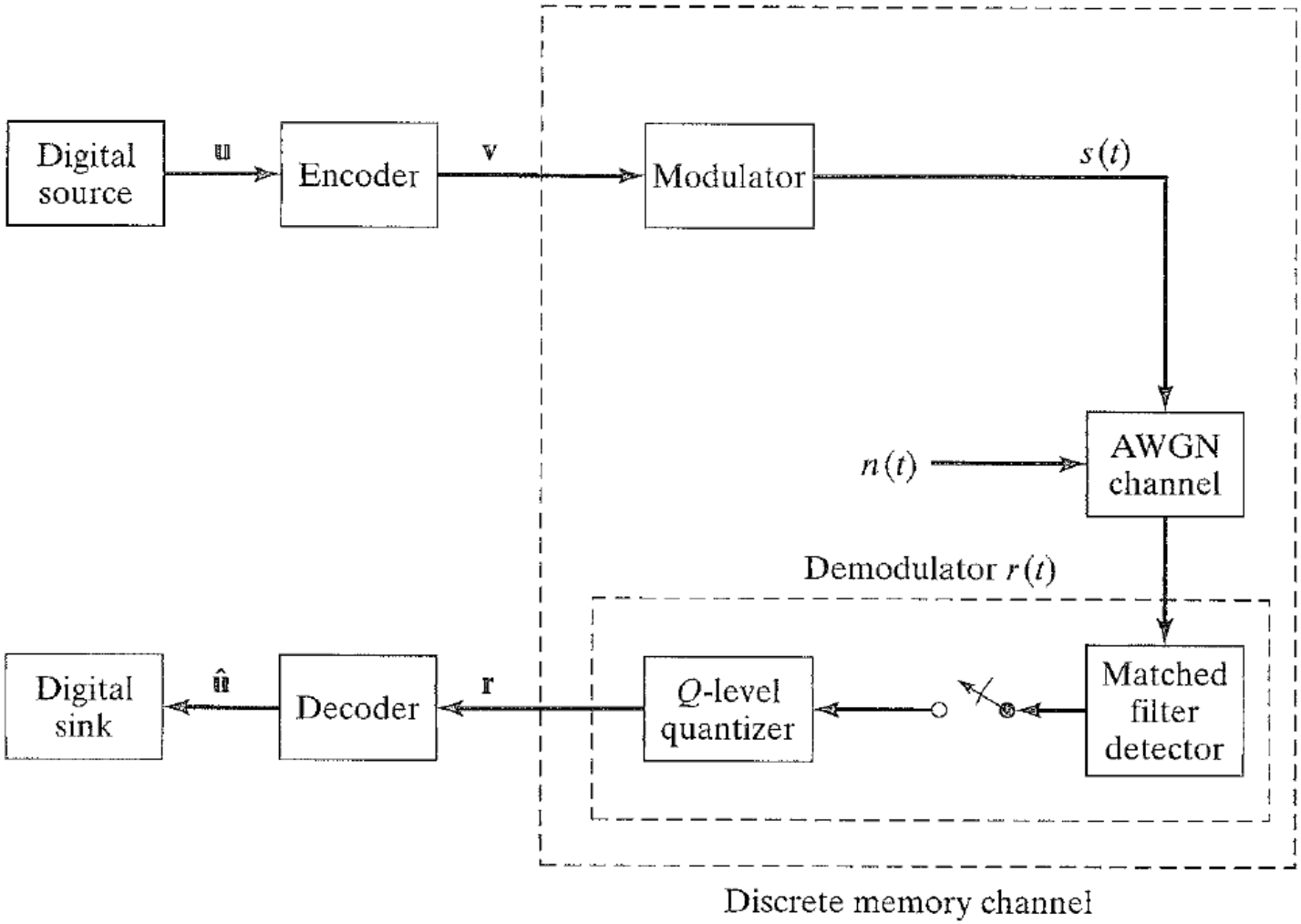


FIGURE 1.7: A coded system on an additive white Gaussian noise channel.

Maximum likelihood decoding (3)

- A decoding rule: is a strategy for choosing an estimated codeword $\hat{v}$ for each possible received sequence r.
- Decoding error occurs when $\hat{v} \neq v$.
- Conditional error probability of the decoder

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

- Probability of error

$$P(E) = \sum_{\mathbb{r}} P(E|\mathbb{r})P(\mathbb{r}),$$

Maximum likelihood decoding (4)

- P(r) is independent of the decoding rule.
- The optimum decoding rule is the one that minimize P(E) → minimize P(E|r) for all r.
- Minimize $P(\hat{v} \neq v|r)$ is equivalent to maximize $P(\hat{v} = v|r)$

$$P(\mathrm{v}|\mathrm{r}) = \frac{P(\mathrm{r}|\mathrm{v})P(\mathrm{v})}{P(\mathrm{r})};$$

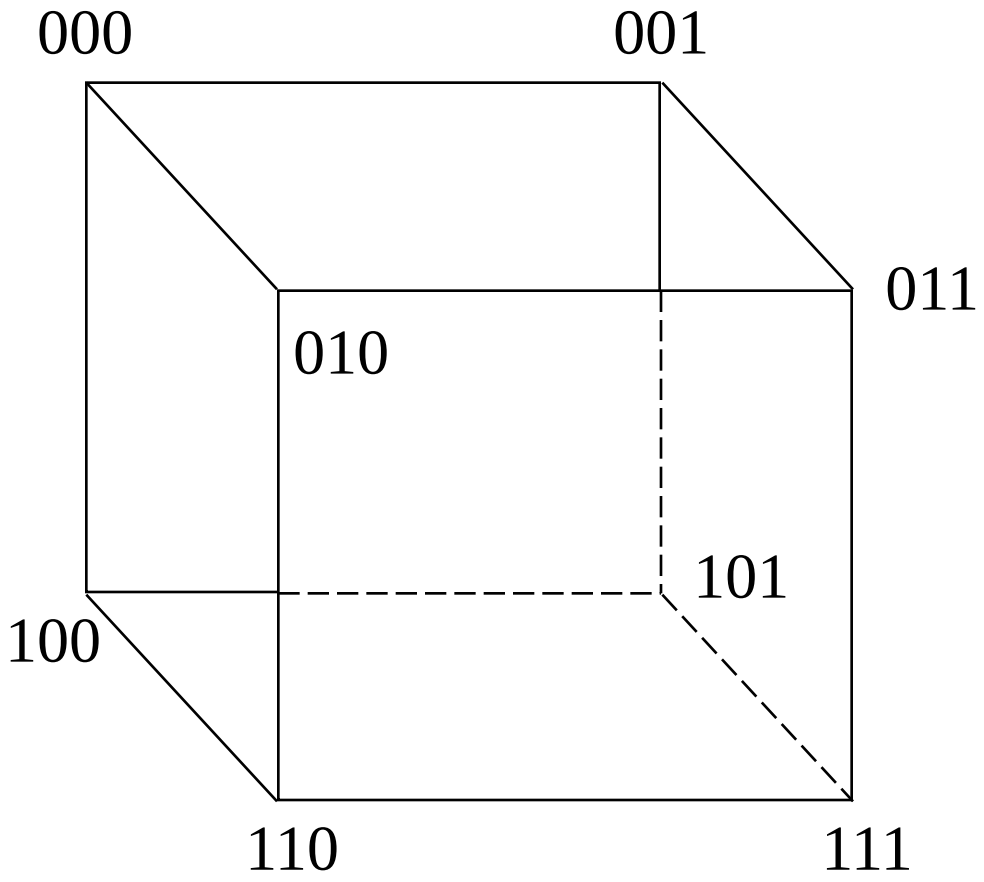
If all the codewords equally likely → P(v) is equal

Maximum likelihood decoding (5)

$$P(\mathbb{r}|\mathbb{v}) = \prod_i P(r_i|v_i),$$

- A decoder that chooses its estimate to maximize this equation is called a maximum likelihood decoder (MLD). [complete (arbitrary) and Incomplete (retransmission)].
- Hamming distance d(r,v) : is the number of positions in which r and v are different.

Maximum likelihood decoding (6)



Maximum likelihood decoding (7)

- Suppose that the codeword v are being transmitted over BSC. If r is received, then the conditional probability is

$$P(v\ recieved|r\ sent) = p^{d(r,v)}(1-p)^{n-d(r,v)}$$

- For P<1/2 → 1-p>p and hence the conditional probability is larger when 1-p increased.
- 1-p term increase by reducing d(r,v) → MLD is equivalent to choosing min d(r,v).

Maximum likelihood decoding (8)

- Suppose codewords from the binary code C={0000,0011,1000,1100,0001,1001} are being sent over BSC. Assuming r=0111 what is the most likely v?

  - 0011 with d=1;

Error types

- Random error channels : transmission error occur randomly in the received sequence (BSC channel). Error in different bits is independent.
- Example : Line-of-sight transmission and satellite channels.
- Code name : random-error correcting codes.

Error types (2)

- On channels with memory, the noise is not independent from one transmission to another.
- Example=??
- The channel has two states “good” in which the error occur infrequently P1~0 and “bad” in which the error occurs frequently P2~0,5.
- The channel is good state most of the time but shifts sometimes to the bad state.
- Burst error correcting codes.
- Combined channel → burst-and-random error correcting codes.

Error types (3)

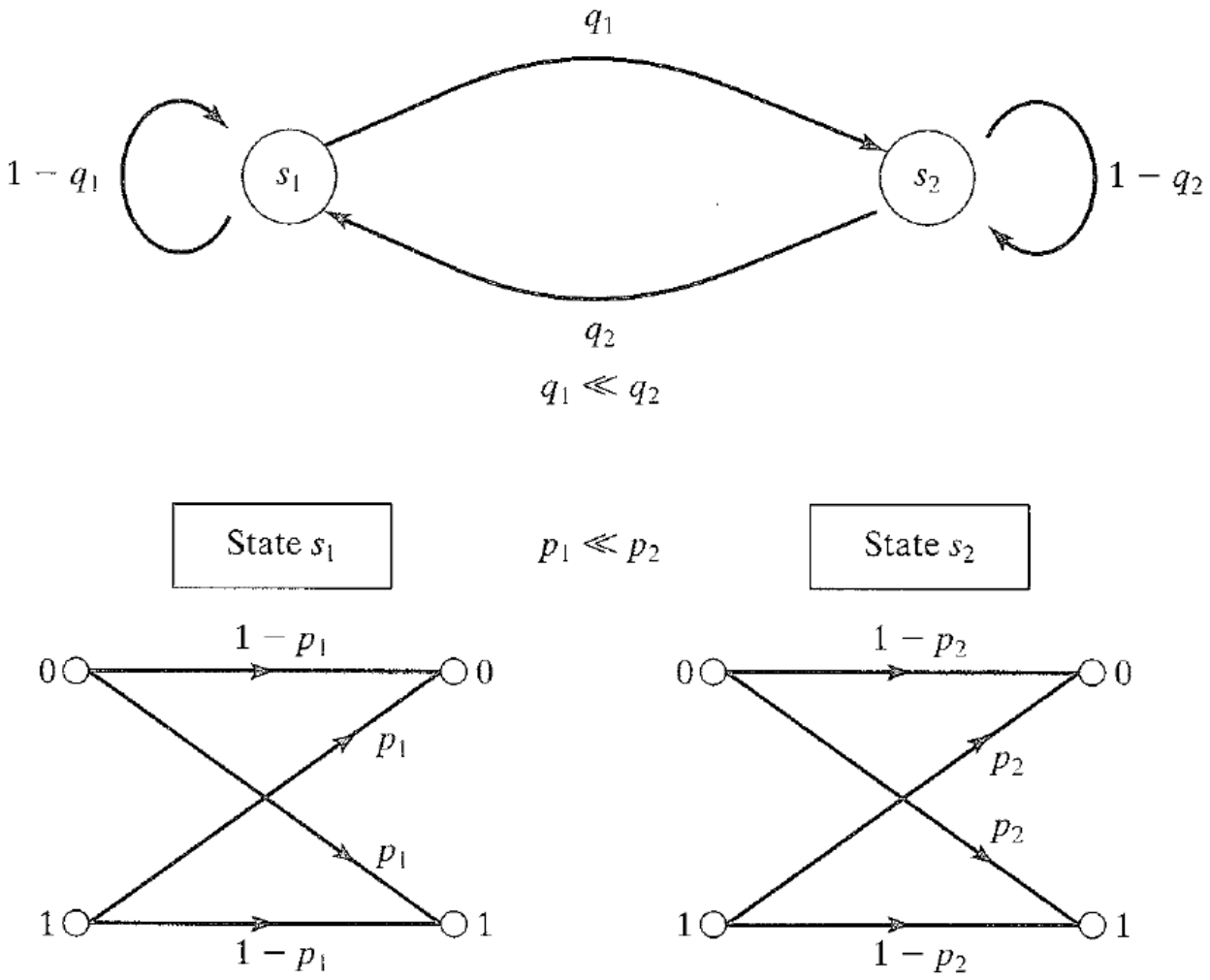


FIGURE 1.8: A simplified model of a channel with memory.

Error Control strategies

- Forward Error Correction (FEC) : used in one way transmission and employ error correction codes that automatically correct errors detected at the receiver.
- Most of the process work done at the transmitter (satellite comm.)
- Majority of the systems apply this technique.

Error Control strategies (2)

- Automatic repeat request (ARQ) : in two way systems . When errors detected at the receiver, a request is sent for the transmitter to repeat the message, and repeat requests until the message is correctly received.
- ARQ simpler than FEC.
- Combination of both is the best, FEC to correct frequent errors while ARQ to correct the rare ones.

Performance measures

- The performance of a coding scheme is measured by
  - Probability of decoding error (error probability)
    - Word or block error probability (WER) and (BLER).
    - Bit error probability (BER).
  - The coding gain is the amount of additional SNR or E_b/N_0 that would be required to provide the same BER performance for an un-coded signal.

$$G_c = \left(\frac{E_b}{N_o}\right)_{\text{uncoded}} - \left(\frac{E_b}{N_o}\right)_{\text{coded}}.$$

Performance measures (2)

SNR threshold

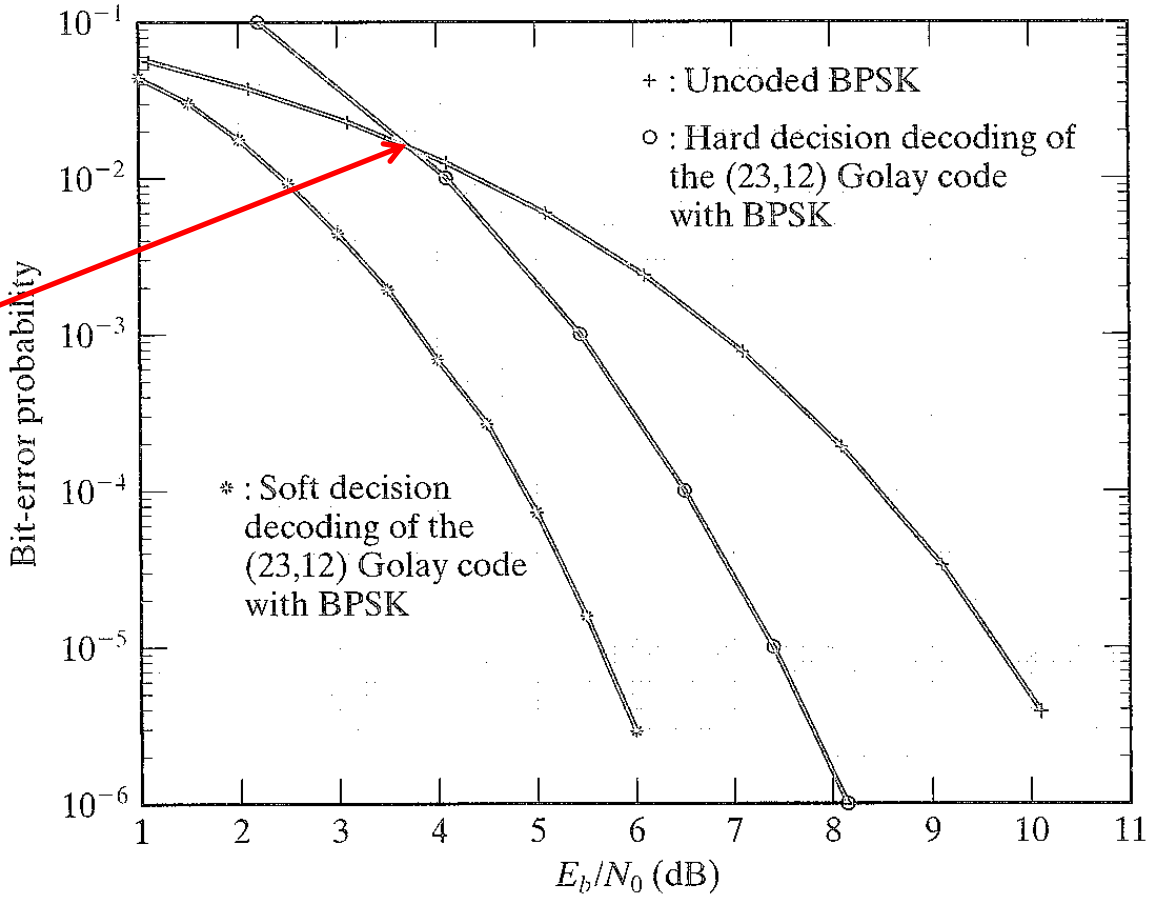


FIGURE 1.9: Bit-error performance of a coded communication system with the (23,12) Golay code.

Next lecture

- Algebra of Finite Fields.