E2 205: Error-Control Coding

Chapter 1: Introduction and Motivation

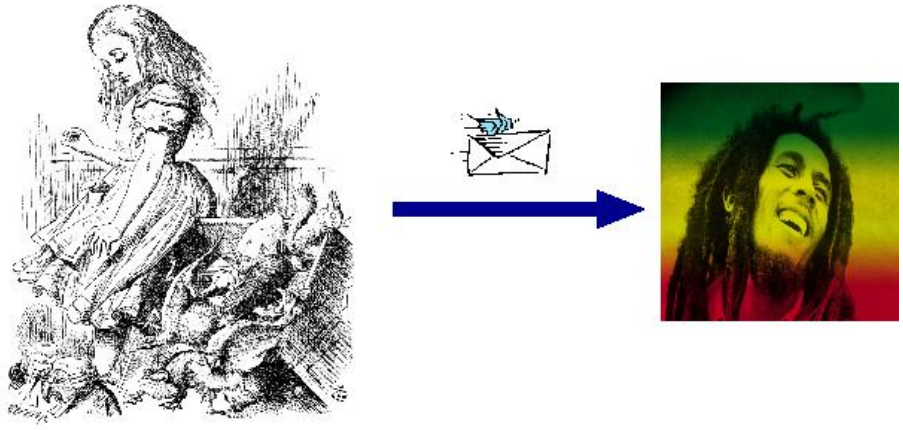
Navin Kashyap

Indian Institute of Science

Introducing Alice and Bob

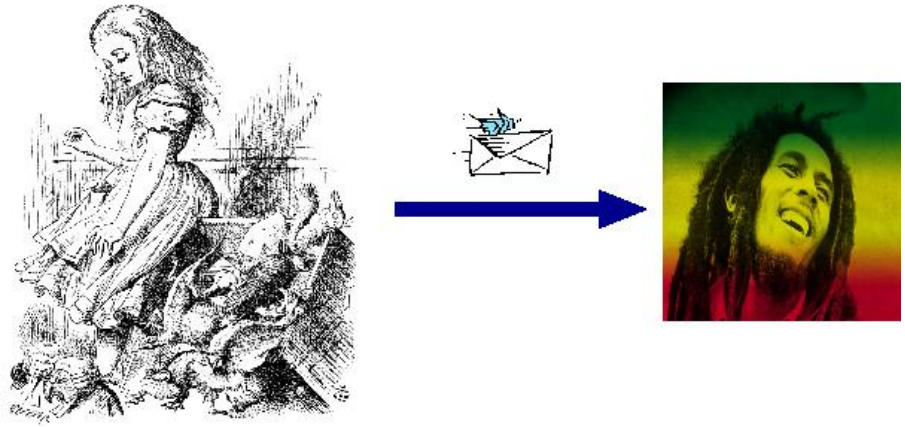
The two central characters in our story.

Alice Communicates to Bob



- Alice must communicate to Bob an important piece of information.

Alice Communicates to Bob



- Alice must communicate to Bob an important piece of information.
- Alice is concerned that the information may be intercepted by her enemies.
- Alice is short on time and money. She needs to send her information across cheaply and quickly.
- The communications channel she uses is noisy and unreliable. She needs to ensure that the information she sends is received correctly and reliably by Bob.

Coding Theory to the Rescue

What is Coding?

The representation of information using symbols, often 0s and 1s.

Coding Theory to the Rescue

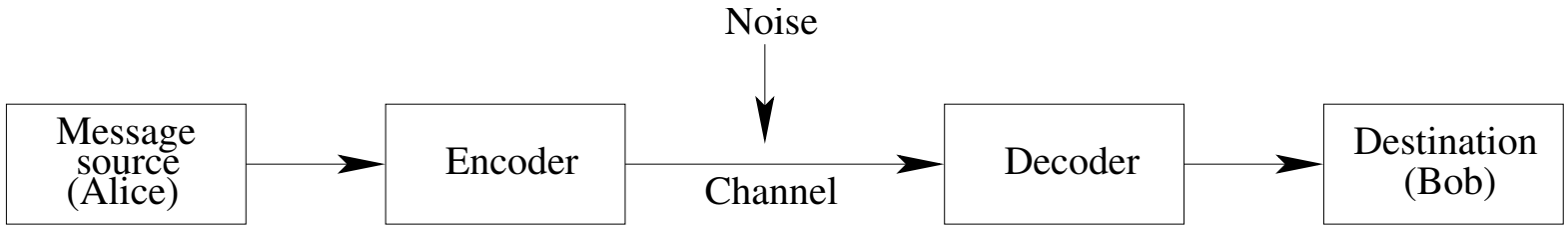
What is Coding?

The representation of information using symbols, often 0s and 1s.

There are three different types of coding:

- Secrecy Coding (aka Cryptography): Enables Alice to *encrypt* her message to foil her enemies.
- Source Coding: Enables Alice to
  - *convert* her message into a format ready for transmission, and
  - *compress* her message to save on the cost of transmission.
- Channel Coding: Enables Alice to *send her message reliably* to Bob, by including some mechanism to counter channel noise.

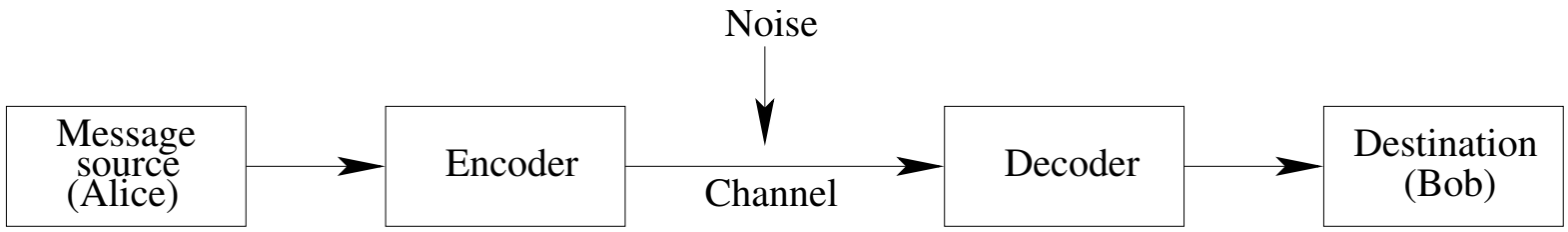
Standard Communication System Model



- The channel is the medium across which information is to be transmitted or communicated.
- Communication may take place across space — e.g., telephone lines, mobile phones, TV/radio/satellite broadcasts, email, postal mail etc.

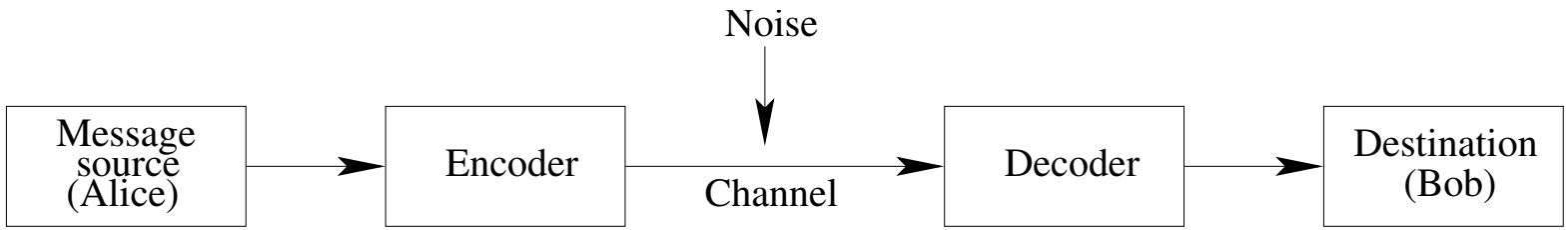
  or across time — e.g., recording media such as clay tablets, paper, magnetic tapes, hard drives, CDs, DVDs, biomolecules such as DNA etc.
- Physical channels are usually noisy.

Channel Noise



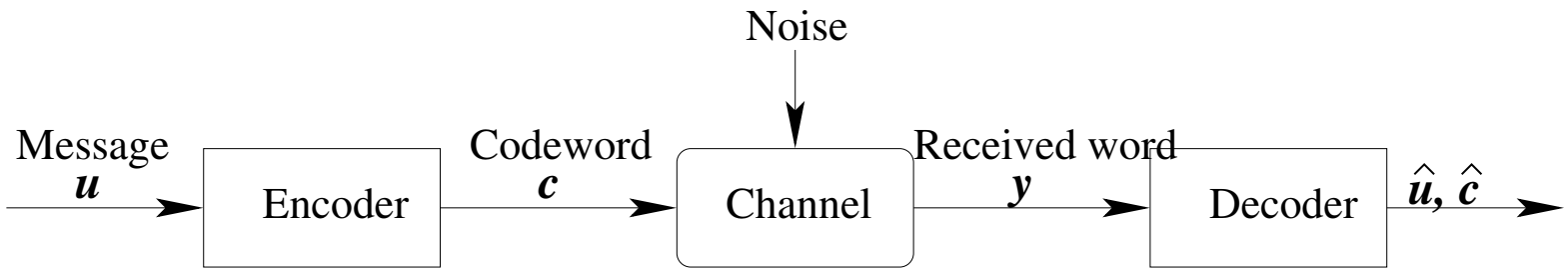
- Channel noise follows a model known to both Alice and Bob, who intend to fully make use of this knowledge to encode and decode.
- Noise may be deterministic or random; if random, it follows a probabilistic model.
- The effect of noise is to introduce errors in the transmitted message.

Channel Noise



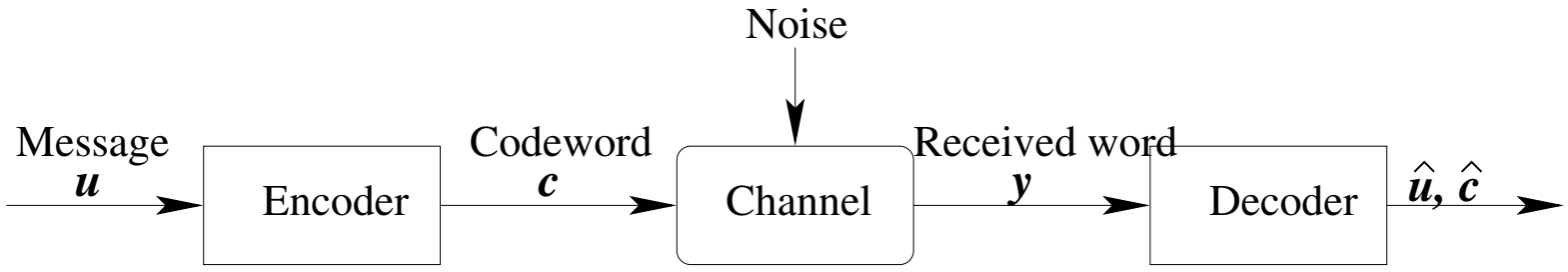
- Channel noise follows a model known to both Alice and Bob, who intend to fully make use of this knowledge to encode and decode.
- Noise may be deterministic or random; if random, it follows a probabilistic model.
- The effect of noise is to introduce errors in the transmitted message.
- The goal of channel coding is to reduce or eliminate the effects of channel noise.

Channel Coding



- The decoder produces estimates $\hat{\mathbf{c}}$ and $\hat{\mathbf{u}}$, with the aim of having $\hat{\mathbf{c}} = \mathbf{c}$ and $\hat{\mathbf{u}} = \mathbf{u}$.
- This means that the encoding map $\mathbf{u} \mapsto \mathbf{c}$ must be one-to-one, so that if the codeword $\mathbf{c}$ is correctly decoded, then the correct message $\mathbf{u}$ can also be recovered.

Channel Coding



- Codewords are finite-length words composed of symbols from an underlying code alphabet.
- Typically, in digital communications, the code alphabet is the binary alphabet consisting of the bits 0 and 1.
- Other alphabets, e.g., octal or hexadecimal, may also be used.
- However, the size of the code alphabet is almost always finite.

Three Types of Channel Codes

Error-Detecting Codes: Allows Bob to *detect* errors in received message; useful in random noise situations.

Error-Correcting Codes: Allows Bob to *correct* errors in received message; useful in random noise situations.

Constrained Codes: Alice encodes the message in such a way as to *prevent* errors from corrupting the message; useful in deterministic noise situations.

Three Types of Channel Codes

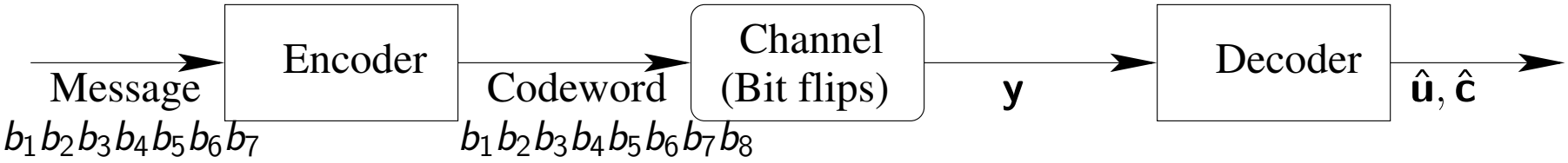
Error-Detecting Codes: Allows Bob to *detect* errors in received message; useful in random noise situations.

Error-Correcting Codes: Allows Bob to *correct* errors in received message; useful in random noise situations.

Constrained Codes: Alice encodes the message in such a way as to *prevent* errors from corrupting the message; useful in deterministic noise situations.

All coding schemes work by adding redundancy to the message to compensate for errors: more symbols are transmitted than are in the original message.

A Simple Error-Detecting Code



Channel Noise: Flips bits at random ($0 \to 1$, $1 \to 0$).

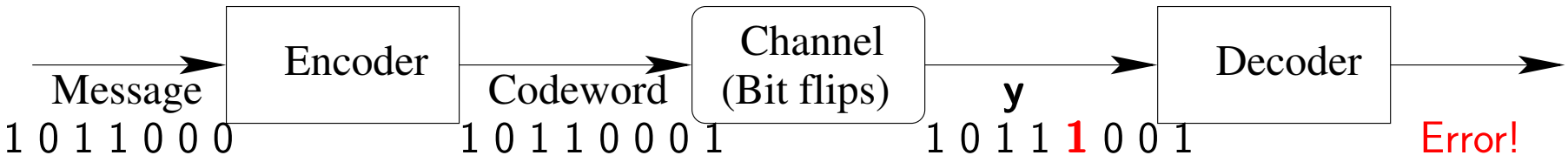
Message: 7-bit binary sequence $(b_1, b_2, b_3, b_4, b_5, b_6, b_7)$

Encoder: Adds 8th bit, called a parity bit, b_8, so that $(b_1, b_2, \ldots, b_8)$ contains an even number of 1s:

$$\sum_{i=1}^{8} b_i \equiv 0 \pmod 2$$

Rate: The number of message bits per coded bit is $7/8$.

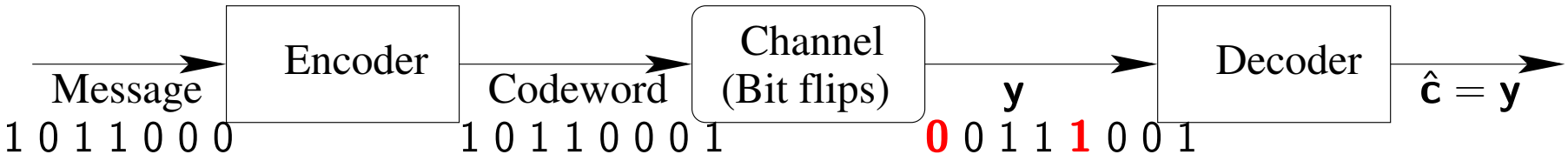
A Simple Error-Detecting Code



- If any one of the transmitted bits gets flipped by the channel, then the no. of 1s becomes odd.

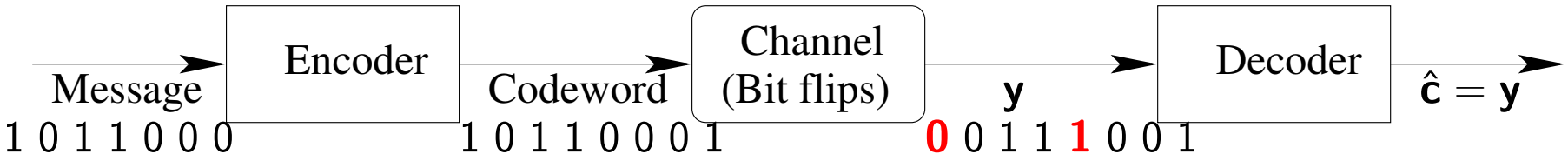
  In this case, decoder realizes that an error has happened in transmission.

A Simple Error-Detecting Code



- If the received word has even parity, decoder accepts it as the transmitted word.

A Simple Error-Detecting Code



- If the received word has even parity, decoder accepts it as the transmitted word.

Decoder:

$$\hat{\mathbf{c}} = \begin{cases} \mathbf{y} & \text{if } \mathbf{y} \text{ has even parity} \\ \text{ERROR} & \text{if } \mathbf{y} \text{ has odd parity} \end{cases}$$

This code detects an odd number of errors.

Applications of Error-Detecting Codes

Computer network communication protocols such as TCP/IP use error-detecting codes extensively to determine if data packets sent across a network have been corrupted or not.

Usual remedy for receipt of a corrupted data packet is to request retransmission.

Applications of Error-Detecting Codes

International Standard Book Number (ISBN):

- ISBN-10 numbers have 10 digits,
  and are of the form x-xxx-xxxxx-x.

  The digits used are $\{0,1,2,\ldots,9,X\}$, where X represents the number 10.

- The first nine digits in an ISBN record information about the book: country, publisher, title and edition;

- The tenth digit is a check digit.

Example: 0-444-85193-3

$$\begin{aligned} 10\times 0 \;+\; 9\times 4 \;+\; 8\times 4 \;+\; 7\times 4 \;+\; 6\times 8 \;+& \\ 5\times 5 \;+\; 4\times 1 \;+\; 3\times 9 \;+\; 2\times 3 \;+\; 1\times 3 \;&=\; 209 \\ &\equiv\; 0 \pmod{11} \end{aligned}$$

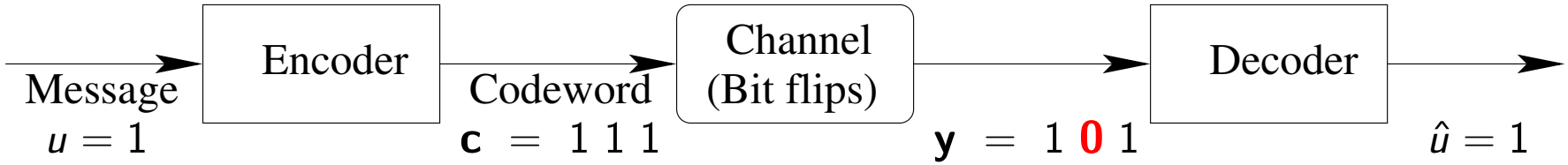
A Simple Error-Correcting Code

Channel Noise: Flips bits at random ($0 \to 1$, $1 \to 0$).

Message: Single bit, $b = 0$ or 1.

Encoder: $0 \mapsto 000$, $1 \mapsto 111$. Thus, rate $= 1/3$.

A Simple Error-Correcting Code



Channel Noise: Flips bits at random ($0 \to 1$, $1 \to 0$).

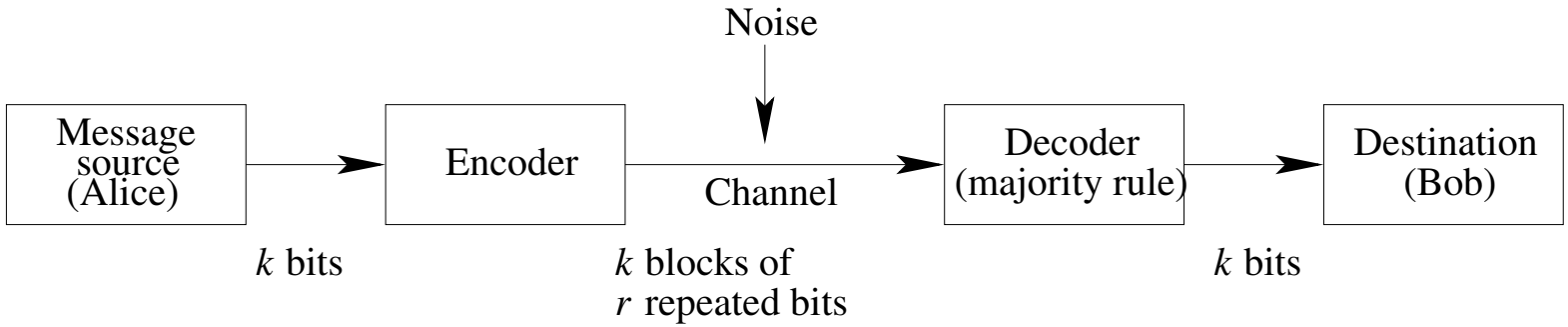
Message: Single bit, $b = 0$ or 1.

Encoder: $0 \mapsto 000$, $1 \mapsto 111$. Thus, rate $= 1/3$.

Decoder: Majority rule — if more 0s than 1s received, then decode as 0; else decode as 1.

This code can correct single errors, and detect (but not correct) double errors.

r-Fold Repetition Codes



Encoder: Repeats each message bit r times.

Decoder: Uses majority rule for each block of r received bits.

Coding Rate: $R = 1/r$

(1 message bit per r coded bits).

Error-Correction Capability: Up to $(r-1)/2$ errors in each block.

Error-Detection Capability: Up to $r-1$ errors in each block.

The Length-7 Hamming Code

Discovered by Richard Hamming (1950)

- Encodes a 4-bit message into a 7-bit codeword:

$$\underbrace{u_1\ u_2\ u_3\ u_4}_{\text{information bits}} \longmapsto u_1\ u_2\ u_3\ u_4\ \underbrace{p_1\ p_2\ p_3}_{\text{parity bits}}$$

- Thus, rate $= 4/7$.

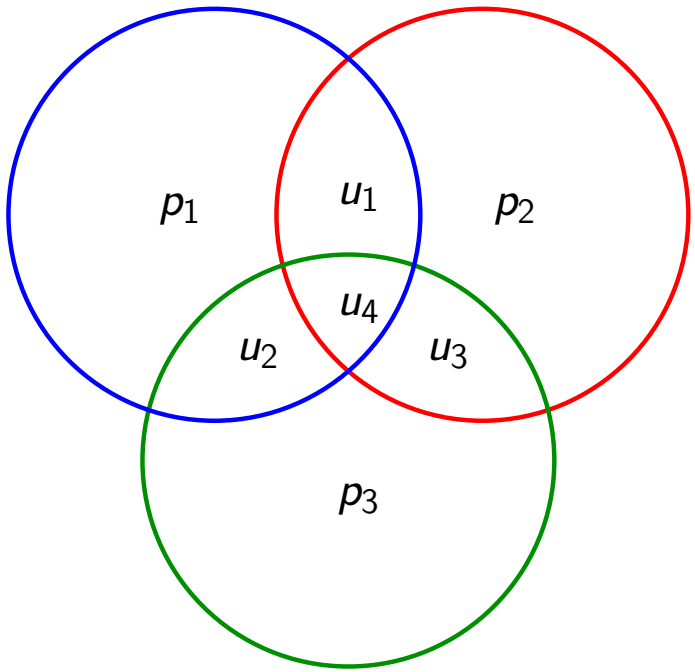
The Length-7 Hamming Code

Discovered by Richard Hamming (1950)

- Encodes a 4-bit message into a 7-bit codeword:

$$\underbrace{u_1\ u_2\ u_3\ u_4}_{\text{information bits}} \longmapsto u_1\ u_2\ u_3\ u_4\ \underbrace{p_1\ p_2\ p_3}_{\text{parity bits}}$$

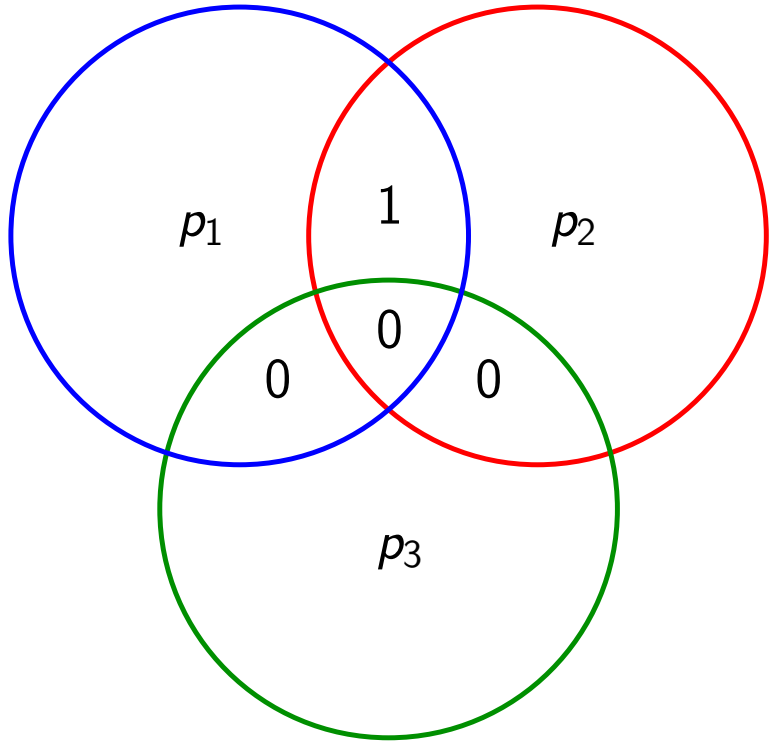
- Thus, rate $= 4/7$.



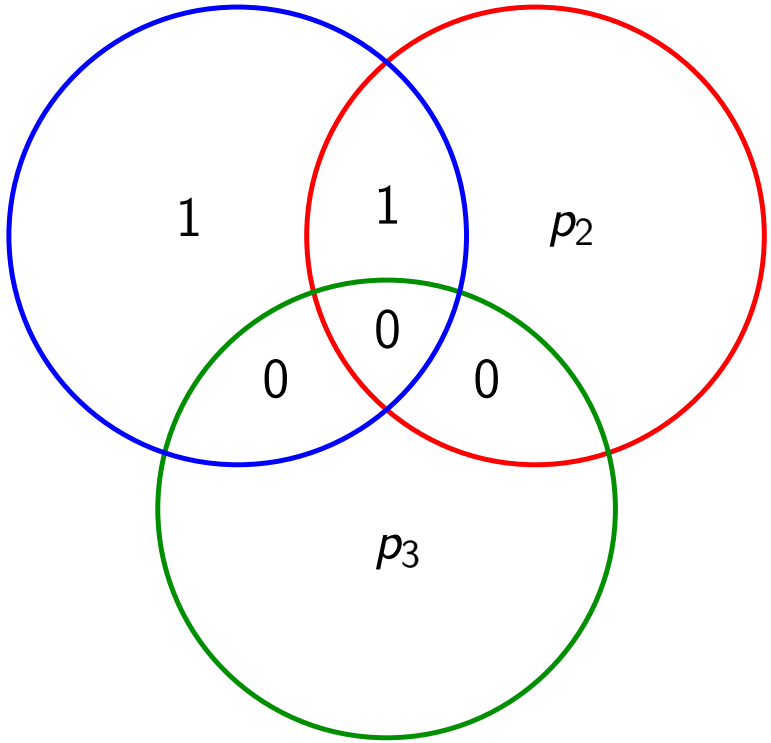
For each choice of (u_1, u_2, u_3, u_4), there is a unique choice of (p_1, p_2, p_3) that makes each circle have an even number of 1s.

$$u_1 + u_2 + u_4 + p_1 \equiv 0 \pmod 2$$
$$u_1 + u_3 + u_4 + p_2 \equiv 0 \pmod 2$$
$$u_2 + u_3 + u_4 + p_3 \equiv 0 \pmod 2$$

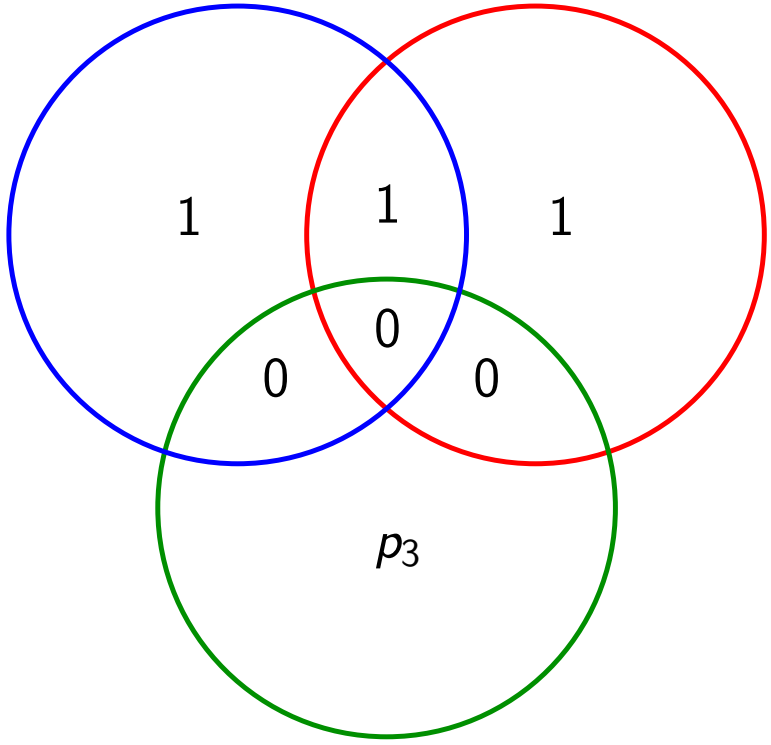
The Length-7 Hamming Code



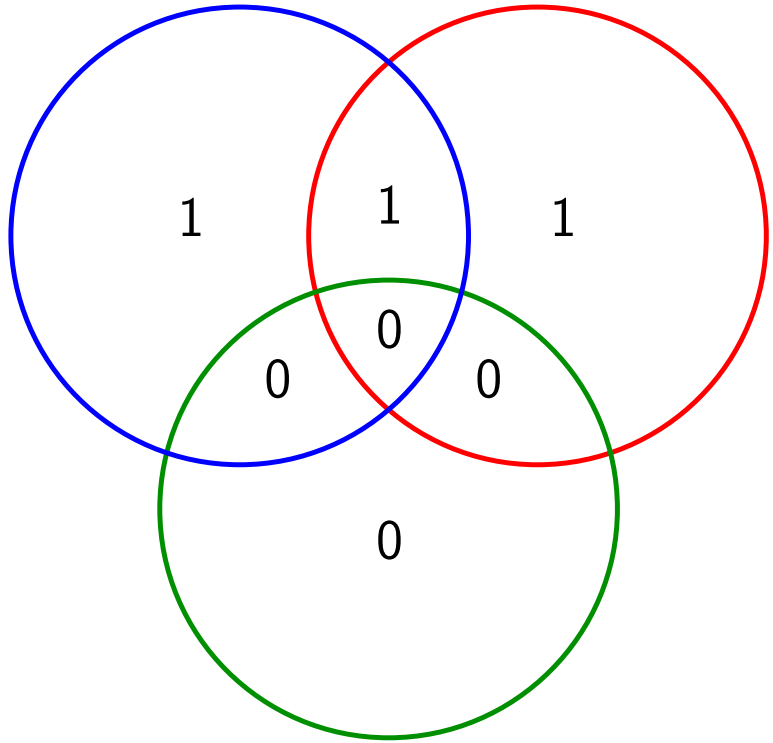
The Length-7 Hamming Code



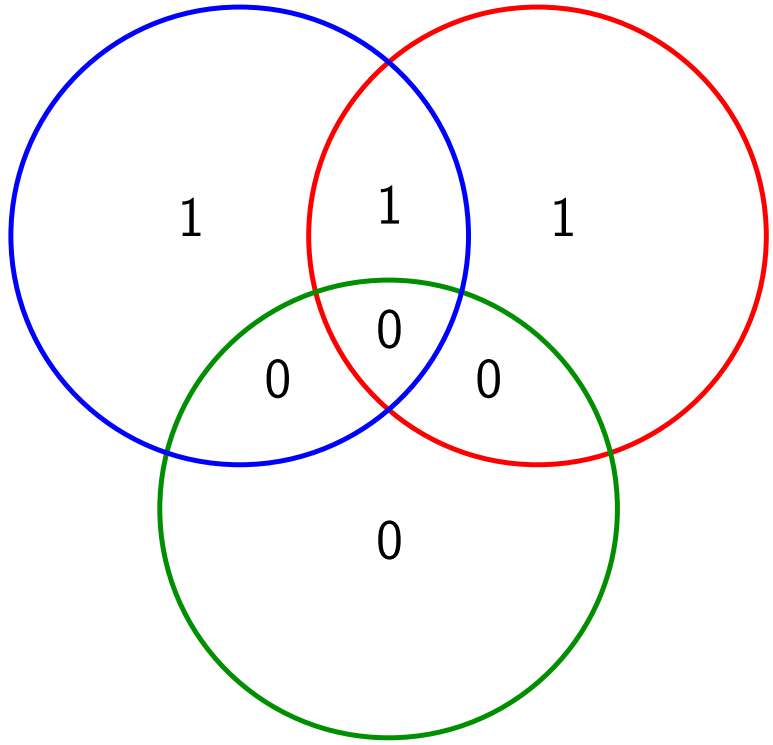
The Length-7 Hamming Code



The Length-7 Hamming Code



The Length-7 Hamming Code



$u_1\ u_2\ u_3\ u_4\ p_1\ p_2\ p_3\ =\ 1\ 0\ 0\ 0\ 1\ 1\ 0$
is a codeword of the Hamming code.

The Length-7 Hamming Code: Single-Error Correction

Encoder (Alice): $(u_1, u_2, u_3, u_4) \mapsto (u_1, u_2, u_3, u_4, p_1, p_2, p_3)$

Channel Noise: Flips bits at random ($0 \to 1$, $1 \to 0$).

The Length-7 Hamming Code: Single-Error Correction

Encoder (Alice): $(u_1, u_2, u_3, u_4) \mapsto (u_1, u_2, u_3, u_4, p_1, p_2, p_3)$

Channel Noise: Flips bits at random ($0 \to 1$, $1 \to 0$).

Suppose that Alice sends 1000110, but Bob receives 1100110:

$$1\ 0\ 0\ 0\ 1\ 1\ 0 \longrightarrow 1\ \mathbf{1}\ 0\ 0\ 1\ 1\ 0$$

The Length-7 Hamming Code: Single-Error Correction

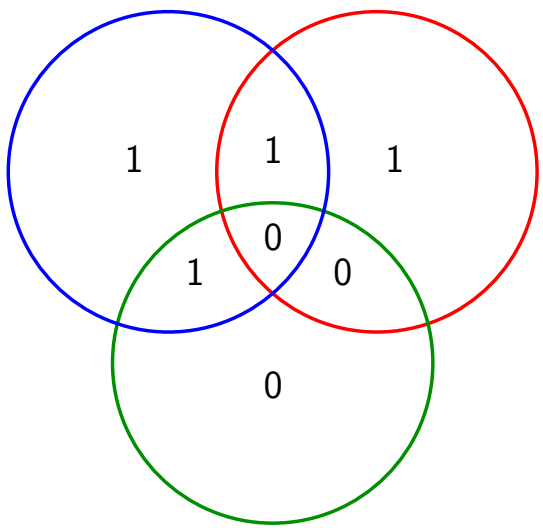
Encoder (Alice): $(u_1, u_2, u_3, u_4) \mapsto (u_1, u_2, u_3, u_4, p_1, p_2, p_3)$

Channel Noise: Flips bits at random ($0 \to 1$, $1 \to 0$).

Suppose that Alice sends 1000110, but Bob receives 1100110:

$$1\ 0\ 0\ 0\ 1\ 1\ 0 \longrightarrow 1\ \mathbf{1}\ 0\ 0\ 1\ 1\ 0$$

Decoder (Bob):



1. Identify circles with wrong parity
2. Flip bit common to those circles only

The Length-7 Hamming Code: Single-Error Correction

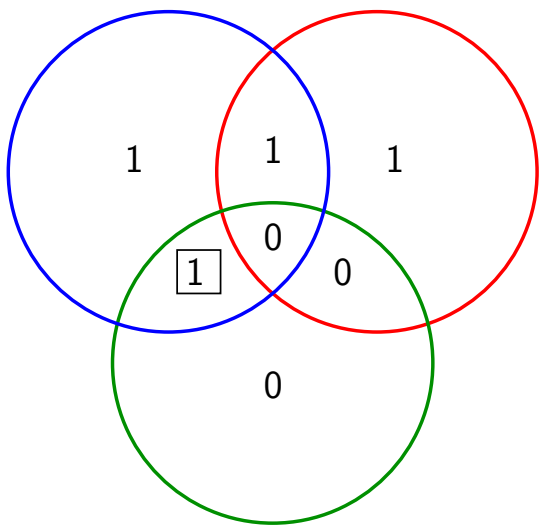
Encoder (Alice): $(u_1, u_2, u_3, u_4) \mapsto (u_1, u_2, u_3, u_4, p_1, p_2, p_3)$

Channel Noise: Flips bits at random ($0 \to 1$, $1 \to 0$).

Suppose that Alice sends 1000110, but Bob receives 1100110:

$$1\ 0\ 0\ 0\ 1\ 1\ 0 \longrightarrow 1\ 1\ 0\ 0\ 1\ 1\ 0$$

Decoder (Bob):



1. Identify circles with wrong parity
2. Flip bit common to those circles only

The Length-7 Hamming Code: Single-Error Correction

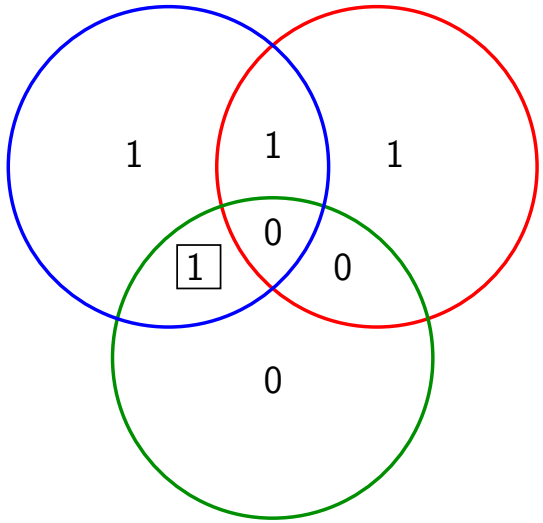
Encoder (Alice): $(u_1, u_2, u_3, u_4) \mapsto (u_1, u_2, u_3, u_4, p_1, p_2, p_3)$

Channel Noise: Flips bits at random ($0 \to 1$, $1 \to 0$).

Suppose that Alice sends 1000110, but Bob receives 1100110:

$$1\ 0\ 0\ 0\ 1\ 1\ 0 \longrightarrow 1\ 1\ 0\ 0\ 1\ 1\ 0$$

Decoder (Bob):



1. Identify circles with wrong parity
2. Flip bit common to those circles only

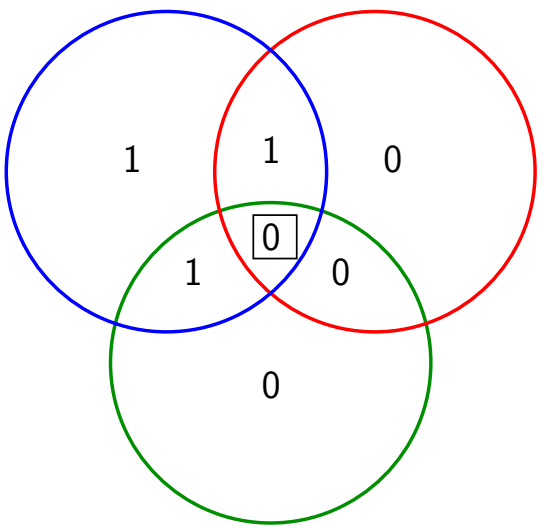
Single errors can be corrected.

The Length-7 Hamming Code: Multiple Errors

Suppose that Alice sends 1000110, but Bob receives 1100100:

$$1\,0\,0\,0\,1\,1\,0 \longrightarrow 1\,\mathbf{1}\,0\,0\,1\,\mathbf{0}\,0$$

Decoder (Bob):



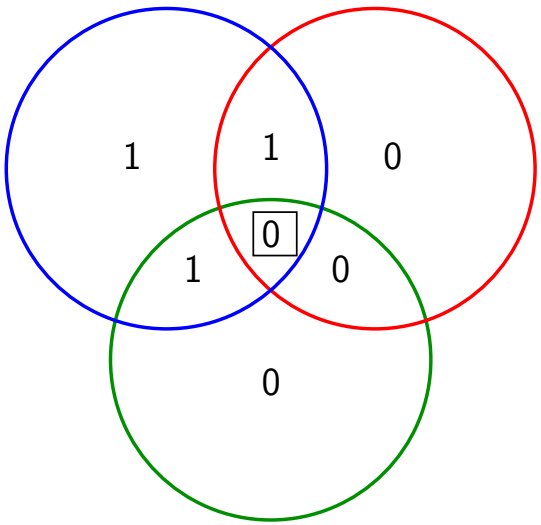
1. Identify circles with wrong parity
2. Flip bit common to those circles only

The Length-7 Hamming Code: Multiple Errors

Suppose that Alice sends 1000110, but Bob receives 1100100:

$$1\ 0\ 0\ 0\ 1\ 1\ 0 \longrightarrow 1\ \mathbf{1}\ 0\ 0\ 1\ \mathbf{0}\ 0$$

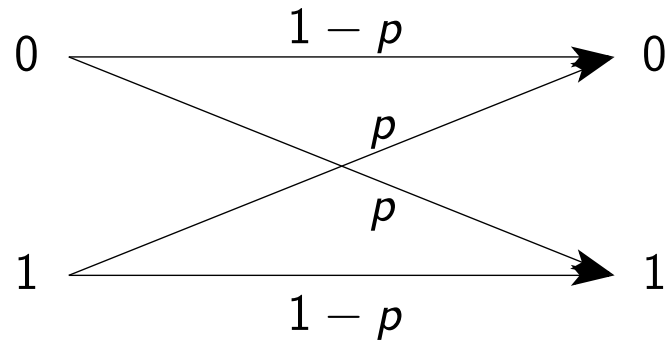
Decoder (Bob):



1. Identify circles with wrong parity
2. Flip bit common to those circles only

Decoded as 1 1 0 1 1 0 0. Multiple errors cannot be corrected.

Memoryless Binary Symmetric Channel



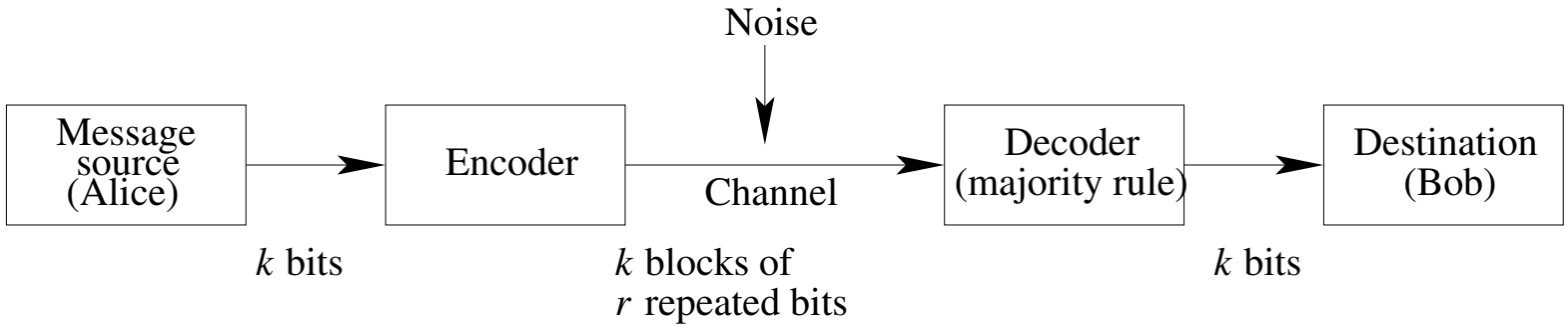
- Alice wants to send a k-bit message to Bob.
- The message is to be encoded and transmitted across a memoryless BSC.
- Each bit transmitted across the channel gets flipped with probability p, independently of other bits.
- For concreteness, $k = 10,000$ and $p = 0.001$.

Uncoded Transmission

- Rate $= 1$
- Probability that the entire k-bit message is recovered by Bob:

$$\begin{aligned} P_C &= (1-p)^k \\ &= 0.000045 \quad \text{for } k = 10,000 \text{ and } p = 0.001 \end{aligned}$$

Repetition Codes



The probability that a single message bit is decoded correctly is

$$P_{b,C} = \sum_{j=0}^{\lfloor \frac{r-1}{2} \rfloor} \binom{r}{j} p^j (1-p)^{r-j}$$

So, the probability that entire k-bit message is decoded correctly is

$$P_C = (P_{b,C})^k$$

$$\approx 0.97 \quad \text{for } k = 10,000,\ p = 0.001, \text{ and } r = 3$$

(Note: 30,000 coded bits are actually transmitted)

Length-7 Hamming Code

To transmit a k-bit message, we first divide the message into 4-bit blocks, encode each using a 7-bit codeword, and transmit.

Thus, $k/4$ codewords (i.e., $7k/4$ coded bits) are transmitted.

Length-7 Hamming Code

To transmit a k-bit message, we first divide the message into 4-bit blocks, encode each using a 7-bit codeword, and transmit.

Thus, $k/4$ codewords (i.e., $7k/4$ coded bits) are transmitted.

- The prob. that a transmitted 7-bit codeword is decoded correctly is

$$\begin{aligned}&\Pr[\text{at most one of the 7 bits is flipped}]\\ &\qquad = (1-p)^7 + 7p(1-p)^6\end{aligned}$$

- Hence, the prob. that the entire k-bit message is recovered correctly by Bob is

$$\begin{aligned}P_C &= \left[(1-p)^7 + 7p(1-p)^6\right]^{k/4}\\ &\approx 0.95 \quad \text{for } k = 10,000 \text{ and } p = 0.001\end{aligned}$$

Length-7 Hamming Code

To transmit a k-bit message, we first divide the message into 4-bit blocks, encode each using a 7-bit codeword, and transmit.

Thus, $k/4$ codewords (i.e., $7k/4$ coded bits) are transmitted.

- The prob. that a transmitted 7-bit codeword is decoded correctly is

$$\begin{aligned}&\Pr[\text{at most one of the 7 bits is flipped}]\\ &\qquad = (1-p)^7 + 7p(1-p)^6\end{aligned}$$

- Hence, the prob. that the entire k-bit message is recovered correctly by Bob is

$$\begin{aligned}P_C &= \left[(1-p)^7 + 7p(1-p)^6\right]^{k/4}\\ &\approx 0.95 \quad \text{for } k = 10,000 \text{ and } p = 0.001\end{aligned}$$

- $(7 \times 10000)/4 \;=\; 17,500$ coded bits are transmitted.

Shannon's Noisy Channel Coding Theorem

Channel Model: BSC with crossover probability p

BSC Channel Capacity: $C(p) = 1 + p \log_2 p + (1-p) \log_2 (1-p)$.

Theorem [Claude Shannon (1948)]:

If $R < C(p)$ and k is sufficiently large, there exists a code which can encode k message bits into $n = k/R$ coded bits to be transmitted across the channel, such that a decoder at the channel output can recover all k message bits correctly with probability close to 1.

Shannon's Noisy Channel Coding Theorem

Channel Model: BSC with crossover probability p

BSC Channel Capacity: $C(p) = 1 + p\log_2 p + (1-p)\log_2(1-p)$.

Theorem [Claude Shannon (1948)]:

If $R < C(p)$ and k is sufficiently large, there exists a code which can encode k message bits into $n = k/R$ coded bits to be transmitted across the channel, such that a decoder at the channel output can recover all k message bits correctly with probability close to 1.

- $C(0.001) \approx 0.9886$.

Shannon's Noisy Channel Coding Theorem

Channel Model: BSC with crossover probability p

BSC Channel Capacity: $C(p) = 1 + p \log_2 p + (1-p)\log_2(1-p)$.

Theorem [Claude Shannon (1948)]:

If $R < C(p)$ and k is sufficiently large, there exists a code which can encode k message bits into $n = k/R$ coded bits to be transmitted across the channel, such that a decoder at the channel output can recover all k message bits correctly with probability close to 1.

- $C(0.001) \approx 0.9886$.
- This means that, to ensure that a 10,000-bit message can be recovered correctly with prob. close to 1, it should be enough to transmit about $10000/0.9886 \approx 10{,}150$ coded bits!

The Goal of Coding Theory

The goal of coding theory is to design coding schemes that can approach Shannon's performance guarantees, while still being relatively easy to implement in practice.

Low complexity, good error-protection capability