What is Coding Theory and What is Cryptography?

The term **coding** is an overloaded and sometimes misunderstood term. Basically, there are three areas the term coding is associated with.

1. Data Compression: concerned with efficient encoding of source information so that it takes as little space as possible. This is possible by removing redundancy from the data. Source encoding is a part of Information Theory and we won't be dealing with it in this course.

2. Error-Correcting Codes: concerned with improving **reliability** of communication over **noisy** channels. This is achieved by adding redundancy.

3. Cryptography (or Cryptology) is concerned with **security, privacy** or **confidentiality** of communication over an insecure channel.

Over the past few decades, the term "coding theory" has become associated predominantly with error correcting codes. A good part of this course will be devoted to coding theory.

It is interesting to note that whereas cryptography strives to render data unintelligible to all but the intended recipient, error-correcting codes attempt to ensure data is decodable despite any disruptions introduced by the medium. Data compression and error correction also contrast one another in that the former involves compaction and the latter data expansion.
Question: Does error correction take place in human communication?

Basic Problem of Coding Theory

Messages are transmitted over a communication channel which is subject to noise. Noise can distort messages

Goals:

1. "Error detection"

2. "Error correction"

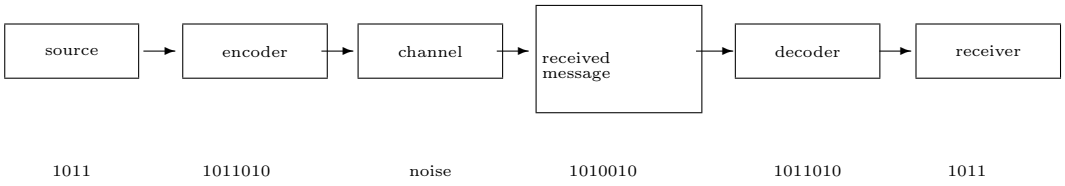
Question: How can we achieve these goals, efficiently?

Simple Examples

I) Duplicate the message to be sent.
$1011 \rightarrow 10111011$
Detect single errors, but no correction.
Cost: Rate = 1/2.

II) Add a parity check, so that there are even number of 1's, or sum of digits is 0 mod 2.
$1011 \rightarrow 10111$
Also detects single errors, no correction.
Cost: Rate = 4/5

Transmission Process of a Message



Applications and Some History of Coding Theory

Error Correcting Codes have a wide range of applications. Here is a list of some of the applications

- Transmission of pictures from distant space
- Quality of sound in CD's: "Reed-Solomon" codes are used in CD's.
- Telephone lines, computer networks
- Universal Product Codes, ISBN numbers
- Most recently, quantum error-correction
- Their uses are ever expanding

The beginning: Claude Shannon's 1948 paper "A Mathematical Theory of Communication" marks the birth of a new subject called "Information Theory", part of which is coding theory. He established the theoretical foundations of the subject. He showed that "good codes" (we will see in this course what that means) exist without showing them! His prove was probabilistic and existential, not constructive. It remained a big challenge to construct and implement efficient codes for a long time.

Richard Hamming was one of the first to actually construct and implement error correcting codes. He did this out of frustration he had due to Bell Lab's mechanical relay computer's inability to deal with errors. He said "Damn it, if the machine can detect an error, why can't it locate the position and correct it?". There is a class of codes known as Hamming Codes which we are going to study.

1965: Mariner 4 was the first spaceship to photograph another planet, taking 22 complete photographs of Mars. Each picture was broken down into 200×200 picture elements. Each element was assigned a binary 6-tuple representing one of 64 brightness levels from white (000000) to black (111111). Thus the total number of bits per picture was 240 000. Data was transmitted at the rate of 8.33 bits per second, so it took 8 hours to transmit a single picture!

1969-72: Much improved pictures of Mars were obtained by Mariners 6,7, and 9 (Mariner 8 was lost during launching). One reason for the improvement was the use of a powerful error-correcting code known as (32,64,16) Reed-Muller code. In this code a binary 6-tuple representing the brightness of a dot in the picture was encoded as binary codeword of length 32. The data transmission rate was increased from 8.33 to 16200 bits per second.

1976: Viking 1 landed on Mars and returned high quality *color* photographs. Surprisingly, the transmission of a color picture in the form of a binary data is almost as easy as transmission of a black-and-white one.

1979: High resolution color pictures of Jupiter and its moons were returned by Voyager 1.

1980: Voyager 1 returned the first high resolution pictures of Saturn and its moons.

....

A less obvious application of error-correcting codes came with the development of the compact disc in 1970's. On CDs the signal in encoded digitally. To guard against scratches, cracks and similar damage "cross interleaved Reed-Solomon codes" which can correct up to 4,000 consecutive errors (about 2.5 mm of track) are used. (Audio disc players can recover from even more damage by interpolating the signal.)

Cryptographic Applications

People have always had fascination with keeping information away from others. History is filled with examples where people tried to keep information secret from adversaries. Kings and generals communicated with their troops using basic cryptographic methods to prevent the enemy from learning sensitive military information. Julius Caesar reportedly used a simple cipher which has been named after him. In World War II, cryptography was a very important tool.

In this information age, the need to protect data is more pronounced than ever. As the world becomes more connected, the demand for information and electronic devices is growing and with the increased demand comes increased dependency on electronic systems. Already the exchange of sensitive information such as credit card number over the internet is common practice. Protecting data and electronic systems is crucial to our way of life.

Cryptography is not only about encrypting and decrypting messages, it is also about solving real-world problems that require information security. Here are some objectives that arise:

1. Confidentiality: Eve should not be able to read Alice's message to Bob. The main tools are encryption and decryption algorithms.

2. Data Integrity: Bob wants to make sure that Alice's message has not been altered. There are cryptographic techniques to detect data manipulation by malicious or accidental adversaries.

3. Authentication: Bob wants to make sure that only Alice could have sent the message he received.

4. Non-repudiation: Alice cannot claim that she did not send the message. Non-repudiation is particularly important in electronic commerce applications where it is important that a customer cannot deny the authorization of a purchase.

5. Secret Sharing: Suppose that you have a combination to a bank safe, but you do not want to trust any single person with the combination to the safe. Rather, you would like to divide the combination among a group of people so that at least two (or any other prescribed number) of these people must be present in order to open the safe.