Congruence modulo m (*review*)

Let x and y be integers.

> We say x is congruent to y modulo m,
> $$x \equiv y \pmod{m},$$
> if $x - y$ is an integer multiple of m.

E.g., $66 \equiv 38 \pmod{7}$, since $66 - 38 = 28 = 4 \times 7$.

If $x \equiv y \pmod{m}$, then x and y have the same remainder when divided by m:

$$66 \div 7 = 9 \text{ R } 3$$
$$38 \div 7 = 5 \text{ R } 3$$

and both are equivalent to the remainder: $66 \equiv 3 \equiv 38 \pmod{m}$.

Congruence classes

We say two integers are in the same congruence class if they are congruent modulo m.

We write $[x]$ for the congruence class containing x, that is, the set of integers congruent to x modulo m.

The set of congruence classes mod m are denoted by Z_m.

Z_m consists of m distinct classes: $[0], [1], [2], \ldots, [m-1]$.

The **International Standard Book Number (ISBN)**

A 10-digit ISBN $a_1 a_2 \cdots a_{10}$ has the property that

$$10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + a_{10}$$

is evenly divisible by 11; that is, $\equiv 0 \pmod{11}$.

Example

Determine the check digit which should be appended to ISBN 0-7167-9811.

$$10\times 0 + 9\times 7 + 8\times 1 + 7\times 6 + 6\times 7 + 5\times 9 + 4\times 8 + 3\times 1 + 2\times 1 + 1\times x = 237 + x$$

$237 \equiv 6 \pmod{11}$ since $237 \div 11 = 21$ R 6

To get $6 + x \equiv 0 \pmod{11}$, choose $x = 5$ for the check digit:

0-7167-9811-5

Error Detection with ISBN

Example: suppose an ISBN-10 is **1-4292-4580-8.**

$$10\times1 + 9\times4 + 8\times2 + 7\times9 + 6\times2 + 5\times4 + 4\times5 + 3\times8 + 2\times0 + 1\times8 = 209$$

Suppose the fourth digit is incorrectly read as **6**. Thus

$$10\times1 + 9\times4 + 8\times2 + 7\times6 + 6\times2 + 5\times4 + 4\times5 + 3\times8 + 2\times0 + 1\times8 = 188$$

and 188 is not a multiple of 11, indicating an error.

The difference between 209 and 188 is $21 = (9 - 6) \times 7$.

No single digit error can produce a difference that is a multiple of 11 and thus every single digit error will be detected!

Transposition Error and ISBN

Example: suppose an ISBN-10 is **1-4292-4580-8.**

$10\times1 + 9\times4 + 8\times2 + 7\times9 + 6\times2 + 5\times4 + 4\times5 + 3\times8 + 2\times0 + 1\times8 = 209$

If the fourth and fifth digits are transposed **1-4229-4580-8**. Then

$10\times1 + 9\times4 + 8\times2 + 7\times2 + 6\times9 + 5\times4 + 4\times5 + 3\times8 + 2\times0 + 1\times8 = 202$

and 202 is not a multiple of 11 indicating an error.

The difference between 209 and 202 is $7 = (7 - 6) \times (9 - 2)$.

No transposition error can produce a difference that is a multiple of 11 and thus all transposition errors will be detected!

Error-Detecting and Error- Correcting Codes

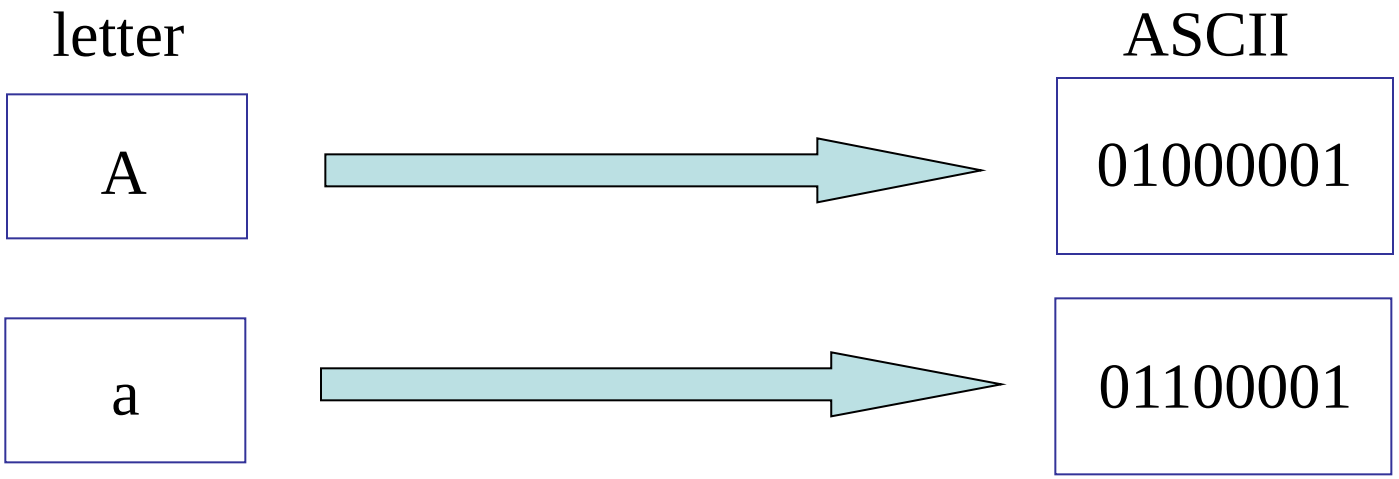
We consider some techniques to detect and correct errors in digitally transmitted messages.

- The basic unit of computer information is the **b**inary dig**it** or **bit.** A bit is either 0 or 1.
- Eight bits is a **byte.**
- Digital information is encoded as a sequence of bits known as “strings”. A systematic way of representing information as bits is referred to as a **Binary Code.** An example is the ASCII code.

ASCII Code

An example of a binary code is the ASCII code.

- ASCII stands for the American Standard Code for Information Interchange. ASCII is a code for representing English characters as 8 bit binary strings.



Binary Addition

- In working with binary digits and binary codes we often use a different “addition” table, the modulo 2 addition or “addition over Z_2”
- 0+0=0
- 1+0=1
- 0+1=1
- 1+1=0

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

+	even	odd
even	even	odd
odd	odd	even

Sum of Binary Sequences

$$\begin{array}{r} 11000111 \\ +\ 01110110 \\ \hline 10110001 \end{array} \qquad \begin{array}{r} 00111011 \\ +\ 01100101 \\ \hline 01011110 \end{array}$$

The sum has a “1” in every position where the strings differ and a “0” where they are the same.

Block Codes

- The number of bits in a codeword is the size or **length** of the codeword.
- If all of the codewords are the same length, we call the code a **block code.**
- Virtually all coding schemes involve taking a message part and adding extra binary digits called **"check digits"** to make the codewords.
- Check digits are used to detect, and sometimes correct, errors in transmission of the codewords.

Parity Check Digits

- The simplest way to add check digits to a binary message is to check whether of not the number of 1's in a binary message is even or odd. We call this checking for **"parity".**
- Example: In ASCII the message BAT is encoded as 01000010 01000001 01010100
- We can add a parity check digit to these blocks. We add a 0 if the message block has an even number of 1's, and a 1 if the message block has an odd number of 1's.

010000100 010000010 010101001

- An error in the first block would be detected by the parity check: 010100100 (three ones – odd)

Size and Efficiency of Block Codes

To have better capability to detect and correct errors, additional check digits can be added. For example, the single check digit in the preceding example would not be able to detect when two bits of the message were switched.

- If the original message words are ***k* bits long** and the added check digits make the encoded message ***n* bits long,** we say the that we have a **(*k*,*n*) block code.**
- The efficiency of a (*k*,*n*) block code is defined to be ***k*/*n***.
- Adding a parity check bit to every 8 bit ASCII string produces an (8,9) block code with efficiency 8/9.

Hamming Distance Between Two Strings in A Binary Code of Equal Length

---- the number of positions in which the strings differ.

Example: u = 1010110
v = 1000110

The Hamming distance between code words u and v is 1.

Example: u = 1000110
v = 0111001

The Hamming distance between code words u and v is 7.

Nearest-Neighbor Decoding

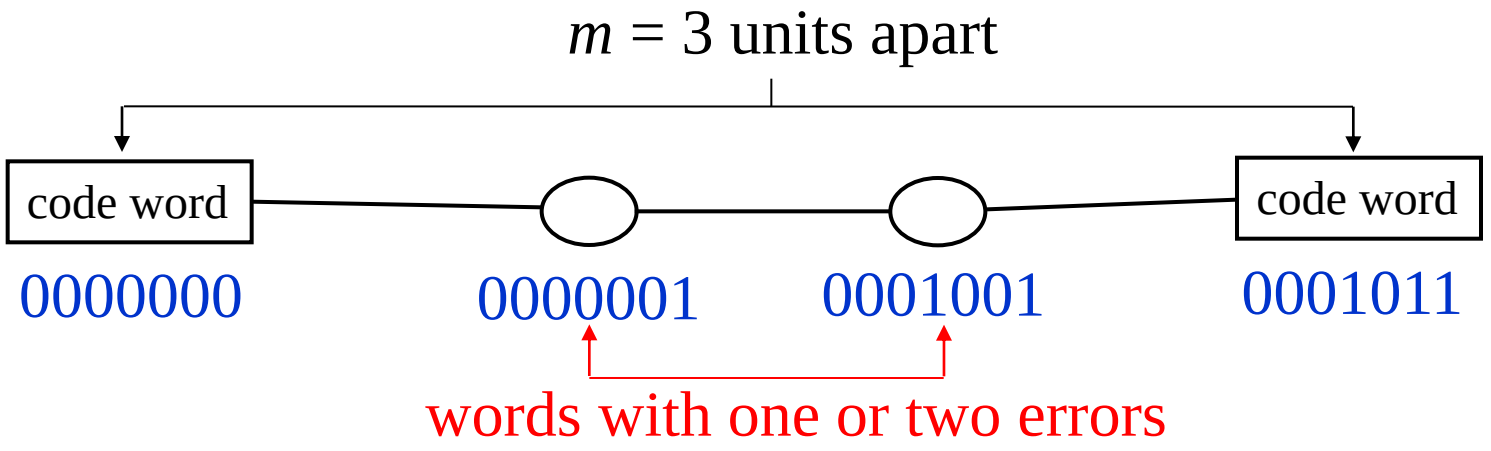
Method decodes a received message as the code word that agrees with the message in the most positions.

1. Compare the string with an error (call it *u*) to all other strings of the same length.
2. The string the least distance from *u* is taken as the true message.
3. If there is more than one possible answer, then the error cannot be decoded.

Error Detection

For a given set of block codes, let m be the minimum distance between two different codewords.

Error detection: the code can detect any $m - 1$ or fewer errors. For example:



Error Correction

Again, let m be the minimum distance between two different codewords. Then

- If m is odd, the code will correct any $(m - 1)/2$ or fewer errors;
- If m is even, the code will correct any $(m - 2)/2$ or fewer errors;