MATH 433

Applied Algebra

Lecture 32:
Error-detecting and error-correcting codes.
Binary codes.
Linear codes.

Error-detecting/correcting codes

Messages sent over electronic and other channels are subject to distortions of various sorts. Therefore it is important to encode a message so that a possible error can be detected. Then the receiver may ask that the message be repeated. Such codes are called **error-detecting**.

To achive this, the message should carry a certain degree of redundancy. One way to do this is a **checksum**. Namely, the sender adds to a message one or several check symbols, which are functions of the message. Then the receiver reevaluates these additional symbols.

In some cases, requesting that the message be repeated is too expensive. For such cases, we need a code that not only can detect an error, but also allows to correct it. Such codes are called **error-correcting**.

ISBN

International Standard Book Number (**ISBN**) is assigned to all published books. It is an example of an error-detecting code.

- ISBN-10 (old standard) consists of 9 decimal digits that constitute the number followed by a check symbol, which is a digit in base 11 (0–9 or X, the Roman notation for 10).

If $a_1 a_2 \ldots a_9 a_{10}$ is the number, then

$$10a_1 + 9a_2 + 8a_3 + \cdots + 3a_8 + 2a_9 + a_{10}$$

is to be divisible by 11. This happens for a unique choice of a_{10}.

The code allows to detect one wrong digit or exchange of two digits.

Example. 0 521 54050 X (ISBN-10 of the textbook).

ISBN

- ISBN-13 (new standard) consists of 13 decimal digits, the last one being a checksum. If $b_1 b_2 \dots b_{12} b_{13}$ is the number, then $b_1 + 3b_2 + b_3 + 3b_4 + \cdots + 3b_{12} + b_{13}$ is to be divisible by 10. This happens for a unique choice of b_{13}.

The code allows to detect one wrong digit or exchange of two neighboring digits.

Old numbers are converted into new ones by adding 978 at the beginning and recalculating the checksum.

Example. ISBN-10 of the textbook is 052154050X. Therefore ISBN-13 of the textbook is 978-052154050d, where

$$9 + 3\cdot 7 + 8 + 3\cdot 0 + 5 + 3\cdot 2 + 1$$
$$+ 3\cdot 5 + 4 + 3\cdot 0 + 5 + 3\cdot 0 + d \equiv 0 \mod 10.$$

We obtain that $d = 6$.

Problem 1. Find the missing digit in an ISBN-10: 04*5011614.

Let d be the missing digit. Then

$$10 \cdot 0 + 9 \cdot 4 + 8d + 7 \cdot 5 + 6 \cdot 0 + 5 \cdot 1 \\ + 4 \cdot 1 + 3 \cdot 6 + 2 \cdot 1 + 4 \equiv 0 \mod 11,$$

which simplifies to $8d + 5 \equiv 0 \mod 11$. The inverse of 8 modulo 11 is 7 (as $7 \cdot 8 = 56 \equiv 1 \mod 11$). It follows that $d \equiv 7 \cdot (-5) \equiv 9 \mod 11$. Thus $d = 9$.

Problem 2. Could this be a valid ISBN-13: 978-0495022613 ?

$$9 + 3 \cdot 7 + 8 + 3 \cdot 0 + 4 + 3 \cdot 9 + 5 \\ + 3 \cdot 0 + 2 + 3 \cdot 2 + 6 + 3 \cdot 1 + 3 \equiv 4 \not\equiv 0 \mod 10,$$

therefore this could not be a valid ISBN-13.

Binary codes

Let us assume that a message to be transmitted is in binary form. That is, it is a word in the alphabet $\mathbf{B} = \{0, 1\}$. For any integer $k \geq 1$, the set of all words of length k is identified with $\mathbf{B}^k$.

A **binary code** (or a **binary coding function**) is an injective function $f : \mathbf{B}^m \to \mathbf{B}^n$.

For any $w \in \mathbf{B}^m$, the word $f(w)$ is called the **codeword** associated to w.

The code f is **systematic** if $f(w) = wu$ for any $w \in \mathbf{B}^m$ (that is, w is the beginning of the associated codeword). This condition clearly implies injectivity of the function f.

Encoding / decoding

The code $f : \mathbf{B}^m \to \mathbf{B}^n$ is used as follows.

Encoding: The sender splits the message into words of length m: $w_1, w_2, \ldots, w_s$. Then he applies f to each of these words and produces a sequence of codewords $f(w_1), f(w_2), \ldots, f(w_s)$, which is to be transmitted.

Decoding: The receiver obtains a sequence of words of length n: $w_1', w_2', \ldots, w_s'$, where w_i' is supposed to be $f(w_i)$ but it may be different due to errors during transmission. Each w_i' is checked for being a codeword. If it is, $w_i' = f(w)$, then w_i' is decoded to w. Otherwise an error (or errors) is detected. In the case of an error-correcting code, the receiver attempts to correct w_i' by applying a correction function $c : \mathbf{B}^n \to \mathbf{B}^n$, then decodes the word $c(w_i')$.

Examples. • Parity bit.

$f : \mathbf{B}^m \to \mathbf{B}^{m+1},\ f(w) = wx,$ where x is the parity bit of w, which means that $x = 0$ if there is an even number of 1's in w and $x = 1$ otherwise. The number of 1's in any codeword is even. This code detects any single error (or an odd number of errors), but correction is not possible.

• Tell three times.

$f : \mathbf{B}^m \to \mathbf{B}^{3m},\ f(w) = www.$

This code detects two errors (for sure) and also can correct one error (using "split decision").

We say that a binary code **detects** k **errors** if a wrong word is detected whenever there are k or fewer errors. We say that the code **corrects** k **errors** if the correction is successful whenever there are k or fewer errors.

The distance $d(w_1, w_2)$ between binary words w_1, w_2 of the same length is the number of positions in which they differ. The **weight** of a word w is the number of nonzero digits, which is the distance to the zero word.

Theorem Let $f : \mathbf{B}^m \to \mathbf{B}^n$ be a coding function. Then **(i)** f allows detection of k or fewer errors if and only if the minimum distance between distinct codewords is at least $k+1$; **(ii)** f allows correction of k or fewer errors if and only if the minimum distance between distinct codewords is at least $2k+1$.

The correction function c is usually chosen so that $c(w)$ is the codeword closest to w.

Linear codes

The binary alphabet $\mathbf{B} = \{0, 1\}$ is naturally identified with $\mathbb{Z}_2$, the field of 2 elements. Then $\mathbf{B}^n$ can be regarded as the n-dimensional vector space over the field $\mathbb{Z}_2$.

A binary code $f : \mathbf{B}^m \to \mathbf{B}^n$ is **linear** if f is a linear transformation of vector spaces. Any linear code is given by a **generator matrix** G, which is an $m \times n$ matrix with entries from $\mathbb{Z}_2$ such that $f(w) = wG$ (here w is regarded as a row vector). For a systematic code, G is of the form $(I_m|A)$.

Theorem If $f : \mathbf{B}^m \to \mathbf{B}^n$ is a linear code, then
- the set W of all codewords forms a subspace (and a subgroup) of $\mathbf{B}^n$;
- the zero word is a codeword;
- the minimum distance between distinct codewords is equal to the minimum weight of nonzero codewords.

Examples. • Parity bit.

$f : \mathbf{B}^3 \to \mathbf{B}^4,\ f(w) = wx,$ where x is the parity bit of w.
This code is linear. The generator matrix is

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Observe that consecutive rows of G are $f(100),\ f(010),$ $f(001)$.

• Tell three times.

$f : \mathbf{B}^2 \to \mathbf{B}^6,\ f(w) = www.$
This code is also linear. The generator matrix is

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Consecutive rows of G are $f(10)$ and $f(01)$.