Vector Spaces

Applications to Coding Theory

Prof.dr. Ferucio Laurențiu Țiplea

Spring 2022

Department of Computer Science
"Alexandru Ioan Cuza" University of Iași
Iași 700506, Romania

e-mail: ferucio.tiplea@uaic.ro

Outline

Information transmission

Error detection and correction

Error detecting and correcting codes

Linear codes

Reading and exercise guide

Information transmission

Information transmission

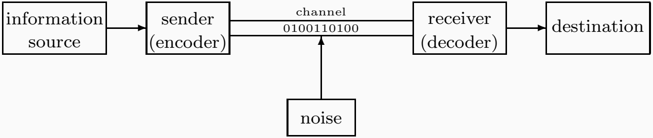
Entities involved in information transmission:

- sender (encoder);
- receiver (decoder);
- channel.

Examples of entities involved in information transmission:

- satellite station, Earth station, atmosphere;
- emission device, reception device, telephone cable.

Noise



Main question: develop codes capable of error detection and correction.

Binary symmetric channels

We will use only bloc binary codes.

Transmission channels can be classified into:

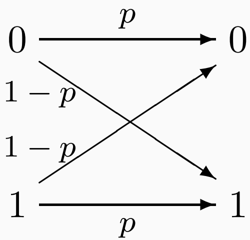
- noiseless channels (also called perfect channels);
- noise channels, which can be
  - symmetric – the probability that a bit is (correctly) received is the same for both bits;
  - asymmetric – it is not symmetric.

We will use only binary symmetric channels (BSC). Basic assumptions about them:

- BSCs do not change the length of the binary sequence transmitted through them;
- receiving order of the bits = sending order of the bits.

Reliability of a BSC

The reliability of a BSC is a real number $p \in (0, 1)$ which gives the probability that the bit b received is the bit b sent.



We may consider only BSCs with reliability $1/2 < p < 1$.

Information rate

Let $C_1 = \{00, 01, 10, 11\}$. With such a code, no error can be detected (but they may occur).

Let $C_2 = \{000, 011, 101, 110\}$ (obtained from C_2 by adding the parity bit). With such a code, any singular error is detected.

Definition 1

The information ratio of a code C of length n is

$$ir(C) = \frac{log_2|C|}{n}.$$

Example 2

$ir(C_1) = 1$ and $ir(C_2) = 2/3$.

Error detection and correction

The effect of error detection and correction

Example 3

Consider a BSC with reliability $p = 1 - 10^{-8}$ and transmission rate 10^7 bits/sec.

- Let $C = \{0,1\}^{11}$. A simple computation shows that
$$\frac{11}{10^8} \cdot \frac{10^7}{11} = 0.1 \text{ code words/sec}$$
with exact one undetected error will be transmitted. This means 8640 code words/day !!!
- Let C' be obtained from C by adding the parity bit. A simple computation shows that
$$\frac{66}{10^{16}} \cdot \frac{10^7}{12} \approx \frac{5.5}{10^9} \text{code words/sec}$$
with undetected errors will be transmitted. This means a code word/2000 days !!!

Minimum distance decoding – Maximum likelihood decoding

Let C be a code of length n. Assume that $w \in \{0,1\}^n$ was received. How do we decode w?

Minimum distance decoding (MDD): choose $v \in C$ to minimize d, the number of positions on which v and w disagree.

Maximum likelihood decoding (MLD): choose $v \in C$ to maximize the probability that v was sent when w was received. This probability is

$$\phi_p(v,w) = p^{n-d}(1-p)^d,$$

where p is the channel reliability and d is as above.

Example 4

Let C be a code of length 5 and p the channel reliability. If $10101 \in C$, then

$$\phi_p(10101, 01101) = p^3(1-p)^2.$$

MDD and MLD are equivalent

Theorem 5

Let C be a code of length n, $v_1, v_2 \in C$, and $w \in \{0,1\}^n$, and d_1 (d_2) be the number of positions on which v_1 and w (v_2 and w, respectively), disagree. Then,

$$\phi_p(v_1, w) \leq \phi_p(v_2, w) \quad \Leftrightarrow \quad d_1 \geq d_2$$

(it is assumed that the channel reliability satisfies $1/2 < p < 1$).

Proof.

See textbook [1], page 374. $\square$

Error detecting and correcting codes

Hamming weight and distance

We will work exclusively with the vector space F_2^n, where $F_2 = \mathbb{Z}_2$. Vector addition and scalar multiplication are given by:

- $x_1 \cdots x_n + y_1 \cdots y_n = (x_1 + y_1) \cdots (x_n + y_n)$;
- $\alpha(x_1 \cdots x_n) = (\alpha \cdot x_1) \cdots (\alpha \cdot x_n)$,

where $\alpha, x_i, y_i \in F_2$, $x_i + y_i$ is the addition modulo 2, and $\alpha \cdot x_i$ is given by

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0 \text{ and } 1 \cdot 1 = 1.$$

Definition 6

Let $v \in \{0,1\}^*$. The Hamming weigth of v, denoted $Hw(v)$, is the number of 1s in v.

Definition 7

Let $v, w \in \{0,1\}^n$, for some n. The Hamming distance of v and w, denoted $Hd(v,w)$, is $Hd(v,w) = Hw(v+w)$.

Properties of the Hamming weight

Prove the following properties!

Proposition 8

For any $n \geq 1$, $u, v, w \in \{0,1\}^n$, *and* $a \in \{0,1\}$, *the following hold:*

1. $0 \leq Hw(v) \leq n$;
2. $Hw(v) = 0$ *iff* $v = 0$;
3. $0 \leq Hd(v, w) \leq n$;
4. $Hd(v, w) = 0$ *iff* $v = w$;
5. $Hd(v, w) = Hd(w, v)$;
6. $Hw(v + w) \leq Hw(v) + Hw(w)$;
7. $Hd(v, w) \leq Hd(v, u) + Hd(u, w)$;
8. $Hw(av) = aHw(v)$;
9. $Hd(av, aw) = aHd(v, w)$.

Code distance and transmission error

Definition 9

Let C be a code. The distance of C, denoted $d(C)$, is

$$d(C) = min\{Hd(v, w) | v, w \in C,\ v \neq w\}.$$

Example 10

1. For the code $C = \{00110011, 01101101, 01010110\}$, $d(C) = 4$
2. For the code $C = \{00110011, 01101101, 01010110, 01010011\}$, $d(C) = 2$

A transmission error for a code C of length n is any non-zero vector e of length n (that is, $e \in \{0, 1\}^n - \{0^n\}$).

Error detecting codes

Definition 11

Let C be a code of length n.

1. C detects the error $e \in \{0,1\}^n - \{0^n\}$ if $v + e \not\in C$, for any $v \in C$.
2. C is a t-detector code if C detects any error with Hamming weight at most t, but there exists an error with Hamming weight $t+1$ that cannot be detected by C.

Theorem 12

Let C be a code of length n and distance d. Then,

1. *C detects all errors $e \in \{0,1\}^n - \{0^n\}$ with $Hw(e) \leq d-1$;*
2. *There exists at least one error $e \in \{0,1\}^n - \{0^n\}$ with $Hw(e) = d$ that cannot be detected by C.*

Proof.

See textbook [1], pages 377-378. □

Error correcting codes

Definition 13

Let C be a code of length n.

1. C corrects the error $e \in \{0,1\}^n - \{0^n\}$ if $Hd(v+e,v) < Hd(v+e,w)$, for any $v \in C$ și $w \in C - \{v\}$.
2. C is a t-corrector code if C corrects all errors with Hamming weight at most t, but there exists at least one error with Hamming weight $t+1$ that cannot be corrected by C.

Theorem 14

Let C be a code of length n and distance d. Then:

1. *C corrects all errors $e \in \{0,1\}^n - \{0^n\}$ with $Hw(e) \leq \lfloor (d-1)/2 \rfloor$;*
2. *There exists at least one error $e \in \{0,1\}^n - \{0^n\}$ with $Hw(e) = \lfloor (d-1)/2 \rfloor + 1$ that cannot be corrected by C.*

Proof.

See textbook [1], pages 377-378. □

Linear codes

Linear codes

Definition 15

Let $\mathbb{F}_q$ be a finite field with q elements. A linear code of length $n \geq 1$ and rank k over $\mathbb{F}_q$, where $1 \leq k \leq n$, also called an $[n, k]$-code over $\mathbb{F}_q$, is a subspace of dimension k of the vector space $\mathbb{F}_q^n$.

If C is an $[n, k]$-code of distance d over $\mathbb{F}_q$, we will also say that C is an $[n, k, d]$-code over $\mathbb{F}_q$.

Any $[n, k]$-code can be specified by a basis B of cardinality k. This basis can be arranged into a matrix $G \in \mathcal{M}_{k,n}(\mathbb{F}_q)$ whose rows are B's vectors. G is called a generating matrix of C.

Encoding by linear codes

Let C be a $[7,4]$-code over $\mathbb{F}_2$ given by the generating matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

To encode $x_1 = (1,1,1,0)$ we compute

$$x_1 G = (1,1,1,0,1,0,0)$$

and to encode $x_2 = (1,0,1,0)$ we compute

$$x_2 G = (1,0,1,0,0,1,1)$$

Dual code and parity check matrix

Definition 16

Let C be an $[n,k]$-code over $\mathbb{F}_q$. The dual code of C, denoted $C^\perp$, is the set of all vectors that are orthogonal on C.

Clearly, $C^\perp$ is an $[n, n-k]$-code over $\mathbb{F}_q$.

A generator matrix for the dual code is called a parity-check matrix for the original code and vice versa. If H is such a matrix, then

$$C = \{v \in \mathbb{F}_q^n | Hv^t = 0\}$$

Proposition 17

If $G = (I_k \ A)$ *is a generating matrix of an* $[n,k]$*-code, then* $H = (-A^t \ I_{n-k})$ *is a parity check matrix of the code.*

Proof.

See textbook [1], pages 390-391. □

Syndrome decoding

Given $y \in \mathbb{F}_q^n$, Hy^t is called the syndrome of y. Therefore, C is the set of all vectors whose syndrome is 0.

Any code of length n induces an equivalence relation on $\mathbb{F}_q^n$:

$$u \sim_C v \quad \Leftrightarrow \quad v - u \in C$$

Clearly, all elements in the same equivalence class have the same syndrome.

Syndrome decoding works as follows:

1. Compute the syndrome of y, $s = Hy^t$;
2. Find the equivalence class where y belongs to and take the minimum-weight vector e in it. e is interpreted as the error;
3. Return $v = y - e$.

Syndrome decoding

Let C be the code given by the generating matrix

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

A parity check matrix for C is

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Assume that $x = (1,1,0)$ is encoded and the error $e = (0,1,0,1,0)$ occurred during transmission. Therefore, the received vector is

$$xG + e = (1,1,0,1,0) + (0,1,0,1,0) = (1,0,0,0,0) = y.$$

The syndrome of y is $Hy^t = (1,1) = s$. One can check that the minimum-weight vector in the equivalence class corresponding to s is e. So, we decode y by $y - e = x$.

Reading and exercise guide

Reading and exercise guide

It is highly recommended that you do all the exercises marked in red from the slides.

Course readings:

1. Pages 368-391 from textbook [1].

References

[1] Ferucio Laurențiu Țiplea. *Algebraic Foundations of Computer Science*. "Alexandru Ioan Cuza" University Publishing House, Iași, Romania, second edition, 2021.