Error-Correcting Codes - Hand out

Monika Zweifel

March 16, 2021

Contents

1 Introduction

Why do we need to do error-correction in codes?

What is the general design of a transmission or a storage system:
Typically such a system contains an information source, such as a human speaker, that produces a message. This message is then transformed into a signal by a transmitter. The signal is sent through a channel where there is some noise. Therefore the signal that is received by the receiver can differ from the sent one. The receiver then re-transform the signal into a message for the destination.

This is where the error-correcting codes come into play. The problem we want to solve is how the messages can be transformed into codes by the transmitter, such that receiver gets the correct message even if the code has been changed slightly by the noise.

2 definitions

First we need some definitions:

Definition 2.1 (Various Definitions)**.**

- *Let F be a finite field. A **code** C over F of lenght n is simply a subset of F^n.*
- *A **codeword** of C has the form $u = (u_1, u_2, \ldots, u_n)$, where $u_i \in F$.*

- *More generally, a code is a system of rules to convert information into another form for communication through a communication channel or storage in a storage medium.*

- *The **Hamming distance** between two codewords u and v of C is the number of coordinates at which they differ, and is denoted by $\|u, v\|_H$ or $d(u, v) = |\{i : u_i \neq v_i\}|$.*

- *The **(Hamming) weight** of a codeword u, $w(u)$, is the number of its nonzero coordinates. Thus,*
$$\|u, v\|_H = w(u - v).$$

- *The **minimal distance** of a code is*
$$d = \min\{d(u, v) : u, v \in C, u \neq v\}$$

- *A code of length n, containing M codewords and with minimal distance d is said to be an **(n,M,d) code**.*

- *A linear code C is a **linear subspace** of F_q^n, i.e. whenever $u, v \in C$, then also $\mu u + \nu v \in C$ holds. A linear code of length n, dimension k and minimal distance d is said to be an **[n,k,d] code** (or sometimes an **[n,k] code**).*
The minimal distance of a linear code is the minimal nonzero weight of any codeword:
$$d = \min\{w(u) : u \in C, u \neq 0\}$$

- *The **dimension k** of a linear code C is the dimension of the subspace C, and there are q^k codewords. ($q = card\{F\}$)*

- *A code C over F is called **cyclic** if whenever $(u_0, u_1, \ldots, u_{n-1})$ is a codeword so is $(u_{n-1}, u_0, u_1, \ldots, u_{n-2})$. (A cyclic code is a priori assumed to be linear.*

- *The **rate** of the code C is*
$$R = \frac{1}{n}\log_2[M] = \frac{k}{n}\log_2 q \quad \textit{bits/symbol}$$

- *A **constant weight code** is one in which all codewords have equal weight.*

Remark. *If a code has minimal distance d, the Hamming spheres of radius $\rho = [\frac{1}{2}(d-1)]$ around the codewords are disjoint (so ρ is the packing radius of the code), and therefore the code can correct ρ errors.*

3 Statement of the Problem

In a good code n is small, M is large and d is large. Naturally, these goals are incompatible. The error-correcting code problem is the following:
Given n and d, find $M(F, n, d)$, the maximum number of codewords in any code over F. When $F = \{0, 1\}$, determining $M(F, n, d)$ is also an interesting geometric problem.

To find solutions for these problems, it is convenient to represent a codeword $u = (u_0, u_1, \ldots, u_{n-1})$ by the polynomial

$$f(x) = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1}$$

in the ring $F_n[x]$ of polynomials modulo $x^n - 1$. Then $xf(x)$ represents a cyclic shift of u, and so a linear cyclic code is represented by an ideal in $F_n[x]$. From algebra we know, that this ideal can be generated by a single polynomial $g(x)$, a **generator polynomial** of the code. $g(x)$ divides $x^n - 1$ over F and the dimension of C is $k = n - \deg g(x)$.

4 Some important codes

First of all, some general principles for cyclic codes. Let n be relatively prime to q, and let ξ be a primitive nth root of unity, so that

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \xi^i).$$

If l is the multiplicative order of q modulo n, then $\xi \in F'$ where F' is a suitable finite field of q^l elements. Also,

$$g(x) = \prod_{j \in J} (x - \xi^j)$$

for some set $J \subseteq \{0, 1, \ldots, n-1)\}$.

Binary Hamming Codes Let $n = 2^l - 1,\ k = n - l,\ d = 3$, and $J = \{1, 2, \ldots, 2^{l-1}\}$. Then the corresponding $g(x)$ generates a binary Hamming code (a $[2^m - 1, n - m, 3]$ code) $\mathcal{H}_n$ over $F = \{0, 1\}$.

Reed-Solomon codes The Reed-Solomon codes are a special case of the Bose-Chaudhuri-Hocquenghem-Codes. The BCH code $\mathcal{B}_{n,d}$ of length n and designed distance d over F is the cyclic code whose generator polynomial $g(x)$ has roots exactly $\xi, \xi^2, \xi^3, \ldots, \xi^{d-1}$ and their conjugates. The actual minimal distance between codewords is at least the designed distance and may exceed it ($d(\mathcal{B}_{n,d}) \geq d$).
The BCH codes over F of length $q - 1$, where $q = card\{F\}$, are called Reed-Solomon codes (a $[q - 1, k, n - k + 1]$ code). In these cases, $d(\mathcal{B}_{n,d}) = d$.

Reed-Muller codes Let $m(k)$ be the number of ones in the binary expansion of k. For $1 \leq j \leq l - 2$, the jth-order binary punctured Reed-Muller code $\mathcal{M}_n$ of length $n = 2^l - 1$ is the cyclic code whose generator polynomial has as roots those ξ^k such that

$$1 \leq k \leq 2^l - 2 \quad \text{and} \quad 1 \leq m(k) \leq l - j - 1$$

where ξ is a primitive element of F. Then, we define

$$\mathcal{M}_{n+1} = \left\{ (u_1, \ldots, u_{n+1}) : (u_1, \ldots, u_n) \in \mathcal{M}_n,\ \sum_{i=1}^{n+1} u_i = 0 \right\}$$

and call it the jth-order Reed-Muller code (a $[2^l, \sum_{i=0}^{j} \binom{l}{i}, 2^{l-j}]$ code) of length $n+1 = 2^l$.

5 Sphere Packings and lattices from codes

Construction A

Theorem 5.1. *Let C be an (n,m,d) binary code, and let h(t) be the number of its codewords u such that* $\|u, 0\|_H = t$. *Define*

$$X = \{x \in E^n : x(\mathrm{mod}\ 2) \in C \sum_{i=1}^{n} x_i \in 4\mathbb{Z}\}$$

$$r = \begin{cases} \frac{\sqrt{d}}{2} & \text{if } d \leq 8, \\ 2 & \text{if } d \geq 8, \end{cases} \quad \text{and}$$

$$\tau = \begin{cases} 2^{d-1}h(d) & \text{if} d < 8, \\ 2n(n-1) + 2^7 h(8) & \text{if} d = 8, \\ 2n(n-1) & \text{if} d > 8. \end{cases}$$

Then $rS_n + X$ *is a periodic packing with density*

$$\delta(rS_n, X) = \frac{m\omega_n r^n}{2^{n+1}},$$

in which the sphere rS_n *touches* τ *others.*
In particular, X is a lattice if and only if C is a linear code. Suppose C is a linear code of dimension k. Then the corresponding lattice sphere packing has density

$$\delta(rS_n, X) = \frac{\omega_n r^n}{2^{n+1-k}}.$$

Construction B

Theorem 5.2. *Let C be an (n,m,d) binary code with the property that the weight of each codeword is even, and let h(t) be the number of codewords u such that* $\|u, 0\|_H = t$. *Define*

$$X = \{x \in E^n : x(\mathrm{mod}\ 2) \in C\}$$

$$r = \begin{cases} \frac{\sqrt{d}}{2} & \text{if } d \leq 4, \\ 1 & \text{if } d \geq 4, \end{cases} \quad \text{and}$$

$$\tau = \begin{cases} 2^d h(d) & \text{if} d < 4, \\ 2n + 2^4 h(4) & \text{if} d = 4, \\ 2n & \text{if} d > 4. \end{cases}$$

Then $rS_n + X$ *is a periodic packing with density*

$$\delta(rS_n, X) = \frac{m\omega_n r^n}{2^n},$$

in which the sphere rS_n *touches* τ *others.*
In particular, X is a lattice if and only if C is a linear code. Suppose C is a linear code of dimension k. Then the corresponding lattice sphere packing has density

$$\delta(rS_n, X) = \frac{\omega_n r^n}{2^{n-k}}.$$

6 References

All these Information can be found in either:

(1) J. H. Conway, N. J. Sloane, Sphere Packings, Lattices and Groups, 3rd edition, Springer-Verlag New York, 2017, Chapter 3.2

(2) C. Zong, Sphere Packings, Universitext, Springer-Verlag New York, 1999., Chapters 5.1, 5.2, 5.3