Lecture 8: Classical Error-Correcting Codes

8.1 Block code $\mathcal{B}$

A block code $\mathcal{B}$ is a non-empty subset of all words of length n over an alphabet A with m letters, i.e.

$$\mathcal{B} \subseteq A^n, \quad \mathcal{B} \neq \emptyset.$$

$\Rightarrow$ In general, we have to store a list of all codewords together with the corresponding message ("meaning").

Rate of the code

$$R = \frac{\log_2 |\mathcal{B}|}{\log_2 |A^n|} = \frac{\log_2 |\mathcal{B}|}{n \cdot \log_2 |A|}$$

8.2 Hamming distance / Hamming weight

The Hamming distance between two words $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ is the number of positions where x and y differ, i.e.

$$d_{\text{Hamming}}(x, y) = |\{i : 1 \leq i \leq n \mid x_i \neq y_i\}|$$

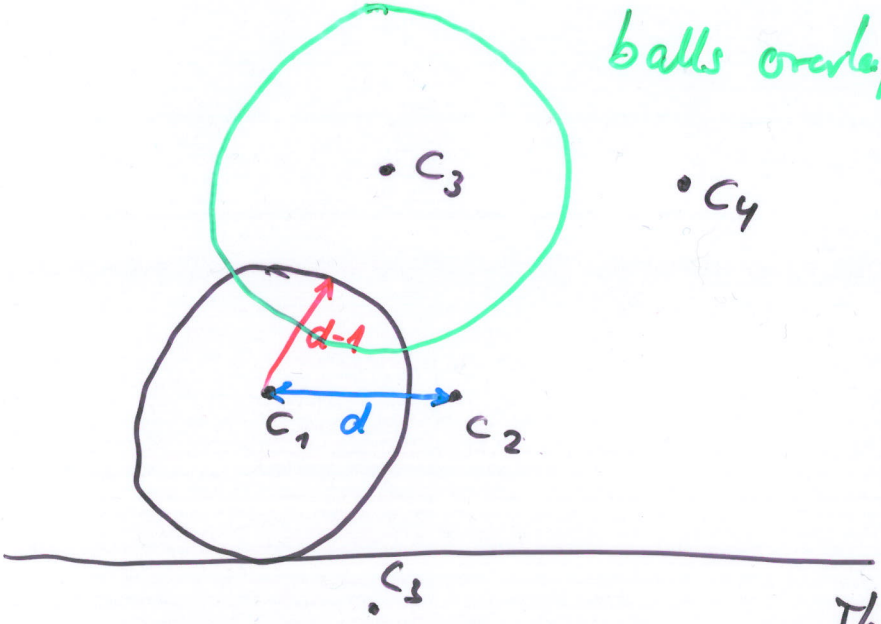
Hamming weight: distance from the word $(0, \ldots, 0)$ for a special symbol $0 \in A$.

8.3 Minimum distance of a block code

The minimum distance of a block code $\mathcal{B}$ is the minimum number of positions in which two distinct codewords differ, i.e

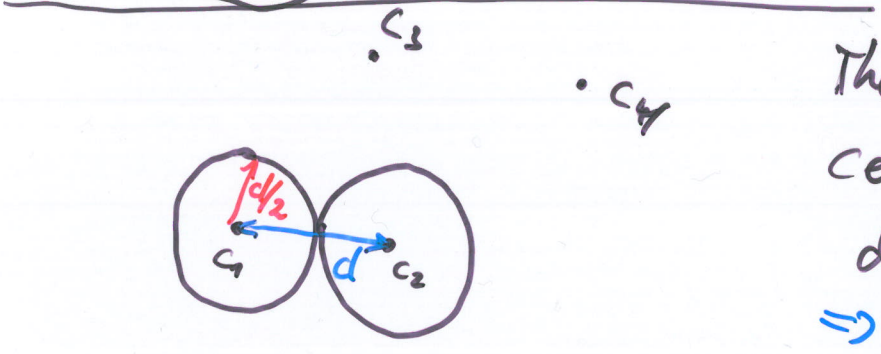
$$d_{min}(\mathcal{B}) := \min \{ d_{Hamming}(x,y) : x,y \in \mathcal{B}, x \neq y \}$$

8.4 A block code $\mathcal{B}$ with minimum Hamming distance d can either detect errors that change up to $d-1$ positions, or it can correct errors that change strictly less than $d/2$ positions.



Every ball with radius $d-1$ centered at a codeword c_i contains exactly one codeword

$\Rightarrow$ error detection



The balls with radius $r < d/2$ centered at codewords are disjoint.

$\Rightarrow$ error correction

In order to obtain more efficient descriptions of the codes, we need more structure.

8.5 Finite fields

a) Prime fields

The integers modulo a prime number p, denoted by $\mathbb{Z}/p\mathbb{Z}$ form a finite field with p elements.

It is clear that $\mathbb{Z}/p\mathbb{Z}$ is closed under addition, subtraction and multiplication.

We have to show that any non-zero element has a multiplicative inverse.

By the Euclidean algorithm, we find

$$1 = \gcd(p, b) = s \cdot p + t \cdot b \quad \text{for } b \neq 0 \bmod p$$

$$\Rightarrow \quad 1 = t \cdot b \bmod p, \text{ i.e. } t = b^{-1} \bmod p$$

Warning: If m is composite, then $\mathbb{Z}/m\mathbb{Z}$ is not a field, e.g. $2 \cdot 2 = 0 \bmod m = 4$

b) extension fields

To construct finite fields with $q = p^m$ elements, consider the polynomials over the field

$$\mathbb{F}_p = GF(p) \cong \mathbb{Z}/p\mathbb{Z}$$

modulo an irreducible monic polynomial f of degree m, i.e. $f(X) = X^m + \sum_{i=0}^{m-1} c_i X^i$ $c_0 \neq 0$

The Euclidean algorithm can be applied to polynomials (in one variable) as well and we get

$$1 = \gcd(f(X), b(X)) = s(X) \cdot f(X) + t(X) \cdot b(X)$$

for any polynomial $0 \neq b(X)$ of degree $< m$.

$\Rightarrow$ In total p^m polynomials of degree $< m$.

Theorem: A finite field $\mathbb{F}_q = GF(q)$ with q elements exists if and only if q is a prime power, i.e. $q = p^m$.

Furthermore, for every prime number p and degree m there exists at least one irreducible polynomial $f(x)$

Examples:

$q = 4 = 2^2$ $\quad \mathbb{F}_2 = GF(2) = \{0, 1\}$

$$f(X) = X^2 + X + 1$$

$(f(0) = f(1) = 1 \mod 2)$

$\Rightarrow f$ is irreducible

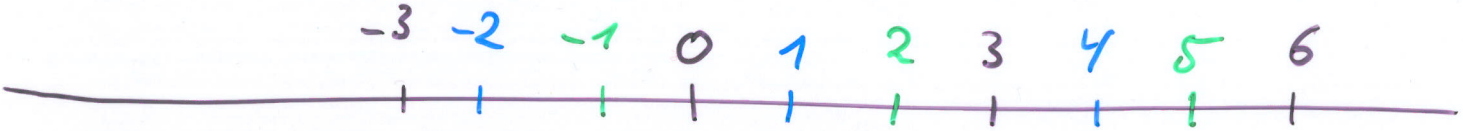
$\mathbb{F}_4 = \{0, 1, X, X+1\} = \{0, 1, \omega, \omega^2\}$

where $f(\omega) = \omega^2 + \omega + 1 = 0$

$q = 9 = 3^2$ $\quad \mathbb{Z}/3\mathbb{Z}$ $\quad \mathbb{F}_3 = GF(3) = \{0, 1, 2\}$

$= \{0, +1, -1\} \mod 3$

$$f(X) = X^2 + 1 \quad (f(0) = 1,\ f(\pm 1) = 2)$$



$\bar{0} = \{0 + k \cdot 3 : k \in \mathbb{Z}\}$

$\bar{1} = \{1 + k \cdot 3 : k \in \mathbb{Z}\}$

$\bar{2} = \{2 + k \cdot 3 : k \in \mathbb{Z}\}$

$$\mathbb{F}_9 \cong \mathbb{F}_3[X]/(X^2+1)$$

$$= \{0, 1, 2, X, X+1, X+2, 2X, 2X+1, 2X+2\}$$

Here a root α of the polynomial $f(X) = X^2+1$ does not generate all non-zero elements of $\mathbb{F}_9$ as powers, since

$$\alpha^2 + 1 = 0 \Rightarrow \alpha^2 = -1$$
$$\Rightarrow \alpha^4 = 1$$

but $\beta = \alpha + 1$, then

$$\mathbb{F}_9 = \{0\} \cup \{\beta, \beta^2, \ldots, \beta^8 = 1\}$$

The elements of a finite field $\mathbb{F}_q$ can always be written as power an element α or 0, i.e. $\mathbb{F}_q = \{0\} \cup \{\alpha, \alpha^2, \ldots, \alpha^{q-1}\}$

α is a primitive element