Aalto University
School of Science
and Technology

Coding Theory on Non-Standard Alphabets

A Brief Introduction into Traditional Coding Theory

Marcus Greferath

Department of Mathematics and Systems Analysis
Aalto University School of Sciences
marcus.greferath@aalto.fi

May 2023

Definition: Let C be an $\mathbb{F}_q$-linear code of length n.

- For every element $f \in \mathbb{F}_q$ we reserve an indeterminate x_f and form the the polynomial ring $\mathbb{C}[x_f \mid f \in \mathbb{F}]$.
- Define the complete (weight) enumerator of C to be the polynomial

$$W(C) := \sum_{c \in C} \prod_{i=1}^{n} x_{c_i}.$$

- In the bivariate polynomial ring $\mathbb{C}[x, y]$ we define the Hamming weight enumerator

$$W_H(C) = \sum_{c \in C} x^{n - w_H(c)} y^{w_H(c)}.$$

- **Remark:** We obtain the Hamming weight enumerator from the complete enumerator by applying the identification homomorphism $\mathbb{C}[x_f \mid f \in \mathbb{F}_q] \longrightarrow \mathbb{C}[x, y]$ that extends

$$x_f \mapsto \begin{cases} x & : \quad f = 0, \\ y & : \quad \text{otherwise.} \end{cases}$$

- **Example:** Consider the binary linear $[7, 3, 4]$-code C generated by the matrix

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

Listing all words reveals the complete and Hamming weight enumerator as

$$W(x, y) = W_H(x, y) = x^7 + 7\,x^3\,y^4.$$

- For $\mathbb{F}_4 = \{0, 1, a, a^2\}$ consider the famous $\mathbb{F}_4$-linear hexacode C generated by the matrix

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

Its complete enumerator in $\mathbb{C}[x, e, u, v]$ is given by

$$\begin{aligned} W(C) &= x^6 + 15\, x^2\, (e^2\, u^2 + e^2\, v^2 + u^2\, v^2) \\ &\quad + 15\, e^2\, u^2\, v^2 + e^6 + u^6 + v^6, \end{aligned}$$

while its Hamming weight enumerator is

$$W_H(D) = x^6 + 45\, x^2\, y^4 + 18\, y^6.$$

- Let $\chi : \mathbb{F}_q \longrightarrow \mathbb{C}^\times$ be a non-trivial character. We consider the $\mathbb{C}$-algebra homomorphism

$$M : \mathbb{C}[x_r | r \in \mathbb{F}_q] \longrightarrow \mathbb{C}[x_r \mid r \in \mathbb{F}_q], \quad f \mapsto Mf$$

extending the assignment

$$x_r \ \mapsto \ Mx_r \ := \ \sum_{s \in \mathbb{F}} \chi(rs) x_s .$$

- Let $C \leq {}_R R^n$ be an $\mathbb{F}_q$-linear code, with complete enumerator

$$W(C) \ := \ \sum_{c \in C} \prod_{i=1}^{n} x_{c_i} .$$

Let $C^\perp$ denote the dual code of C.

- **Theorem:** With notation introduced above, there holds

$$W(C^{\perp}) \;=\; \frac{1}{|C|}\, M\, W(C).$$

- Now consider the $\mathbb{C}$-algebra homomorphism

$$N : \mathbb{C}[x, y] \longrightarrow \mathbb{C}[x, y], \quad f \mapsto Nf$$

extending the assignment

$$x \;\mapsto\; Nx := x + (q-1)\, y \;\text{ and }\; y \mapsto Ny := x - y.$$

- Let C be an $\mathbb{F}_q$-linear code of length n with Hamming weight enumerator

$$W_H(C) \;:=\; \sum_{c \in C} x^{n - w_H(c)}\, y^{w_H(c)}.$$

- With notation introduced above, there holds

$$W_H(C^\perp) \;=\; \frac{1}{|C|}\, N\, W_H(C).$$

- **Example:** Consider the binary linear $[7,3,4]$-code C generated by the matrix

$$G \;=\; \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

  Its Hamming weight enumerator is

$$W_H(C) \;=\; x^7 + 7\, x^3\, y^4.$$

  Its dual code $C^\perp$ is a $[7,4]$ code.

- We compute the Hamming weight enumerator of $C^\perp$ as

$$\begin{aligned} W_H(C^\perp) &= \frac{1}{8}\left[(x+y)^u + 7\,(x+y)^3(x-y)^4\right] \\ &= x^7 + 7\,x^4y^3 + 7\,x^3y^4 + y^7. \end{aligned}$$

- This particularly shows that $d_{\min}(C^\perp) = 3$.
- Have another look at the $\mathbb{F}_4$-linear hexacode C generated by the matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & a & a \\ 0 & 1 & 0 & a & 1 & a \\ 0 & 0 & 0 & a & a & 1 \end{bmatrix}$$

with Hamming weight enumerator

$$W_H(C) = x^6 + 45\,x^2\,y^4 + 18\,y^6.$$

- Its dual code $C^\perp$ has the Hamming weight enumerator

$$\begin{aligned} W_H(C^\perp) &= \frac{1}{4^3}\left[(x+3\,y)^6 + 45\,(x+3\,y)^2(x-y)^4 + 18\,(x-y)^6\right] \\ &= x^6 + 45\,x^2\,y^4 + 18\,y^6, \end{aligned}$$

  which means, C and $C^\perp$ have the same Hamming weight enumerators.

- This observation would usually raise the suspicion that D actually is a self-dual code, however this is not the case.

- We call C a formally self-dual code if $W_H(C) = W_H(C^\perp)$.

- If C is equivalent to $C^\perp$, then we call C an iso-dual code.

Existence Bounds and Code Families

- One of the foremost problems of Coding theory is the maximization of $M = |C|$, whenever the length n and the minimum distance d is given.

- Alternatively, we seek to maximize d, once n and M have been specified.

- A third version is to minimize n, when M and d are given.

- **Sphere-Packing Bound:** If C is an (n, M, d) code over a q-element alphabet, and $t = \lfloor \frac{d-1}{2} \rfloor$ then

$$M \cdot \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \le q^n.$$

- Codes that meet the sphere-packing bound with equality, are called perfect codes.

- **Theorem:** The parameter triples of all perfect codes are known.
  - For q-ary alphabets, these are $(n = \frac{q^r-1}{q-1}, q^{n-r}, 3)$, where r is a positive integer, and q is a prime power.
  - In the binary and ternary case we have the parameters $(23, 2^{12}, 7)$ and $(11, 3^6, 5)$.

- All other perfect codes have trivial parameter, i.e. are 1-element, repetition, or full space codes.

- **Singleton Bound:** For every (n, M, d) code over a q-element alphabet, there holds

$$M \leq q^{n+1-d}.$$

- Codes that meet the Singleton bound with equality, are called maximum distance separable codes (MDS).
- The characterization of all MDS codes is a still open problem.
- We refer to the famous MDS conjecture: If C is an $[n, k, d]$ MDS code over $\mathbb{F}_q$ then if $k \leq q$ then $n \leq q + 1$ except in a certain set of cases, where $n \leq q + 2$.

- **Gilbert Bound:** There exists a code with parameters (n, M, d) over $\mathbb{F}_q$ that satisfies

$$M \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i}.$$

- **Varshamov Bound:** There exists a linear code with parameters $[n, k, d]$ provided, that

$$\sum_{i=0}^{d-1} \binom{n-1}{i}(q-1)^i < q^{n-k}.$$

- Although the proof for the Gilbert bound is greedy-based in principle, it does not provide an efficient scheme of construction.

- Let $\mathbb{F}_q$ be the underlying finite field, and recall the $\mathbb{C}$-algebra homomorphism

$$N : \mathbb{C}[x, y] \longrightarrow \mathbb{C}[x, y], \quad f \mapsto Nf$$

extending the assignment

$$x \ \mapsto \ Nx := x + (q-1)\, y \ \text{ and } \ y \mapsto Ny := x - y.$$

- Define the Krawtchouk polynomials implicitly by

$$N(x^{n-z}y^z) \ = \ \sum_{i=0}^{n} P_i(z) x^{n-i} y^i.$$

- Alternatively, their explicit form is:

$$P_i(z) \ = \ P_i(z, q, n) \ = \ \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{z}{j} \binom{n-z}{k-j}.$$

- **Linear Programming Bound:** Let C be an (n, M, d)-code. With the above notation, we have: holds:

$$M \leq \max_{A} \sum_{i=0}^{n} A_i$$

where the max is taken over all $A := (A_i)_{i=0}^{n}$ satisfying

$$\begin{aligned} A_i &\geq 0 \\ A_i &= \begin{cases} 1 & \text{if} \quad i = 0 \\ 0 & \text{if} \quad 0 < i < d \end{cases} \qquad \text{and} \\ \sum_{j=0}^{n} A_j P_i(j) &\geq 0 \quad \text{for all } i = 0, \ldots, n \end{aligned}$$

- Let $\mathbb{P}(\mathbb{F}_q^r)$ be the projective space of rank r over $\mathbb{F}_q$.
- Each point of this space is of the form $\mathbb{F}_q x$ where $0 \neq x \in \mathbb{F}_q^r$.
- Choose a generator x in each of these points in such a way, that its first non-zero entry is a 1.
- Sort the $\frac{q^r-1}{q-1}$ chosen vectors lexicographically order and put them into an $r \times \frac{q^r-1}{q-1}$ matrix $H = H(q,r)$.
- **Definition:** The code checked by H is called Hamming Code of rank r over the field $\mathbb{F}_q$. Its parameters are $[n := \frac{q^r-1}{q-1}, n-r, 3]$.

- For $\mathbb{F}_3$ and $r = 3$, we have the Hamming matrix

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix},$$

  where we have assumed $0 < 1 < 2$.

- $\mathbb{F}_4 = \{0, 1, a, a^2\}$, ordered as presented, meaning $0 < 1 < a < a^2$. For space reasons, we restrict to $r = 2$ and obtain

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & a & a^2 \end{bmatrix}.$$

- Hamming codes satisfy the sphere packing bound with equality, and they form an example class of what we call perfect codes.
- Decoding the Hamming codes is easy. If $y = c + e$ is the received word, where c is the codeword and e is a single Hamming error, say $e = \lambda e_i$, then we compute the syndrome

$$s := yH^T = eH^T = \lambda e_i H^T = \lambda H_i^T,$$

  where H_i is the i-th column of H.
- The error value of e is then the first nonzero entry of yH^T, for the position search for $\frac{s}{\lambda}$ in the lexicographically sorted check matrix H.

- **Example:** Let $q = 3$ and $r = 3$, so that H is the matrix in the above example. Assume, we have received the word $y = [1, 0, 2, 1, 2, 0, 0, 1, 2, 0, 2, 2, 2]$.

- Compute the syndrome $s := yH^T = [2, 0, 1]^T$ and conclude that the error value $\lambda = 2$.

- After dividing the syndrome by λ, we seek $\frac{s^T}{\lambda} = [1, 0, 2]^T$ among the columns of H and arrive at column 7.

- For this reason, the single error is a 2 in the 7th position of y. Consequently, the codeword we search for is

$$\begin{aligned} c &= y - [0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0] \\ &= [1, 0, 2, 1, 2, 0, 1, 1, 2, 0, 2, 2, 2]. \end{aligned}$$

- Let $q = 2$ and m be a natural number. For $0 \le r \le m$ we define the two-parametric family of codes $\mathrm{RM}(r, m)$ by
  - $\mathrm{RM}(0, m)$ is the repetition code of length 2^m.
  - $\mathrm{RM}(m, m)$ is the full space code of length 2^m.
  - $\mathrm{RM}(r, m) := \mathrm{RM}(r, m-1) \oplus \mathrm{RM}(r-1, m-1)$ for all $1 \le r \le m-1$. Here $\oplus$ denotes the Plotkin sum that we studied earlier.
- **Definition:** The codes $\mathrm{RM}(r, m)$ are called Reed Muller Codes.
- They are $[n, k, d]$ codes for

$$n = 2^m, \quad k = \sum_{i=0}^{r} \binom{m}{i}, \quad \text{and} \quad d = 2^{m-r}.$$

- **Example:** Find a generator matrix for $\mathrm{RM}(2,3)$!
- First, observe that $\mathrm{RM}(2,3) = \mathrm{RM}(2,2) \oplus \mathrm{RM}(1,2)$, and $\mathrm{RM}(1,2) = \mathrm{RM}(1,1) \oplus \mathrm{RM}(0,1)$.
- Writing down generator matrices $G_{r,m}$ for all components $\mathrm{RM}(r,m)$, we start with

$$G_{2,2} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad G_{1,1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and

$$G_{0,1} = \begin{bmatrix} 1 & 1 \end{bmatrix}$$

- Therefore, we obtain

$$G_{1,2} = \left[\begin{array}{c|c} G_{1,1} & G_{1,1} \\ \hline 0 & G_{0,1} \end{array}\right] = \left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 1 \end{array}\right].$$

- Finally, we arrive at

$$G_{2,3} = \left[\begin{array}{c|c} G_{2,2} & G_{2,2} \\ \hline 0 & G_{1,2} \end{array}\right] = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right].$$

- **Definition:** The cyclic code Gol_{23} of length 23 that is generated by the polynomial

$$x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1 \in \mathbb{F}_2[x],$$

and the cyclic code Gol_{11} of length 11 generated by the polynomial

$$x^5 + x^4 - x^3 + x^2 - 1 \in \mathbb{F}_3[x]$$

are called Golay Codes.

- **Remark:** Gol_{23} and Gol_{11} are perfect codes with parameters $[23, 12, 7]$ and $[11, 6, 5]$, respectively.
- A result by van Lint and Tietäväinen (1973), says that any (non-trivial) perfect code must have the parameters of either the Hamming Codes or the two Golay Codes.

- The extended versions Gol_{24} and Gol_{12} have attracted a lot of interest for many combinatorial reasons. They are examples of self-dual codes.

- They are closely related to prominent structures in group theory, and can be used to construct very dense lattices.

- E. Viterbo and M. Elia have designed what are called algebraic decoders for the cyclic versions.

- There is a quite entertaining article by A. Barg describing the history around the discovery of the Golay codes.