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

Linear Codes and Their Duals

- **Definition:** Let $\mathbb{F}_q$ denote the q-element field, and let $w_H : \mathbb{F}_q \longrightarrow \{0,1\}$ with

$$w_H(x) = \begin{cases} 1 & : \quad x \neq 0 \\ 0 & : \quad x = 0 \end{cases}$$

  Extend this additively to the Hamming weight on $\mathbb{F}_q^n$, by

$$\begin{aligned} w_H : \mathbb{F}_q^n &\longrightarrow \mathbb{N}, \\ x &\mapsto \sum_{i=1}^{n} w_H(x_i) = \#\{i \in \{1,\ldots,n\} \mid x_i \neq 0\}, \end{aligned}$$

- This weight induces the Hamming distance

$$d_H : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{N},\ (x,y) \mapsto d_H(x,y) := w_H(x-y).$$

- As we sar, d_H is indeed a metric on $\mathbb{F}_q^n$, i.e. positive, symmetric, with triangle inequality.
- Its one-argument version w_H is often easier to handle, while essentially describing the same phenomena.
- A block code $C \subseteq \mathbb{F}_q^n$ will be called a linear code, if it is a subspace of $\mathbb{F}_q^n$. We will write $C \leq \mathbb{F}_q^n$ in this case.
- As before, n is called the length of the code, whereas $k := \dim(C)$ is the dimension, so that we have $M = q^k$, and the rate $R = \frac{k}{n}$.
- If d is the minimum Hamming distance of C, we refer to C as an $[n, k, d]$-code, or an $[n, k, d]_q$-code including a reference to the (size of the) the field alphabet.

- The minimum distance d of a linear code is equivalently described by its minimum weight, which means

$$d_{\min}(C) \;=\; w_{\min}(C) \;=\; \min\left\{w_H(c) \mid c \in C - \{0\}\right\}.$$

- Combinatorially, an $\mathbb{F}_q$-linear $[n, k, d]_q$-code is a block code with parameters (n, q^k, d) over a size q alphabet.
- Linearity is implicitly emphasized by the choice of square brackets: $[n, k, d]_q$ instead of (n, M, d), where $M = q^k$.
- **Example:** The binary repetition code $C := \{[0, 0, 0], [1, 1, 1]\}$ is a linear code with parameters $[3, 1, 3]$.
- **Example:** The even weight code $E_3 := \{[0, 0, 0], [0, 1, 1], [1, 0, 1], [1, 1, 0]\}$ is a linear code with parameters $[3, 2, 2]$.

- **Definition:** Let C be an $\mathbb{F}_q$-linear code of length n. A $k \times n$-matrix G with entries from $\mathbb{F}_q$ is called a generator matrix for C, if
$$C = \{xG \mid x \in \mathbb{F}_q^k\}.$$
In this case, the rows of G span C.

- **Definition:** G is called a check matrix for C, if
$$C = \{z \in \mathbb{F}_q^n \mid zG^T = 0\}.$$
This means the given code is the null space of G^T.

- In most cases it is convenient (or even required) to assume that generator and check matrices are of full rank.

- **Nota Bene:** If C is an $\mathbb{F}_q$-linear $[n, k]$-code, then there exists a $k \times n$-generator matrix and an $(n-k) \times n$-check matrix for C.
- If $G = [I_k \mid A]$ is a generator matrix C, where I_k is the $k \times k$ identity matrix and A is an $k \times (n-k)$ matrix, then $H := [-A^T \mid I_{n-k}]$ will be a check matrix for C.
- Not in each case, though, a code C possesses a generator matrix in standard form $[I_k \mid A]$.
- A coordinate permutation will help to arrive at generator matrix that allows for the standard form.
- This permutation will of course have to be reversed, once the check matrix of this matrix has been derived.

- Consider the binary matrix

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

  which is a generator matrix for a binary $[7, 3, 4]$ code.

- This code is called simplex code which is closely related to the binary Hamming code with parameters $[7, 4, 3]$ that we are going to discuss soon.

- The binary repetition code C of length 3 has the 1×3-matrix $B = [1, 1, 1]$ as generator matrix. The even weight code E_3 is generated by the matrix

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

- **Example:** For $\mathbb{F}_4 = \{0, 1, a, a^2\}$, the matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & a \\ 0 & 0 & 1 & 1 & a^2 \end{bmatrix},$$

generates a $[5, 3, 3]$-code, that may be recognized as $\mathbb{F}_4$-linear Hamming Code of rank 2.

- This code is equally well described by the check matrix

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

- **Proposition:** Let C be an $\mathbb{F}_q$-linear code of length n, and let H be a check matrix for C. Then the following are equivalent:
  - The minimum distance of C is d.
  - Any $d-1$ columns of H are linearly independent, and there exists a d-element selection of linearly dependent columns.

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

$$C^{\perp} := \{x \in \mathbb{F}_q^n \mid cx = 0 \text{ for all } c \in C\}$$

and call it the dual code of C.

- Linear Algebra tells us that if $W \leq \mathbb{R}^n$ is a real vector space, then $W \cap W^\perp = \{0\}$, as there is no (non-zero) real vector which is orthogonal to itself.
- In finite Linear Algebra, this may be different, so that a code can even contain (or be contained in) its own dual.
- For example in even length, the binary repetition code is contained in the even weight code, which is its dual.
- **Definition:** A code C will be called self-dual, if $C^\perp = C$.
- It has been observed, that many good codes (of rate $1/2$) are actually self-dual. Therefore self-dual codes form a classically hot topic in algebraic coding theory.

- **Definition:** A block code $C \subseteq F^n$ is called a cyclic code, if with every codeword $[c_0, \ldots, c_{n-1}] \in C$ also the word $[c_{n-1}, c_0, \ldots, c_{n-2}] \in C$. This means, C is invariant under cyclic permutations.
- **Observation:** A cyclic linear code $C \leq \mathbb{F}_q^n$ can be represented as an ideal in the quotient ring $\frac{\mathbb{F}_q[x]}{(x^n-1)}$.
- This representation is based on the one-to-one correspondence:

$$[c_0, \ldots, c_{n-1}] \in \mathbb{F}_q^n \longleftrightarrow \sum_{i=0}^{n-1} c_i x^i + (x^n - 1) \in \frac{\mathbb{F}_q[x]}{(x^n - 1)}.$$

- The cyclic shift is represented by multiplication by x.

- It is clumsy to write $\sum_{i=0}^{n-1} c_i x^i + (x^n - 1)$ for the elements of this residual ring.

- So, one omits the expression $(x^n - 1)$ in general, or one occasionally writes $\pmod{x^n - 1}$ when it is suggested.

- **Proposition:** Let C be a cyclic $\mathbb{F}_q$-linear code. Then there is a unique monic divisor g of $x^n - 1$ in $\mathbb{F}_q[x]$ such that

$$C = \frac{\mathbb{F}_q[x]\, g}{(x^n - 1)}.$$

- **Definition:** The polynomial g above is called the generator polynomial of C.

- The above allows to characterize all distinct cyclic codes of a given length, which only requires knowledge about the factorization of $x^n - 1$ in the polynomial ring $\mathbb{F}_q[x]$.
- **Example:** Over the binary field $\mathbb{F}_2$, we factorize

$$x^7 + 1 \;=\; (x+1)\,(x^3+x+1)\,(x^3+x^2+1).$$

  As there are 3 irreducible divisors involved, we conclude that we will have to deal with 8 distinct cyclic codes.
- The co-divisor $h = \frac{x^n-1}{g}$ is usually referred to as the check polynomial of C.
- The polynomial $h^{\text{rev}}(x) = x^{\deg(h)} h(\frac{1}{x})$ generates $C^{\perp}$.

- We wonder, how to derive new codes from given ones.
- **Puncturing:** Let C be an $\mathbb{F}_q$-linear Code of length n. For chosen $i \in \{1, \ldots, n\}$ define the code

$$C_i := \{[c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n] \mid [c_1, \ldots, c_n] \in C\}$$

  and say, C_i is the code C punctured in coordinate i.
- C_i is linear of length $n' = n - 1$; its dimension k' and minimum distance d' satisfy $k - 1 \leq k' \leq k$ and $d - 1 \leq d' \leq d$.
- Generally, we have $k' = k$, at least if $d \geq 2$, and mostly $d' = d - 1$, however $d' = d$ can happen as well in given cases.

- **Example:** Let C be the binary $[8,4,4]$-code spanned by the rows of the generator matrix

$$G = \left[\begin{array}{ccccccc|c} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right].$$

  Let C_8 be the code resulting from puncturing C in the 8th coordinate.

- The matrix consisting of the first 7 columns of G is a generator matrix for C_8.
- It turns out that C_8 has parameters $[7,4,3]$.

- **Extending:** Let C be an $\mathbb{F}_q$-linear Code of length n. For a linear form $\lambda : C \longrightarrow \mathbb{F}_q$, define the code

$$C_\lambda \;:=\; \{[c_1, \ldots, c_n, \lambda(c)] \mid c = [c_1, \ldots, c_n] \in C\}$$

  and call C_λ the extended code of C.

- In most cases, a special choice of λ is used, namely

$$\lambda(c) \;=\; -\sum_{i=1}^{n} c_i \quad \text{for } c \in C.$$

- **Example:** Let C be the binary $[6, 3, 3]$-code spanned by the rows of the generator matrix

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

- Extending this code yields the code C_{ext}, and we find the matrix

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

  to be a suitable generator matrix for C_{ext}. It turns out that this code has parameters $[7, 3, 4]$.

- **Shortening:** Let C be an $\mathbb{F}_q$-linear Code of length n. For a chosen $i \in \{1, \ldots, n\}$ we define the code

$$C_i := \{[c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n] \mid [c_1, \ldots, c_n] \in C \text{ and } c_i = 0\}$$

  and say, C_i is the code C shortened in coordinate i.

- C^i is a linear of length $n' = n - 1$ for any $i \in \{1, \ldots, n\}$.
- Its dimension k' and minimum distance d' satisfy $k - 1 \leq k' \leq k$ and $d' = d$.
- Generally, we have $k' = k - 1$, except in the case, where position i was a zero coordinate of C.
- Such a situation will never be interesting in applications, however for the theory, it might be worth mentioning.
- **Example:** Let C be the binary $[8, 4, 4]$-code spanned by the rows of the generator matrix

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

- Applying Gaussian elimination focusing on the 8th coordinate, we obtain the generator matrix

$$G' = \left[\begin{array}{ccccccc|c} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right].$$

- Shortening C in the 8th coordinate yields the code C^8, for which the lower left part G'' of G' is a generator matrix.

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

generates C^8, which has parameters $[7, 3, 4]$.

- Puncturing and shortening a code allows repeated application, so that many different codes of various length $n' \leq n$ will result.
- **Plotkin Sum:** Assume that C_1 is an $[n, k_1, d_1]$ code and C_2 is an $[n, k_2, d_2]$ code. Define the code

$$C_1 \oplus C_2 \; := \; \Big\{[x, x+y] \mid x \in C_1,\; y \in C_2\Big\}.$$

- The length of $C_1 \oplus C_2$ is $2n$, the dimension is $k_1 + k_2$, and the minimum distance is given by $\mathtt{min}\{2d_1, d_2\}$.
- This is superior to

$$C_1 \boxplus C_2 \; := \; \Big\{[x, y] \mid x \in C_1,\; y \in C_2\Big\},$$

which is actually of minimum distance $\mathtt{min}\{d_1, d_2\}$

- **Code Equivalence:** We say, two block codes C and D are equivalent, if they are isometric, meaning there is a bijective mapping $\varphi : C \longrightarrow D$ such that

$$d_H(\varphi(x), \varphi(y)) = d_H(x, y) \text{ for all } x, y \in C.$$

- If C and D are linear codes, we ask that φ be a linear mapping, which will be an isometry, if it preserves the weight w_H.
- **Definition:** An endomorphism $\varphi \in \mathrm{End}(\mathbb{F}_q^n)$ is called a monomial transformation, if there is a permutation $\pi \in S_n$ and $u_1, \ldots, u_n \in \mathbb{F}_q^\times$ such that

$$\varphi([x_1, \ldots, x_n]) \;=\; [x_{\pi(1)}u_1, \ldots, x_{\pi(n)}u_n] \quad \text{for all } x \in \mathbb{F}_q^n.$$

- Every monomial transformation φ of $\mathbb{F}_q^n$ is a Hamming isometry of this full vector space.
- If $\varphi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ is a Hamming isometry, then φ is a monomial transformation.
- If $C \leq \mathbb{F}_q^n$ is a linear code and $\varphi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ is a monomial transformation, then C and $\varphi(C)$ are equivalent.
- **Lemma:** Let C be an $\mathbb{F}_q$-linear code of length n. Then

$$\frac{1}{|C|} \sum_{c \in C} w_H(c) \ = \ \frac{q-1}{q} |\mathrm{supp}(C)|,$$

  where $\mathrm{supp}(C)$ is the set of all coordinates, in which C takes nonzero values.

- **Corollary:** Let $C \leq \mathbb{F}_q^n$ be a linear code and $\psi : C \longrightarrow \mathbb{F}_q^n$ a Hamming isometry. Then

$$|\{i \mid \pi_i(C) = \{0\}\}| = |\{i \mid \pi_i\psi(C) = \{0\}\}|.$$

- **Theorem:** Let C and D be $\mathbb{F}_q$-linear codes of length n, and let $\psi : C \longrightarrow D$ be a Hamming isometry. Then there is a monomial transformation φ on $\mathbb{F}_q^n$ such that $\varphi|C = \psi$.

- **Remarks on proof:**
  - The theorem was proved first by F. J. MacWilliams in her thesis in 1962 for linear codes over prime fields.
  - It can be proved in various ways, the simplest among which being induction on the length and using the above corollary.