Easy to construct and adopt to different situations

A linear $[n,m]$-code C is called a cyclic code if and only if $\forall x \in \{x_1 \dots x_n\}$

$x_1 \cdots x_n \in C \Rightarrow x^{\triangleright} := x_n x_1 \cdots x_{n-1} \in C$

every cyclic shift of a codeword is a code word

seems strict but actually it isn't

example Ham(3,2) is not cyclic but equivalent to a cyclic one if we take another parity check matrix and generator matrix.

instead of $H := \begin{pmatrix} 0&1&1&1&1&0&0 \\ 1&0&1&1&0&1&0 \\ 1&1&1&0&0&0&1 \end{pmatrix}$ we take $H := \begin{pmatrix} 1&0&1&1&1&0&0 \\ 0&1&0&1&1&1&0 \\ 0&0&1&0&1&1&1 \end{pmatrix}$ rows are cyclic permutations of each other

↑ their linear combinations are cyclic as well

since $x^{\triangleright} \cdot y^{\triangleright} = x \cdot y$ the orthogonal complement of a cyclic code is also cyclic

With every element of $\mathbb{F}_q^n$ we can associate a polynomial of degree at most $n-1$

$\mathbb{F}_q^n \to \mathbb{F}_q[X] : c_0 \cdots c_{n-1} \longrightarrow c_0 + c_1 X^1 + c_{n-1} X^{n-1}$

if we multiply this poly. with X we see that all the coefficients shift one position to the right

But since c_{n-1} also shifts one to the right and not to the first position, the new poly. doesn't correspond anymore to a codeword.

We solve this by identifying x^n with 1. This means we work with the quotient ring $\mathbb{F}_q[X]/(X^n-1)$ rather than $\mathbb{F}_q[X]$. So we work modulo x^n-1

Multiplying by X corresponds to a cyclic shift of the coefficients.

We have a bijective map

$$\mathcal{P}: \mathbb{F}_q^n \to \mathbb{F}_q[X]/(x^n-1) : c_0 \cdots c_{n-1} \to c_0 + c_1 X^1 \cdots c_{n-1} X^{n-1} \pmod{x^n-1}$$

This map satisfies that: $\mathcal{P}(c^{\triangleright}) = X\,\mathcal{P}(c)$

The image of a cyclic code under $\mathcal{P}$ corresponds to a subset of $\mathbb{F}_q[X]/(x^n-1)$ closed under addition and multiplication by X (hence mult. by every p. mod x^n-1).

$$(a_0 + a_1 X \cdots a_K X^K)\,\mathcal{P}(c) = \mathcal{P}\left(a_0 c + a_1 c^{\triangleright} + \dots + a_K c^{\overbrace{\triangleright \dots \triangleright}^{K X}}\right)$$

theorem

Cyclic codes of length n are in 1 to 1 correspondance with linear subspaces of $\mathbb{F}_q[X]/(X^n-1)$ closed under multiplication and addition.

Generator polynomial and check polynomial

theorem for every cyclic code $c \subset \mathbb{F}_q[x]/(x^n-1)$ there exist a polynomial $g \in c$ such that:

$$c := \{a(x) \in \mathbb{F}_q[x]/(x^n-1) \mid a(x) \text{ is a multiple of } g(x)\}$$

proof: define $g(x)$ to be a polynomial of the lowest degree.
Every other polynomial $f(x) \in c$ must be divisible by $g(x)$. If not we could perform a division and write $f(x) = q(x)g(x) + r(x)$ with $\deg(r(x)) < \deg(g(x))$.
Since c is closed under addiction and multiplication with elements of $\mathbb{F}_q(x)/(x^n-1)$
$r(x) = f(x) - q(x)g(x)$ is again a code polynomial. This contradicts that $g(x)$ was of the lowest degree.

we call $g(x)$ a generator polynomial of c

writing $g(x) = g_0 + g_1 x \dots g_v x^v$ we see that $g(x), Xg(x), \dots, X^{n-v-1}g(x)$ form an $\mathbb{F}_q$-basis for c and hence

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_v & & \\ & g_0 & \dots & \dots & g_v & \\ & & \ddots & & \ddots & \\ & & & g_0 & \dots & g_v \end{pmatrix} \in \mathrm{Mat}_{n-v \times n}(\mathbb{F}_q)$$

is a generator matrix for the code.
The number of rows of G is $n-v$ so the dimension of c is $k = n-v$

theorem
for a non-trivial cyclic code $c \in \mathbb{F}_q[x]/(x^n-1)$ the generator polynomial divides x^n-1

proof: if $g(x)$ doesn't divide x^n-1 then one can look at the rest of x^n-1 divided by $g(x)$.
this rest $r(x)$ has lower degree than $g(x)$ but is a linear combination of $g(x)$ and x^n-1 $(=0 \bmod x^n-1)$ so it's an element of the code. But that is impossible because $g(x)$ is the element of the code with the element of the code with the lowest degree.

we define $h(x) := \dfrac{x^n-1}{g(x)}$ to be the parity check polynomial of c

we can prove that $c(x)$ is a code polynomial if and only if $h(x)c(x) = 0 \pmod{x^n-1}$

We can encode using systematic encoding.
If we encode just multiplying by g it will not contain the original message because G doesn't contain the identity matrix. We can fix this.
Suppose $u(x)$ is the message we want to encode and that $n-k$ is the degree of $g(x)$
$x^{n-k}u(x)$ will then be the message shifted to the last k of n digits of the code words.
However $x^{n-k}u(x)$ itself is not the codeword. We have to change the first $n-k$ digits.
Bcz of the division algorithm we have the identity

$$\exists q(x), r(x): x^{n-k}u(x) = q(x)g(x) + r(x)$$

this implies that $x^{n-k}u(x) - r(x)$ is a code word satisfying our demands, because the two terms of the sum do not overlap

finding all cyclic codes

cyclic codes are in 1 to 1 correspondence with divisors of x^n-1, each divisor can be seen as the generator poly. of a cyclic code.
The problem is reduced to factorizing x^n-1 over $\mathbb{F}_q[x]$

Lemma:

Over $\mathbb{F}_q[x]$ with q prime, we have the following identities

- $x^{uv}-1 = (x^u-1)(x^{(v-1)u} + x^{(v-2)u} + \cdots + x^u + 1)$ for any $u, v \in \mathbb{N}$
- $x^{uv}+1 = (x^u+1)(x^{(v-1)u} - x^{(v-2)u} - \cdots - x^u + 1)$ for any $u, v \in \mathbb{N}$ and v odd
- $x^{2u}+1 = (x^u+a)(x^u-a)$ if $a^2+1=0 \bmod q$ (eg. if $q=5$, $a=2$ $2^2+1=0 \bmod 5$)
- $x^{qu} \pm 1 = (x^u \pm 1)^q$

theorem

a cyclotomic coset modulo n is a set of the form $\{s, sp, sp^2, \dots\}$ where s is an integer and the elements of the set are calculated modulo n.
Suppose p prime $p \nmid n$. Then the sizes of the cyclotomic coset modulo n are the same as the degrees of the irreducible divisors of x^n-1 over $\mathbb{F}_q$.
No irreducible poly. appears more than once as a divisor of x^n-1.

given any divisor $g(x) \mid x^n-1$ we have a unique cyclic $[n, m, d]$-code with $g(x)$ as generator polynomial. $m = n - \deg(g(x))$, but d is not clear for a given $g(x)$ or how to find $g(x)$ so that d is a given number
Later this will be discussed.