Review Sessions
Tue., April 9 10:30-12
Fri., April 12 2:30-4
in Math. Annex 1105 or 1102 (check both rooms)

Lecture 21
Math 342.
Tue., April 2, 2019

Last time: Cyclic codes.

(a₀, ..., aₙ₋₁) ⟷ a(x) = a₀ + a₁x + ... + aₙ₋₁xⁿ⁻¹

View a(x) as an element of \( R_n = \mathbb{F}_q[x]/x^n - 1 \).

Proposition: \( C \subseteq R_n \) correspond to a cyclic code if and only if

1. \( a(x), b(x) \in C \implies (a + b)(x) \in C \)
2. \( a(x) \in C, r(x) \in R_n \implies (r \cdot a)(x) \in C \)
For any \( g(x) \in R_n \), we can define 
\[ C = \langle g(x) \rangle \subseteq R_n \] as follows
\[ C = \langle \{ r(x)g(x) \mid r(x) \in R_n \} \rangle = \langle g(x) \rangle \]
This is a cyclic code by Proposition (check).

**Theorem:** Let \( C \subseteq R_n \) be a cyclic code.
Assume \( C \neq \{0\} \).
Then
(1) There exists a unique monic polynomial \( g(x) \) of minimal degree.
(2) \( C = \langle g(x) \rangle \)
(3) \( g(x) \) divides \( x^n - 1 \).

**Proof:** (1) **Existence.** Let \( f(x) \) be a poly.
of minimal degree in \( C \), say
\[ f(x) = f_0 + f_1 x + \ldots + f_d x^d \]
where \( f_0, \ldots, f_d \in F_q, f_d \neq 0 \). Set \( g(x) = f_d^{-1} f(x) \).
Then \( g(x) \in C \), monic, min. degree.
Uniqueness. Suppose \( g_1(x) \) is another monic polynomial of minimal degree, then \( g(x) - g_1(x) \in \mathbb{C} \) is of lower degree \( \Rightarrow g(x) - g_1(x) = 0 \), i.e., \( g(x) = g_1(x) \).

2) Let \( f(x) \) be an element of \( \mathbb{C} \). Divide \( f(x) \) by \( g(x) \) with remainder:

\[
f(x) = q(x) g(x) + r(x)
\]

where \( \deg(r) < \deg(g) \). Since \( f(x) \in \mathbb{C}, g(x) \in \mathbb{C} \), \( f(x) - q(x) g(x) = r(x) \in \mathbb{C} \). Since \( g(x) \) has minimal degree, we conclude that \( r(x) = 0 \). Thus \( f(x) \in \langle g(x) \rangle \). This shows that \( \langle g(x) \rangle = \mathbb{C} \).

3) Divide \( x^n - 1 \) by \( g(x) \) with remainder.

\[
x^n - 1 = q_1(x) g(x) + r_1(x), \quad \deg(r_1) < \deg(g)
\]

Note that \( x^n - 1 = 0 \) in \( \mathbb{R}_n \), so \( r_1(x) \equiv q_1(x) \cdot g(x) \in \langle g(x) \rangle = \mathbb{C} \). Since \( \deg(r_1) < \deg(g) \), we conclude
that \( r_1(x) = 0 \). Thus
\[
x^n - 1 = q_1(x) g(x),
\]
i.e., \( g(x) \) divides \( x^n - 1 \). \( \text{Q.E.D.} \)

\( g(x) \) is called the generator polynomial of \( C \).

\[
\begin{align*}
\text{Cyclic codes } C & \quad \text{Monic polynomials dividing } x^n - 1 \\
\text{of length } n & \quad \text{of degree } n \\
\text{over } \mathbb{F}_q & \quad \text{over } \mathbb{F}_q
\end{align*}
\]

\[
C = \{03\} \quad \xrightarrow{g(x) = x^n - 1} \quad g(x) = x^n - 1.
\]

Example: \( q = 3, n = 4 \).
\[
x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1)
\]
\( \text{no roots in } \mathbb{F}_3 \)
\( \Rightarrow \) irreducible.

There are 8 cyclic codes of length 4 over \( \mathbb{F}_3 \).
They are of the form \( \langle g(x) \rangle \),
where \( g(x) = (x-1)^{\varepsilon_1} (x+1)^{\varepsilon_2} (x^2+1)^{\varepsilon_3} \),
\( \varepsilon_1, \varepsilon_2, \varepsilon_3 = 0 \) \ or \ 1.

For example, if \( \varepsilon_1 = \varepsilon_2 = \varepsilon_3 = 0 \), then \( g(x) = 1 \), and \( C = \langle g(x) \rangle = \mathbb{R}_n \).

Corresponding code is \( F_3^4 \) (every word of length 4 is included).

Another example: \( \varepsilon_1 = 1, \varepsilon_2 = \varepsilon_3 = 0 \).
\( g(x) = (x-1) \). \( C = \langle g(x) \rangle = \{ (x-1)h(x) \mid h(x) \in \mathbb{R}_n \} \)

\[ = \{ f(x) \mid f(1) = 0 \} = \{ f_0 + f_1 x + x^3 + f_2 x^3 + f_3 x^0 \mid f_0, f_1, f_2, f_3 \in F_3 \} \]

\( C = \{ (a_0, a_1, a_2, a_3) \mid a_0 + a_1 + a_2 + a_3 = 0 \mbox{ in } F_3 \} \).

**Proposition:** Suppose \( C \) is cyclic code of length \( n \) with generator polynomial
\[ g(x) = g_0 + g_1 x + \ldots + g_n x^n \]. Then

(1) \( g_0 \neq 0 \mbox{ in } F_q \).
(2) \( \dim(C) = n - d \)

(3) \[
G = \begin{pmatrix}
G_0 & G_1 & \ldots & G_d & 0 \\
G_0 G_1 & G_0 G_2 & \ldots & G_0 G_d & 0 \\
0 & G_0 & \ldots & G_0 G_d
\end{pmatrix}
\]
is a generator matrix for \( C \).

Proof: (1) We know that \( g(x) \) divides \( x^{n-1} \), say

\[
g(x) \cdot h(x) = x^{n-1}
\]

Assume \( g_0 = 0 \). Then \( g(0) = 0 \) but \( g(0) \cdot h(0) = -1 \), a contradiction. This proves (1).

To prove (2) and (3), we need to show that \( g(x), xg(x), \ldots, x^{n-1-d} g(x) \) form a basis of \( C \).

To see that these polynomials span \( C \), let \( f(x) \) be an arbitrary element of \( C \).
The check polynomial

Let \( C \) be a cyclic code with generator polynomial \( g(x) \). Then
\[
g(x) \cdot h(x) = x^n - 1 \quad \text{in} \quad \mathbb{F}_q[x].
\]

\( h(x) \) is called the check polynomial of \( C \). It is also monic (same as \( g(x) \)).

**Lemma:** \( f(x) \in C \) if and only if
\[
f(x) \cdot h(x) = 0 \quad \text{in} \quad \mathbb{R}_n.
\]

**Proof:** If \( f(x) \in C \), then \( f(x) = a(x)g(x) \) for some \( a(x) \in \mathbb{F}_q[x] \). Then
\[
f(x) \cdot h(x) = a(x)g(x)h(x) = a(x) \cdot (x^n - 1) = 0 \quad \text{in} \quad \mathbb{R}_n.
\]

Conversely, suppose \( f(x) \cdot h(x) = 0 \quad \text{in} \quad \mathbb{R}_n. \)
Want to show that \( f(x) \in C \), i.e., \( f(x) \) is a multiple of \( g(x) \).
That is, \( f(x) = a(x)g(x) \)
for some poly. \( a(x) \).

Divide \( a(x) \) by \( h(x) \) with remainder. Here \( h(x) \) is as in \( \bigcirc \).

\[
deg(h) = n-d
\]

\[
a(x) = q(x)h(x) + r(x)
\]

where \( \deg(r) < \deg(h) \). Now

\[
f(x) = a(x)g(x) = q(x)\underbrace{h(x)g(x)}_{=0 \text{ in } R_n} + r(x)g(x)
\]

Thus \( f(x) = r(x)g(x) \) in \( R_n \).

Write \( r(x) = \underbrace{r_0 + r_1x + \cdots + r_{n-d-1}x^{n-d-1}}_{R_{n-d-1}} \).

Now \( f(x) = r_0g(x) + r_1xg(x) + \cdots + r_{n-d-1}x^{n-d-1}g(x) \)

This shows that \( C = \text{Span}(g, xg, \ldots, x^{n-d-1}g) \).

To show that \( g, xg, \ldots, x^{n-d-1}g \) are lin. indep., note that by (1) the matrix 
\( G \) is in REF and has no zero rows.

Q.E.D.
Divide $f(x)$ by $g(x)$ with remainder

$$f(x) = q(x)g(x) + r(x), \quad \text{deg}(r(x)) < \text{deg}(g(x))$$

Now

$$0 = f(x)h(x) = q(x)g(x)h(x) + r(x)h(x) = 0 \text{ in } \mathbb{R}_n$$

$$0 = \frac{r(x)h(x)}{\text{degree } n}$$

Thus $r(x) = 0$, i.e. $f(x) = q(x)g(x) \in C$, as desired.

Q.E.D.

**Theorem:** Let $C$ be a cyclic code with check matrix polynomial

$$h(x) = h_0 + h_1x + \ldots + h_kx^k, \quad h_k = 1.$$ 

Then (1) $H = \left( \begin{array}{ccc} h_k & h_{k-1} & \cdots & h_0 \\ h_k & h_{k-1} & \cdots & h_0 \\ \vdots & \vdots & \ddots & \vdots \\ h_k & h_{k-1} & \cdots & h_0 \end{array} \right)$

is a parity check matrix for $C$. 


(2) \( C^⊥ \) is the cyclic code with generator polynomial \( h^{-1} \overline{h}(x) \), where
\[
\overline{h}(x) = h_k + h_{k-1}x + \ldots + h_1x^k = x^k h(x^{-1})
\]

**Proof of (1):** Let \( f(x) = f_0 + f_1x + \ldots + f_{n-1}x^{n-1} \).
Need to show that \( f(x) \cdot h(x) = 0 \) in \( \mathbb{F}_q \), if and only if
\( (f_0, f_1, \ldots, f_{n-1}) \) is orthogonal to every row of \( H \).

To be continued.