Last time

Recall that a linear code $C$ of length $n$ is cyclic if $(a_0, \ldots, a_{n-1}) \in C$, then $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ also lies in $C$.

Identify word $(a_0, \ldots, a_{n-1})$ in $\mathbb{F}_q^n$ with polynomial $a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ in $\mathbb{R}_n = \mathbb{F}_q[x] / (x^n - 1)$. Then $x a(x)$ is identified with $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$.

Cyclic codes in $\mathbb{R}_n$ are of the form $\langle g(x) \rangle = \text{span} \{ g(x), x g(x), \ldots, x^{n-1} g(x) \}$ where $g(x)$ is a polynomial of degree $d$ such that $g(x)$ is monic and divides $x^n - 1$. If $x^n - 1 = f_1(x) \cdots f_m(x)^{e_m}$ in $\mathbb{F}_q[x]$ where $f_1(x), \ldots, f_m(x)$ are distinct monic irreducible factors of $x^n - 1$, then
every monic polynomial \( g(x) \) which divides \( x^n - 1 \) is of the form

\[
g(x) = f_1(x)^{l_1} \cdots f_m(x)^{l_m}
\]

where 0 \( \leq l_1 \leq e_1 \), 0 \( \leq l_2 \leq e_2 \), \ldots, 0 \( \leq l_m \leq e_m \).

There are \( e_1 + 1 \) choices of \( l_1 \),
\( e_2 + 1 \) choices of \( l_2 \),
\( e_m + 1 \) choices of \( l_m \).

Thus there are

\[(e_1 + 1)(e_2 + 1) \cdots (e_m + 1)\]

choices of \( g(x) \),
and thus there are

\[(e_1 + 1)(e_2 + 1) \cdots (e_m + 1)\]

cyclic codes of length \( n \).

If \( g(x) = g_0 + g_1 x + \cdots + g_d x^d \), then by \( \circ \)

\[
G = \begin{pmatrix}
g_0 & g_1 & \cdots & g_d \\
g_0 & g_1 & \cdots & g_d \\
g_0 & g_1 & \cdots & g_d \\
g_0 & g_1 & \cdots & g_d \\
\end{pmatrix}
\]

is a generator matrix for \( C = \langle g(x) \rangle \).
Suppose \( g(x) h(x) = x^{n-1} \)
where \( h(x) = h_0 + h_1 x + \ldots + h_k x^k \).
Here \( k = \text{deg}(h) \), \( k + d = n \), \( d = \dim(C) \).

Proposition: (a) \( H = \begin{pmatrix} h_k & h_{k-1} & h_0 & 0 \\ 0 & h_k & h_{k-1} & h_0 \\ 0 & 0 & h_k & h_{k-1} & h_0 \end{pmatrix} \)

is a parity check matrix for \( C \).

(b) \( h(x) = h_k + h_{k-1} x + \ldots + h_0 x^k = x^k h(x^{-1}) \)
generates \( C^+ \). That is, \( C^+ = \langle h(x) \rangle \), \( h(x) \) is a polynomial of minimal degree in \( C^+ \), i.e., \( h^{-1} h(x) \) is the generator polynomial for \( C^+ \).

Proof: (a) Let \( f(x) = f_0 + f_1 x + \ldots + f_{n-1} x^{n-1} \).
Last time we showed that \( f(x) \in C \)
if and only if \( f(x) \cdot h(x) = 0 \) in \( \mathbb{R}_n \).
Now observe that $f(x) \cdot h(x) = 0$ in $R_n$ if and only if $f(x) \cdot h(x)$ has degree $\leq k-1$ (after reducing mod. $x^{n-1}$).

Indeed, 

suppose $f(x) \cdot h(x) - q(x)(x^{n-1})$

is of degree $\leq k-1$. Then factoring out $h(x)$, we see that

$$h(x)(f(x) - q(x)g(x))$$

is of deg. $\leq k-1$

has deg. $k$.

This is only possible if $q(x)g(x) = f(x)$, i.e., if $f(x) \in C$.

Now compute $f(x) \cdot h(x)$

$$f(x) \cdot h(x) = \ldots + x^k (k \alpha_k f_0 h_k + f_1 h_{k-1} + \ldots + f_k h_0)$$

$$+ x^{k+1} (f_1 h_k + f_2 h_{k-1} + \ldots + f_{k+1} h_0)$$

$$+ \ldots$$

$$+ x^{n-1} (f_{n-k-1} h_k + \ldots + f_{n-1} h_0)$$
Thus \( fe \in C \) if and only if
\[
\begin{align*}
fo h_k^* + f_1 h_{k-1} + \cdots + f_k h_0 &= 0 \\
f_1 h_k + \cdots + f_{k+1} h_0 &= 0 \\
fn-k h_k^* + fn-1 h_0 &= 0
\end{align*}
\]
or equivalently, the dot product of 
\((fo, \ldots, fn-1)\) with every row of \( H \) is 0.

(b) \( H \) is a generator matrix for the cyclic code \(<h(x)>\), provided that we can prove that \( h(x) \) divides \( x^n-1 \).
To show that \( h(x) \) divides \( x^n-1 \), note that
\[
\begin{align*}
\bar{h}(x) \cdot \bar{g}(x) &= x^n h(x^{-1}) x^{n-k} g(x^{-1}) \\
&= x^n g(x^{-1}) h(x^{-1}) = x^n (x^{-1})^{n-1} \\
&= 1 - x^n
\end{align*}
\]
This shows that \( h(x) \) divides \( x^n-1 \).
Q.E.D.
Another way to construct parity check matrix for $C = \langle g(x) \rangle$.
Reduce $1, x, x^2, \ldots, x^{n-1}$ modulo $g(x)$. Let us say, $\deg g(x) = d$, and $x^i \equiv r_i(x) \mod g(x)$, where $\deg r_i(x) \leq d-1$. Write

$$r_i(x) = a_{0i} + a_{1i} x + \ldots + a_{d-1i} x^{d-1}$$

**Proposition:** $H = (\overrightarrow{C}_0, \ldots, \overrightarrow{C}_{n-1})$, where $\overrightarrow{C}_i = \begin{pmatrix} a_{0i} \\ a_{1i} \\ \vdots \\ a_{d-1i} \end{pmatrix}$ is a parity check matrix for $C$. Moreover $H$ is in standard form.
Proof: Let \((a_0, \ldots, a_{n-1}) \in F_q^n\), denote it by \(\mathbf{a}\).

Then
\[
\mathbf{a} \cdot H^T = a_0 \mathbf{e}_0 + a_1 \mathbf{e}_1 + \cdots + a_{n-1} \mathbf{e}_{n-1}
\]

This column vector is 0 if and only if
\[
a_0^{(x)} + a_1 r_1(x) + \cdots + a_{n-1} r_{n-1}(x) = 0 \text{ in } F_q[x].
\]
But \(a_0 r_0(x) + a_1 r_1(x) + \cdots + a_{n-1} r_{n-1}(x)\)
is \(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}\) reduced modulo \(g(x)\).

Thus \(\mathbf{a} \cdot H^T = \mathbf{0}\) if and only if
\(a_0 r_0(x) + \cdots + a_{n-1} r_{n-1}(x)\) is the zero poly.

\(\uparrow\)

\((a_0, a_1, \ldots, a_{n-1}) \in C\). This means that \(H\) is a parity check matrix for \(C\).

\(H\) is in standard form by construction.
Theorem: \( d(C) = 7 \).

Proof: In the text.

Corollary: \( C \) is a perfect code of length 23, min. dist. 7.

Proof: Need to check: \( |C| = 2^{\text{dim}(C)} = 2^{12} \)
equals \[
\frac{2^{23}}{1 + 23 + \binom{23}{2} + \binom{23}{3}}
\]
\[
\binom{23}{2} = \frac{23 \cdot 22}{2} = 23 \cdot 11 \neq \]
\[
\binom{23}{3} = \frac{23 \cdot 22 \cdot 21}{3 \cdot 2} = 23 \cdot 11 \cdot 7
\]
\[
= \frac{2^{23}}{2048} = \frac{2^{23}}{2^{11}} = 2^{12}
\]

G.E.D.
There is also ternary Golay code $\langle g(x) \rangle = C$, where

$$x^6 - 1 = (1-x)g(x)\overline{g}(x) \text{ in } F_3[x]$$

$$g(x) = x^5 - x^3 + x^2 - x - 1.$$  

This code is perfect of min. dist. 5.

Theorem: Every non-trivial perfect code has the same as Hamming codes or Golay codes.

Here parameters mean $q, n, M, d$.

Trivial: $F_q^n$, a code with just one word, repetition codes of odd length.