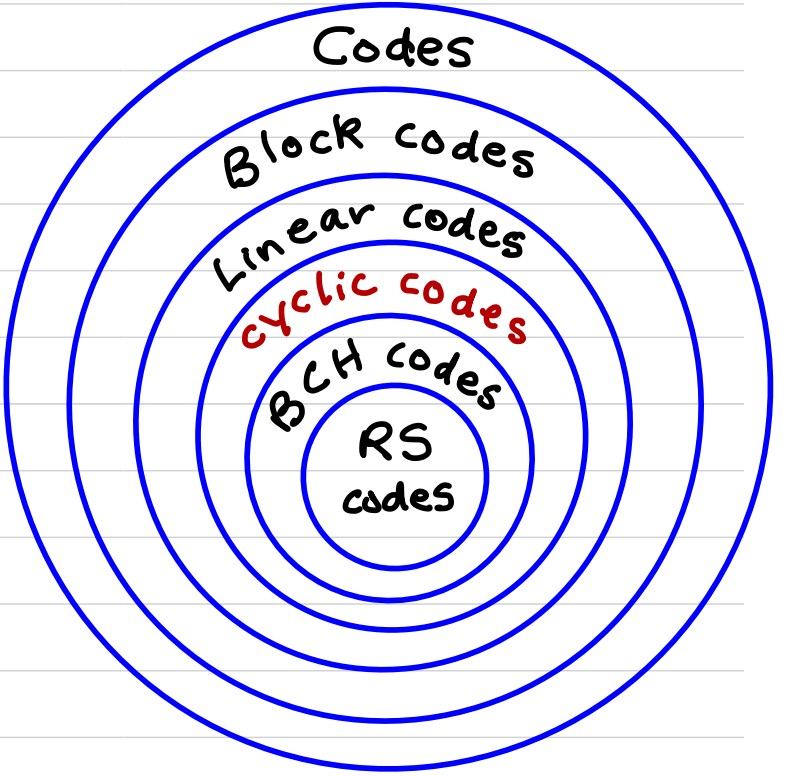
V5a Cyclic Codes

DEFINITION A subspace S of $V_n(F)$ is cyclic if $(a_0, a_1, \ldots, a_{n-1}) \in S$ implies that $(a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in S$.

A cyclic code is a cyclic subspace of $V_n(F)$.



NEXT GOAL:

An algebraic characterization of cyclic subspaces of $V_n(F)$ as ideals of the polynomial ring $R = F[x]/(x^n - 1)$.

THE POLYNOMIAL RING $R = F[x]/(x^n-1)$

- Let $R = F[x]/(x^n-1)$ where $F = GF(q)$. Then R is a commutative ring (but not a field since x^n-1 is reducible over F).

- We have the following bijection between $V_n(F)$ and R:

$$a = (a_0, a_1, a_2, \ldots, a_{n-1}) \longleftrightarrow a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}.$$

- This bijection preserves vector addition and scalar multiplication:
  If $a, b \in V_n(F)$ and $\lambda \in F$, then $a+b \longleftrightarrow a(x) + b(x)$
  and $\lambda a \longleftrightarrow \lambda a(x)$.

- We can use this bijection to define a natural multiplication on $V_n(F)$:

DEFINITION Let $a, b \in V_n(F)$. Then $a \cdot b = c \in V_n(F)$, where
$c \longleftrightarrow c(x) = a(x) \cdot b(x) \mod (x^n-1)$.

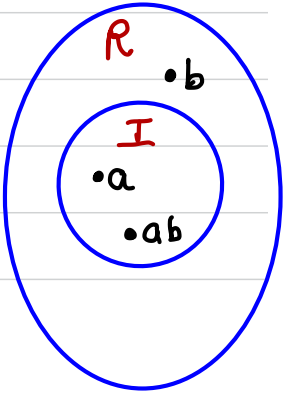
WHY CHOOSE x^n-1 AS THE MODULUS IN R?

- Let $a=(a_0,a_1,\ldots,a_{n-1}) \in V_n(F)$, and let $a(x)$ be the associated polynomial in R. Then

$$x\cdot a(x) = a_0x + a_1x^2 + \cdots\cdots + a_{n-2}x^{n-1} + a_{n-1}x^n$$
$$\equiv a_{n-1} + a_0x + a_1x^2 + \cdots + a_{n-2}x^{n-1} \pmod{x^n-1}$$
$$\longleftrightarrow (a_{n-1}, a_0, a_1, \ldots, a_{n-2}).$$

- So, multiplication by x of a polynomial in R corresponds to a (right) cyclic shift of the associated vector in $V_n(F)$.

DEFINITION Let R be a finite commutative ring. A non-empty subset I of R is an ideal of R if (i) $a,b\in I \Rightarrow a+b\in I$, and (ii) $a\in I, b\in R \Rightarrow a\cdot b\in I$.



EXAMPLE $\{0\}$ and R are (trivial) ideals of R.

THEOREM (algebraic characterization of cyclic subspaces of $V_n(F)$) Let S be a non-empty subset of $V_n(F)$, and let I be the set of associated polynomials in $R = F[x]/(x^n - 1)$. Then S is a cyclic subspace of $V_n(F)$ iff I is an ideal of R.

PROOF ($\Rightarrow$) Suppose S is a cyclic subspace of $V_n(F)$. Since S is non-empty and closed under addition, so is I. Now, let $a(x) \in I$ and $b(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} \in R$. Since S is a cyclic subspace, $x \cdot a(x) \in I$. Hence, $x^i a(x) \in I$ for all $0 \leq i \leq n-1$. Since S is closed under scalar multiplication, we have $b_i x^i a(x) \in I$ for all $0 \leq i \leq n-1$. Finally, since S is closed under addition, $\sum_{i=0}^{n-1} b_i x^i a(x) = b(x) a(x) \in I$. Thus, I is an ideal of R.

($\Leftarrow$) Suppose I is an ideal of R. Since I is non-empty and closed under addition, so is S. Since I is closed under multiplication by constant polynomials (i.e., elements of F), S is closed under scalar multiplication. Thus, S is a subspace of $V_n(F)$.
Finally, since I is closed under multiplication by x, S is closed under right cyclic shifts. Thus, S is a cyclic subspace of $V_n(F)$. □

So, to study cyclic subspaces of $V_n(F)$, we proceed to study ideals of $R = F[x]/(x^n-1)$.

V5b Ideals of $R = F[x]/(x^n - 1)$

Definitions Let R be a (finite commutative) ring, and let $g \in R$.

- Let $\langle g \rangle = \{g \cdot r : r \in R\}$. Then $\langle g \rangle$ is an ideal of R, called the ideal generated by g.
- An ideal I of R is principal if $I = \langle g \rangle$ for some $g \in I$.
- R is a principal ideal ring if every ideal of R is principal.

THEOREM $R = F[x]/(x^n - 1)$ is a principal ideal ring.

PROOF Let I be an ideal of R.

- If $I = \{0\}$, then $I = \langle 0 \rangle$.
- If $I \neq \{0\}$, then let $g(x)$ be a nonzero polynomial of smallest degree in I. We now show that $I = \langle g \rangle$.
  Let $h \in I$. We can write $h(x) = \ell(x)g(x) + r(x)$, where $\ell, r \in F[x]$ and $\deg(r) < \deg(g)$. Now, $h(x), \ell(x)g(x) \in I$ implies that $h(x) - \ell(x)g(x) \in I$, so $r(x) \in I$. But $\deg(r) < \deg(g)$, so we must have $r(x) = 0$. Thus, $h(x) = \ell(x)g(x)$, so $h \in \langle g \rangle$. Thus, $I \subseteq \langle g \rangle$.
  And, since $g \in I$, we have $\langle g \rangle \subseteq I$. Thus, $I = \langle g \rangle$. □

NOTE In the previous proof, we can take $g(x)$ to be monic, i.e. a polynomial whose leading coefficient is 1. This is because if $g(x) = g_0 + g_1 x + \cdots + g_t x^t \in I$ where $g_t \neq 0$, then $g_t^{-1} g(x) = g_0 g_t^{-1} + g_1 g_t^{-1} x + \cdots + x^t \in I$ is monic.

DEFINITION Let I be an ideal of $R = F[x]/(x^n - 1)$.

- If $I = \{0\}$, then $x^n - 1$ is the canonical generator of I.
- If $I \neq \{0\}$, then the monic polynomial of smallest degree in I is the canonical generator of I.

- The following theorem justifies the qualifier "the" in the above definition.

THEOREM Let I be a nonzero ideal of $R = F[x]/(x^n-1)$.
1) There is a unique monic poly. $g(x)$ of smallest degree in I, and $I = \langle g(x) \rangle$.
2) $g(x) \mid (x^n-1)$ in $F[x]$.

PROOF 1) Let $g(x), h(x)$ be monic polynomials of (the same) smallest degree in I. Then $g(x)-h(x) \in I$. But $\deg(g-h) < \deg(g)$. Hence $g(x)-h(x) = 0$, so $g(x) = h(x)$. This proves uniqueness of $g(x)$.
2) Write $x^n-1 = \ell(x)\, g(x) + r(x)$, where $\ell, r \in F[x]$, $\deg(r) < \deg(g)$.
Then $r(x) = -\ell(x)\, g(x) + x^n - 1 \equiv -\ell(x)\, g(x) \pmod{x^n-1}$.
Thus, $r(x) \in I = \langle g \rangle$, and so we must have $r(x) = 0$ since $\deg(r) < \deg(g)$. Hence $g(x) \mid (x^n-1)$. $\square$

THEOREM Let $h(x)$ be a monic divisor of x^n-1 in $F[x]$. Then $h(x)$ is the canonical generator of $I=\langle h(x)\rangle$.

PROOF • If $h(x)=x^n-1$, then $I=\{0\}$.

• Suppose that $h(x)\neq x^n-1$, so $I\neq\{0\}$. Let $g(x)$ be the monic polynomial of smallest degree in I. Since $h(x)$ generates I, we can write $g(x)=a(x)\,h(x) \mod(x^n-1)$ for some $a(x)\in F[x]$, $\deg(a)<n$.

Hence, $g(x)=a(x)\,h(x)+\ell(x)\,(x^n-1)$ for some $\ell(x)\in F[x]$.

Since $h(x)\mid(x^n-1)$, we have $h(x)\mid g(x)$, so $\deg(h)\leq\deg(g)$.

But $\deg(g)\leq\deg(h)$, so $\deg(g)=\deg(h)$.

Finally, since g and h are both monic, we have $g(x)=h(x)$.

Hence, $h(x)$ is the canonical generator of $\langle h(x)\rangle$. □

COROLLARY There is a 1-1 correspondence between ideals of R and monic divisors of x^n-1 over F, and thus also a 1-1 correspondence between cyclic subspaces of $V_n(F)$ and monic divisors of x^n-1 over F.

NOTE (monic divisors of x^n-1 over F)

Let $x^n-1 = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_t(x)^{e_t}$ be the complete factorization of x^n-1 over F, where $p_1, p_2, \ldots, p_t$ are monic irreducible polynomials in $F[x]$, and $e_i \geq 1$. Then the set of all monic divisors of x^n-1 over F is

$$\{ p_1(x)^{f_1} p_2(x)^{f_2} \cdots p_t(x)^{f_t} : 0 \leq f_i \leq e_i \}.$$

Hence, the number of monic divisors of x^n-1 over F is

$$(e_1+1)(e_2+1)\cdots(e_t+1).$$

EXAMPLE Find all cyclic subspaces of $V_3(\mathbb{Z}_2)$.

SOLUTION The complete factorization of x^3-1 over $\mathbb{Z}_2$ is

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

So, the monic divisors of x^3-1 over $\mathbb{Z}_2$ are

$$g_1(x)=1, \quad g_2(x)=x+1, \quad g_3(x)=x^2+x+1, \quad g_4(x)=(x+1)(x^2+x+1).$$

Hence, $V_3(\mathbb{Z}_2)$ has 4 cyclic subspaces.

CYCLIC SUBSPACE	DIMENSION
$\langle g_1(x)\rangle = S_1 = \{000, 001, 010, 011, 100, 101, 110, 111\} = V_3(\mathbb{Z}_2)$.	3
$\langle g_2(x)\rangle = S_2 = \{000, 110, 011, 101\}$.	2
$\langle g_3(x)\rangle = S_3 = \{000, 111\}$.	1
$\langle g_4(x)\rangle = S_4 = \{000\}$	0

V5C Dimension and a GM of a Cyclic Code

THEOREM Let $g(x)$ be a monic divisor of x^n-1 over F, where $F=GF(q)$. Suppose $\deg(g)=n-k$. Then the cyclic subspace S of $V_n(F)$ generated by $g(x)$ has dimension k.

PROOF Recall that $\langle g(x)\rangle = \{a(x)g(x) \bmod (x^n-1) : a(x)\in F[x], \deg(a)<n\}$. We claim that $\langle g(x)\rangle = \{b(x)g(x) : b(x)\in F[x], \deg(b)<k\}$. To see this, let $h(x)=a(x)g(x) \bmod (x^n-1)$ for some $a(x)\in F[x]$, $\deg(a)<n$. Then we can write $a(x)g(x) = h(x)+l(x)(x^n-1)$ for some $l(x)\in F[x]$. Since $g(x)\mid(x^n-1)$, we have $g(x)\mid h(x)$, so $h(x)=b(x)g(x)$ for some $b(x)\in F[x]$, $\deg(b)<k$. This proves the claim.
Finally since there are q^k polynomials of degree $<k$ in $F[x]$, $\langle g(x)\rangle$ has size q^k. Thus, S has dimension k. □

EXAMPLE Construct a $(7,4)$-cyclic code over $F=\mathbb{Z}_2$.

SOLUTION We need a monic divisor of x^7-1 over $\mathbb{Z}_2$ of degree 3.

Now, the complete factorization of x^7-1 over $\mathbb{Z}_2$ is

$$x^7-1=(x+1)(x^3+x+1)(x^3+x^2+1).$$

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

Then $C=\langle x^3+x^2+1\rangle$ is a $(7,4)$-cyclic code over $\mathbb{Z}_2$.

Let's find a GM for C. We need a basis for C, i.e. 4 linearly independent codewords in C. We can choose $g(x), xg(x), x^2g(x), x^3g(x)$ to get

$$G=\begin{bmatrix} 1&0&1&1&0&0&0 \\ 0&1&0&1&1&0&0 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&0&1&1 \end{bmatrix} \begin{matrix} \leftarrow g(x) \\ \leftarrow xg(x) \\ \leftarrow x^2g(x) \\ \leftarrow x^3g(x) \end{matrix}$$

NOTE: C is systematic

EXAMPLE (cont'd) Encode the message $m = 1001$.

SOLUTION

$$c = mG = [1\,0\,0\,1] \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = \underline{1010011}.$$

Equivalently, $c(x) = m(x)\,g(x)$

$$= (1 + x^3)(1 + x^2 + x^3)$$

$$= 1 + x^2 + x^5 + x^6$$

$$\leftrightarrow \underline{1010011}.$$

A GM FOR A CYCLIC CODE

THEOREM Let $g(x)$ be the canonical generator of an (n,k)-cyclic code C over F (so $g(x)$ is a monic divisor of x^n-1 over F of degree $n-k$). Then a (non-standard) GM for C is

$$G_1 = \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ \vdots \\ x^{k-1} g(x) \end{bmatrix}_{k \times n}.$$

ENCODING Source messages are the polynomials in $F[x]$ of degree $< k$. If $m(x) = m_0 + m_1 x + \cdots + m_{k-1} x^{k-1} \in F[x]$, then the encoding of m w.r.t. G_1 is $c = [m_0, m_1, \ldots, m_{k-1}]G_1 = m_0 g(x) + m_1 x g(x) + \cdots + m_{k-1} x^{k-1} g(x)$, so $\boxed{c(x) = m(x)\, g(x).}$ [NOTE: No reduction by x^n-1 is needed.]

SUMMARY

- $V_n(F) \longleftrightarrow R = F[x]/(x^n-1)$
- $a=(a_0,a_1,\dots,a_{n-1}) \in V_n(F) \longleftrightarrow a(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1} \in R$
- C cyclic subspace of $V_n(F) \longleftrightarrow I$ ideal of R
- $\dim(C)=k \longleftrightarrow$ The canonical generator of I has degree $n-k$.
- Encoding: $c=mG_1 \longleftrightarrow c(x)=m(x)g(x)$, where $G_1=\begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix}_{k\times n}$
- $C^\perp$ is cyclic $\overset{V5d}{\longleftrightarrow}$ The canonical generator is $h^*(x)$, where $h(x)=(x^n-1)/g(x)$.
- Syndrome w.r.t. $a \overset{V5e}{\longleftrightarrow} s(x)=r(x) \bmod g(x)$ particolar PCM
- MISSING: Distance of a cyclic code.

V5d The Dual Code of a Cyclic Code

- Let C be an (n,k)-cyclic code over F with canonical generator $g(x)$.
- Let $g(x) = \underbrace{g_0}_{\neq 0} + g_1 x + \cdots + \underbrace{g_{n-k}}_{=1} x^{n-k} + \underbrace{g_{n-k+1} x^{n-k+1} + \cdots + g_{n-1} x^{n-1}}_{=0}$.

Definition The parity-check polynomial of C is $h(x) = (x^n - 1)/g(x)$.

- Let $h(x) = \underbrace{h_0}_{\neq 0} + h_1 x + \cdots + \underbrace{h_k}_{=1} x^k + \underbrace{h_{k+1} x^{k+1} + \cdots + h_{n-1} x^{n-1}}_{=0}$.
- Let $a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} = g(x)\,h(x) \bmod (x^n - 1)$.

  Note that $a(x) = 0$. Equating coefficients of x^i for $0 \le i \le n-1$, gives:

  $$a_i = 0 = g_0 h_i + g_1 h_{i-1} + \cdots + g_i h_0 + g_{i+1} h_{n-1} + g_{i+2} h_{n-2} + \cdots + g_{n-1} h_{i+1}.$$
- Thus, the vector $g = (g_0, g_1, \ldots, g_{n-1})$ is orthogonal to the vector $\overline{h} = (h_{n-1}, h_{n-2}, \ldots, h_1, h_0)$ and all its cyclic shifts.

A PCM FOR C

- It follows that all cyclic shifts of g are orthogonal to all cyclic shifts of $\bar{h}$, where $\bar{h}(x) = h_{n-1} + h_{n-2}x + \cdots + h_2 x^{n-3} + h_1 x^{n-2} + h_0 x^{n-1}$.
- Recall the following GM for C:

$$G_1 = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & \cdots 0 \\ \vdots & & & & & \vdots & \\ 0 & \cdots & \cdots & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix}_{k \times n}.$$

- DEFINE:

$$H = \begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_0 & \cdots & 0 \\ \vdots & & & & & \vdots & \\ 0 & \cdots & \cdots & 0 & h_k & h_{k-1} & \cdots h_0 \end{bmatrix}_{(n-k) \times n}.$$

- From the above observation, we have $GH^T = 0$.
  Thus, $C' \subseteq C^\perp$, where C' is the code generated by the rows of H.
  But $\text{rank}(H) = n-k$ (since $h_k = 1$), so $\dim(C') = n-k = \dim(C^\perp)$.
  Hence, $C' = C^\perp$, and H is a (non-standard) PCM for C.

$C^\perp$ is CYCLIC

DEFINITION Let $h(x) = h_0 + h_1 x + \cdots + h_k x^k$ be a polynomial of degree k (so $h_k \neq 0$). The reciprocal polynomial of $h(x)$ is

$$h_R(x) = x^k h(1/x) = h_k + h_{k-1} x + \cdots + h_1 x^{k-1} + h_0 x^k.$$

If $h_0 \neq 0$, we define $h^*(x) = h_0^{-1} h_R(x)$. [$h^*(x)$ is monic]

THEOREM Let C be an (n,k)-cyclic code over F with canonical generator $g(x)$. Let $h(x) = (x^n - 1)/g(x)$. Then $C^\perp$ is cyclic, with canonical generator $h^*(x)$.

PROOF We have $g(x)h(x) = x^n - 1$, so $g(\frac{1}{x})h(\frac{1}{x}) = (\frac{1}{x})^n - 1$. Multiplying both sides by x^n gives $x^{n-k} g(\frac{1}{x}) x^k h(\frac{1}{x}) = -(x^n - 1)$. Hence $g_R(x) h_R(x) = -(x^n - 1)$, so $h_R(x) \mid (x^n - 1)$. Thus, $h^*(x)$ is a monic divisor of $x^n - 1$. We saw on slide 121 that the $(n, n-k)$-cyclic code generated by $h_R(x)$ (and thus also by $h^*(x)$) is $C^\perp$. □

V5e Computing Syndromes

- Let C be an (n,k)-cyclic code over F with canonical generator $g(x)$.
- We will find a "nice" PCM for C.

1) Find a GM for C of the form $[R \mid I_k]$.

For $0 \le i \le k-1$, long division gives $x^{n-k+i} = l_i(x)g(x) + r_i(x)$, $\deg(r_i) < n-k$, $\deg(l_i) < k$.

Then, $x^{n-k+i} - r_i(x) = l_i(x)g(x) \in C$.

Thus, a GM for C is:

$$G_1 = \underbrace{\begin{bmatrix} -r_0(x) + & x^{n-k} \\ -r_1(x) + & x^{n-k+1} \\ \vdots & \\ -r_{k-1} + & x^{n-1} \end{bmatrix}}_{\substack{n-k \\ k}} {}_{k\times n} = \underbrace{\left[\begin{array}{c} -x^{n-k} \bmod g(x) \\ -x^{n-k+1} \bmod g(x) \\ \vdots \\ -x^{n-1} \bmod g(x) \end{array}\right.}_{n-k} \underbrace{\left.\begin{array}{c} \\ \\ \\ \\ \end{array}\right]}_{k} {}_{k\times n} = [R \mid I_k].$$

NOTE: $\text{rank}(G_1) = k$.

a) A (standard form) PCM for C is $H = [I_{n-k} \mid -R^T]$.

Note that $H^T = \left[\frac{I_{n-k}}{-R}\right]$, so the rows of H^T (the columns of H) are $x^0 \bmod g(x)$, $x^1 \bmod g(x)$, ..., $x^{n-1} \bmod g(x)$.

THEOREM (computing syndromes) The syndrome of $r \in V_n(F)$ w.r.t. the above PCM is $s \in V_{n-k}(F)$, where $s(x) = r(x) \bmod g(x)$.

PROOF Let $r = (r_0, r_1, \ldots, r_{n-1}) \in V_n(F)$. The syndrome of r is $s = Hr^T$.

Hence $s(x) = [r_0 x^0 \bmod g(x)] + [r_1 x^1 \bmod g(x)] + \cdots + [r_{n-1} x^{n-1} \bmod g(x)]$

$= (r_0 + r_1 x + \cdots + r_{n-1} x^{n-1}) \bmod g(x)$

$= r(x) \bmod g(x)$. □

EXAMPLE Consider the $(15,9)$-binary cyclic code C with canonical generator $g(x)=1+x+x^2+x^3+x^6$. Compute the syndrome of $r=(1100\ 1000\ 1110\ 000)$.

SOLUTION $r(x)=1+x+x^4+x^8+x^9+x^{10}$.

$$
\begin{array}{r|l}
 & x^4+x^3+x^2+x \quad \leftarrow r(x) \\
\hline
x^6+x^3+x^2+x+1 \ (g(x)) & x^{10}+x^9+x^8+x^4+x+1 \\
 & x^{10}+x^7+x^6+x^5+x^4 \\
\hline
 & x^9+x^8+x^7+x^6+x^5+x+1 \\
 & x^9+x^6+x^5+x^4+x^3 \\
\hline
 & x^8+x^7+x^4+x^3+x+1 \\
 & x^8+x^5+x^4+x^3+x^2 \\
\hline
 & x^7+x^5+x^2+x+1 \\
 & x^7+x^4+x^3+x^2+x \\
\hline
s(x) \rightarrow & x^5+x^4+x^3+1
\end{array}
$$

$$
\begin{array}{r|l}
 & 1\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1 \\
\hline
1\,0\,0\,1\,1\,1\,1 & \\
 & 1\,0\,0\,1\,1\,1\,1 \\
\hline
 & 1\,1\,1\,1\,1\,0\,0\,0\,1\,1 \\
 & 1\,0\,0\,1\,1\,1\,1 \\
\hline
 & 1\,1\,0\,0\,1\,1\,0\,1\,1 \\
 & 1\,0\,0\,1\,1\,1\,1 \\
\hline
 & 1\,0\,1\,0\,0\,1\,1\,1 \\
 & 1\,0\,0\,1\,1\,1\,1 \\
\hline
 & 1\,1\,1\,0\,0\,1
\end{array}
$$

Hence, $s=100111$.

- The syndromes of a vector and its cyclic shifts are closely related.

THEOREM Let $r \in V_n(F)$ with syndrome polynomial $S(x) = S_0 + S_1 x + \cdots + S_{n-k-1} x^{n-k-1}$.
The syndrome of $xr(x)$ is (i) $xS(x)$, if $S_{n-k-1} = 0$
(ii) $xS(x) - S_{n-k-1} g(x)$, if $S_{n-k-1} \neq 0$.

cyclic shift of r

not cyclic shifts

PROOF Since $r(x)$ has syndrome $S(x)$, we have $r(x) = l(x)g(x) + S(x)$ for some $l \in F[x]$. Hence, $xr(x) = xl(x)g(x) + xS(x)$. Since $g(x) | (x^n - 1)$, $xr(x)$ and $xr(x) \bmod (x^n - 1)$ leave the same remainder upon division by $g(x)$.

(i) If $S_{n-k-1} = 0$, then $\deg(S) < n-k-1$, so $\deg(xS) < n-k$. Hence, $xS(x)$ is the (unique) remainder upon dividing $xr(x)$ by $g(x)$.

(ii) If $S_{n-k-1} \neq 0$, then $xr(x) = xl(x)g(x) + xS(x) - S_{n-k-1}g(x) + S_{n-k-1}g(x)$
$= [xl(x) + S_{n-k-1}]g(x) + [xS(x) - S_{n-k-1}g(x)]$. Notice that $\deg(\bar{S}) < n-k$, so $\bar{S}(x)$ is the unique remainder upon dividing $xr(x)$ by $g(x)$. $\square$

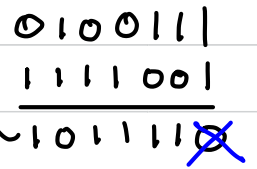
$\bar{S}(x)$

- So, given the syndrome s of t, we can easily compute the syndromes of cyclic shifts of t.

- **EXAMPLE** (continuing the example on Slide 125)

$g(x) = x^6 + x^3 + x^2 + x + 1 \leftrightarrow 1111001$, $t = 1100\ 1000\ 1110\ 000$, $s = 100111$.

i	$s_i(x)$ = syndrome of $x^i t(x)$
0	100111
1	101111
2	101011
3	101001
4	101000
5	010100
6	001010
7	000101
⋮	⋮



V5f Burst Error Correction

- Cyclic codes are good for correcting burst errors.

DEFINITION Let $e \in V_n(F)$. The cyclic burst length of e is the length of the shortest cyclic block of e that contains all its nonzero components.

EXAMPLE The cyclic burst length of $e = 0110100010$ is 7.

DEFINITION A linear code C is a t-cyclic burst error correcting code if all cyclic burst errors of length $\leq t$ are in different cosets of C, i.e. have different syndromes. The largest such t is called the cyclic burst error correcting capability of C.

EXAMPLE $g(x) = x^6 + x^3 + x^2 + x + 1$ is the canonical generator for a $(15, 9)$-binary cyclic code C. In fact, C is a 3-cyclic burst error correcting code. To check this, we verify that all cyclic bursts of length ≤ 3 have different syndromes.

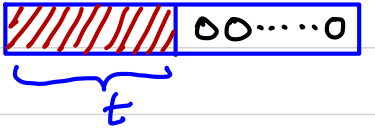
cyclic burst error	Syndrome	Integer representation
0	000000	0
x^0	100006	32
x^1	010000	16
x^2	001000	8
x^3	000106	4
x^4	000010	2
x^5	000001	1
x^6	111100	60
x^7	011110	30
x^8	001111	15
x^9	111011	59
x^{10}	100001	33
x^{11}	101100	44
x^{12}	010110	22
x^{13}	001011	11
x^{14}	111001	57
$1+x$	110000	48
$x(1+x)$	011000	24
⋮	⋮	⋮
$x^{14}(1+x)$	011001	25
$1+x+x^2$	111000	56
$x(1+x+x^2)$	011100	28
⋮	⋮	⋮
$x^{14}(1+x+x^2)$	001001	9
$1+x^2$	101000	40
$x(1+x^2)$	010100	20
⋮	⋮	⋮
$x^{14}(1+x^2)$	101001	41

EXAMPLE $g(x) = x^8+x^7+x^6+x^4+1$ is the canonical generator for a $(15,7)$-binary cyclic code C. C is a 4-cyclic burst error correcting code.

THEOREM (bounds on t, the cyclic burst error correcting capability of C)
Let C be an (n,k,d)-code over $F=GF(q)$. Then $\lfloor (d-1)/2 \rfloor \leq t \leq n-k$.

PROOF • Recall that the vectors of weight $\leq \lfloor (d-1)/2 \rfloor$ lie in different cosets of C. In particular, all cyclic burst errors of length $\leq \lfloor (d-1)/2 \rfloor$ lie in different cosets of C. Thus, $t \geq \lfloor (d-1)/2 \rfloor$.

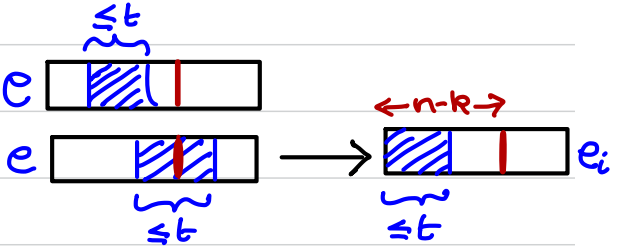
• No two cyclic burst errors of length $\leq t$ lie in the same coset of C. In particular, no two vectors in which all the nonzero components are in the first t coordinate positions can lie in the same coset of C. Since there are q^t such vectors and q^{n-k} cosets, we must have $q^t \leq q^{n-k}$. Hence, $t \leq n-k$. □



V5g DECODING ALG. FOR CYCLIC BURST ERROR CORRECTING CODES

- Let C be an (n,k)-cyclic code over F with canonical generator $g(x)$. Let t be the cyclic burst error correcting capability of C, so $t \le n-k$.
- Recall that $H=[I_{n-k}|-R^T]$ is a standard form PCM for C. The syndrome of $r \in V_n(F)$ w.r.t. this PCM is $s(x)=r(x) \bmod g(x)$.

- IDEA OF DECODING ALGORITHM Suppose the error vector e is a cyclic burst of length $\le t$. Then, some cyclic shift of e, say $e_i \longleftrightarrow x^i e(x)$, has all its nonzero components in the first $n-k$ coordinate positions. Then $s_i = He_i^T$ has (non)-cyclic burst length $\le t$, and $x=(s_i,0)$ satisfies $Hx^T=s_i$. Thus, $e_i=(s_i,0)$ and $e(x)=x^{n-i}e_i(x)$.



QUESTION How to compute s_i? Let $r = c + e$, so $x^i r - x^i e = x^i c \in C$. Thus, $x^i r$ and $x^i e$ have the same syndrome. So, we compute syndromes of $r_i \longleftrightarrow x^i r(x)$ for $0 \le i \le n-1$.

ERROR TRAPPING ALGORITHM FOR CYCLIC BURST ERROR CORRECTING CODES

- Let r be the received word.
- For i from 0 to $n-1$ do:
  - Compute $s_i(x)$, the syndrome of $x^i r(x)$.
  - If $s_i(x)$ has non-cyclic burst length $\le t$ then
    - Let $e(x) = x^{n-i}(s_i, 0)$.
    - Decode r to $c = r - e$ and STOP.
- Reject r.

CORRECTNESS

If the error vector is in fact a cyclic burst error of length $\le t$, then the algorithm will make the correct decision.

EXAMPLE Recall that $g(x) = x^6 + x^3 + x^2 + x + 1$ is the canonical generator for a $(15,9)$-binary cyclic code with cyclic burst error correcting capability $t = 3$. Decode $r = 1110\ 1110\ 1100\ 000$ using error trapping.

SOLUTION

i	$S_i(x)$ = syndrome of $x^i r(x)$
0	110011 ← $S(x) = r(x) \bmod g(x)$
1	100101
2	101110
3	010111
4	101111
5	100111
6	101111
7	101011
8	101001
9	101000

→ burst of length ≤ 3

- So, $e(x) = x^{15-9} S_9(x)$
  $= x^6(1 + x^2)$
  $= 0000\ 0010\ 1000\ 000.$
- Decode r to $c = r - e$
  $= 1110\ 1100\ 0100\ 000$
- Check: $g(x) \mid c(x)$.

INTERLEAVING

PURPOSE: Increase the cyclic burst error correcting capability of a code.

- Let C be an (n,k)-code with cyclic burst error correcting capability t.

Suppose $c_1 = (c_{11}, c_{12}, \ldots, c_{1n}) \in C$,
$c_2 = (c_{21}, c_{22}, \ldots, c_{2n}) \in C$,
$\vdots$
$c_s = (c_{s1}, c_{s2}, \ldots, c_{sn}) \in C$.

- Interleaving to a depth s: Instead of sending $c_1, c_2, \ldots, c_s$ in that order, transmit the columns of the above array:

$$c^* = (c_{11}, c_{21}, \ldots, c_{s1}, \mid c_{12}, c_{22}, \ldots, c_{s2}, \mid \ldots\ldots, \mid c_{1n}, c_{2n}, \ldots, c_{sn}).$$

Then, any cyclic burst error of length $\leq st$ in c^* results in cyclic burst errors of length $\leq t$ in each of the original codewords $c_1, c_2, \ldots, c_s$ (and these errors can be corrected).

THEOREM (interleaving) Let C be an (n,k)-code over F with cyclic burst error correcting capability t. Let C^* be the code obtained by interleaving C to a depth s.

1) C^* is an (ns,ks)-code over F with cyclic burst error correcting capability ts.

2) Suppose C is cyclic with canonical generator $g(x)$. Then C^* is cyclic with canonical generator $g(x^s)$.

PROOF (sketch) 1) Show that C^* is a vector subspace, has length ns, size q^{ks} (so dimension ks), and cyclic burst error correcting ts.

2) Show that $g(x^s)$ is a monic divisor of $x^{ns}-1$ of degree $ns-ks$, and that $g(x^s) \mid c^*(x)$ for all $c^* \in C^*$. □

EXAMPLE (cf. slide 133) $g(x^{100}) = x^{600}+x^{300}+x^{200}+x^{100}+1$ is the canonical generator of a $(1500, 900)$-binary cyclic code with cyclic burst error correcting capability $t=300$.