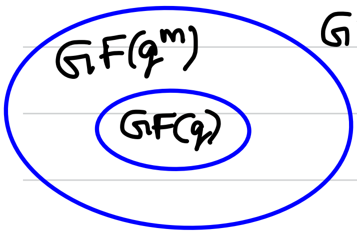
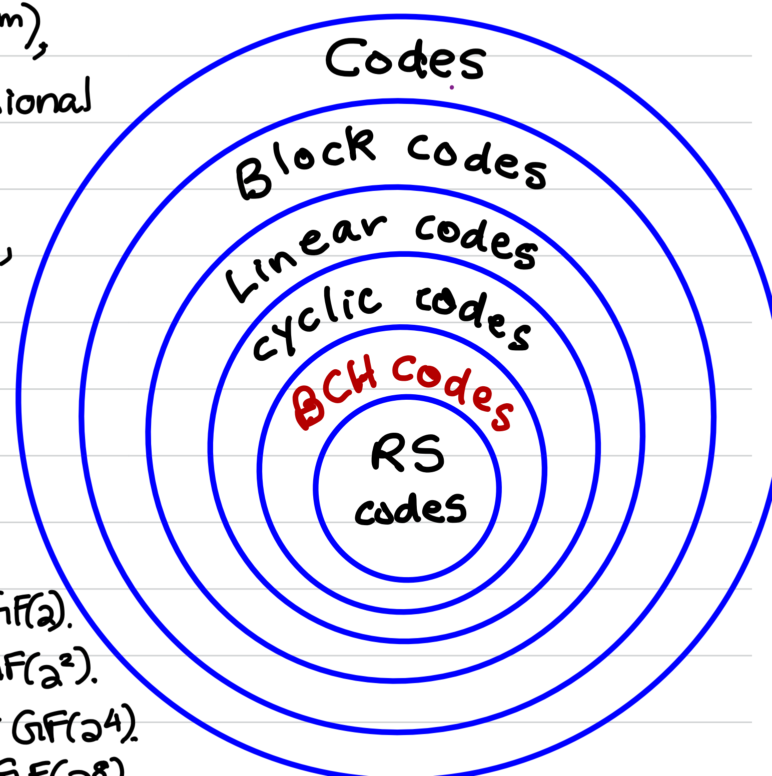
V6a BCH CODES

- Recall that $\mathbb{Z}_p$ is a subfield of $GF(p^m)$, and we can view $GF(p^m)$ as an m-dimensional vector space over $\mathbb{Z}_p$.
- More generally, for any prime power q,

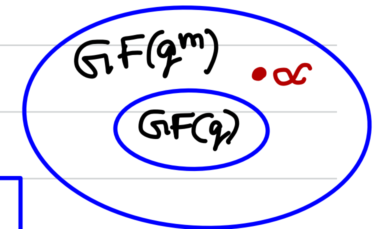


$GF(q)$ is a subfield of $GF(q^m)$, and we can view $GF(q^m)$ as an m-dimensional vector space over $GF(q)$.



- EXAMPLE
  - $GF(2^{16})$ is a 16-dimensional v.s. over $GF(2)$.
  - " " an 8-dimension v.s. over $GF(2^2)$.
  - " " a 4-dimensional v.s. over $GF(2^4)$.
  - " " a 2-dimensional v.s. over $GF(2^8)$.
  - " " a 1-dimensional v.s. over $GF(2^{16})$.

MINIMAL POLYNOMIALS



• We call $GF(q^m)$ an extension field and $GF(q)$ a subfield.

DEFINITION Let $\alpha \in GF(q^m)$. The minimal polynomial of α over $GF(q)$, denoted $m_\alpha(y)$, is the monic polynomial of smallest degree in $GF(q)[y]$ that has α as a root.

NOTES 1) If $m(y) \in GF(q)[y]$ is a nonzero polynomial with $m(\alpha)=0$, and c is its leading coefficient, then $\bar{m}(y) = c^{-1} m(y)$ is a monic polynomial in $GF(q)[y]$ with $\bar{m}(\alpha)=0$ and $\deg(\bar{m}) = \deg(m)$.

2) More generally, multiplying a polynomial by a nonzero constant does not change the roots of the polynomial.

3) We have $m_0(y) = y$.

4) If $\alpha \neq 0$, then let t be the order of α in $GF(q^m)$, and recall that $t \mid (q^m - 1)$. Then, α is a root of $y^t - 1 \in GF(q)[y]$. Hence, there does indeed exist a monic polynomial of smallest degree in $GF(q)[y]$ having α as a root.

EXAMPLE Let's find the minimal polynomials over $GF(2)$ of elements in $GF(2^2) = \mathbb{Z}_2[x]/(x^2+x+1) = \{0, 1, x, x+1\}$.

SOLUTION
- $m_0(y) = y$.
- $m_1(y) = y+1$,
- $m_x(y) = y^2+y+1$,
- $m_{x+1}(y) = y^2+y+1$,

PROPERTIES OF MINIMAL POLYNOMIALS

THEOREM Let $\alpha \in GF(q^m)$.

1) The minimal polynomial $m_\alpha(y)$ of α over $GF(q)$ is unique.
2) $m_\alpha(y)$ is irreducible over $GF(q)$.
3) $\deg(m_\alpha) \leq m$.
4) If $f \in GF(q)[y]$, then $f(\alpha) = 0 \iff m_\alpha(y) \mid f(y)$.

PROOF 1) Suppose $m_1(y), m_2(y) \in GF(q)[y]$ are two monic polynomials of the same smallest degree with $m_1(\alpha) = m_2(\alpha) = 0$. Consider $r(y) = m_1(y) - m_2(y)$. Then $r(\alpha) = m_1(\alpha) - m_2(\alpha) = 0$. But $\deg(r) < \deg(m_1)$, so we must have $r(y) = 0$. Hence, $m_1(y) = m_2(y)$. $\square$

- **PROOF OF 2)** Suppose that $m_\alpha(y)$ is reducible over $GF(q)$, say $m_\alpha(y) = s(y)t(y)$ where $s, t \in GF(q)[y]$ and $1 \leq \deg(s), \deg(t) < \deg(m_\alpha)$. Then $m_\alpha(\alpha) = s(\alpha)t(\alpha) = 0$, so either $s(\alpha) = 0$ or $t(\alpha) = 0$. In either case we have a contradiction of the minimality of $\deg(m_\alpha)$. We conclude that $m_\alpha(y)$ is irreducible over $GF(q)$. $\square$

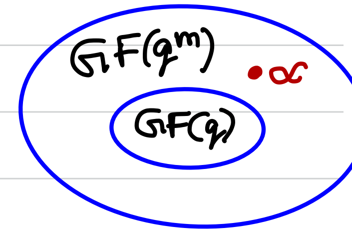
- **PROOF OF 3)** Recall that $GF(q^m)$ is an m-dimensional vector space over $GF(q)$. So, the field elements $1, \alpha, \alpha^2, \ldots, \alpha^m$ are linearly dependent over $GF(q)$. Thus, we can write $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_m\alpha^m = 0$ for some $a_0, a_1, \ldots, a_m \in GF(q)$ that are not all 0. Hence, α is a root of the nonzero polynomial
$$m(y) = a_0 + a_1 y + a_2 y^2 + \cdots + a_m y^m \in GF(q)[y]$$
of degree $\leq m$. It follows that $\deg(m_\alpha) \leq m$. $\square$

- **PROOF OF 4)** Let $f(y) \in GF(q)[y]$. By long division, we can write $f(y) = l(y)\, m_\alpha(y) + r(y)$, where $l, r \in GF(q)[y]$ and $\deg(r) < \deg(m_\alpha)$.
  Now, $f(\alpha) = l(\alpha)\, m_\alpha(\alpha) + r(\alpha) = r(\alpha)$ (since $m_\alpha(\alpha) = 0$).
  Hence, $f(\alpha) = 0 \iff r(\alpha) = 0$

  $\iff r(y) = 0$ (since $\deg(r) < \deg(m_\alpha)$)

  $\iff m_\alpha(y) \mid f(y)$. $\square$

V6b Computing Minimal Polynomials



- We will show that the roots of $m_\alpha(y)$ are precisely the "conjugates" of α over $GF(q)$.
- We'll need the following result.

THEOREM Let $\alpha \in GF(q^m)$. Then $\alpha \in GF(q)$ iff $\alpha^q = \alpha$.

PROOF Since $\beta^q = \beta$ for all $\beta \in GF(q)$, the elements of $GF(q)$ are all roots of the polynomial $Y^q - Y \in GF(q)[Y]$. Since this polynomial has degree q, it can't have any other roots in $GF(q^m)$. Thus, $\alpha^q = \alpha$ iff $\alpha \in GF(q)$. $\square$

DEFINITION Let $\alpha \in GF(q^m)$. Let t be the smallest positive integer such that $\alpha^{q^t} = \alpha$ (note: $t \leqslant m$). Then the set of conjugates of α w.r.t. $GF(q)$ is $C(\alpha) = \{\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{t-1}}\}$.

NOTE The t conjugates in $C(\alpha)$ are distinct. This is because if $\alpha^{q^i}=\alpha^{q^j}$ where $0\leq i<j\leq t-1$, then $\alpha^{q^j}-\alpha^{q^i}=0$, so $(\alpha^{q^{j-i}}-\alpha)^{q^i}=0$. Hence $\alpha^{q^{j-i}}-\alpha=0$, so $\alpha^{q^{j-i}}=\alpha$, which contradicts the minimality of t.

THEOREM Let $\alpha\in GF(q^m)$. Then the minimal polynomial of α over $GF(q)$ is $m(y)=\prod_{\beta\in C(\alpha)}(y-\beta)=(y-\alpha)(y-\alpha^q)(y-\alpha^{q^2})\cdots(y-\alpha^{q^{t-1}})$.

PROOF i) Clearly, $m(y)$ is monic and $m(\alpha)=0$.

ii) Let $f\in GF(q)[y]$, $f\neq 0$, with $f(\alpha)=0$. Let's prove that $\deg(f)\geq t$.

Let $f(y)=\sum_{i=0}^{d} f_i y^i$. Then $f(\alpha^q)=\sum_{i=0}^{d} f_i\alpha^{iq}=\left(\sum_{i=0}^{d} f_i\alpha^i\right)^q=f(\alpha)^q=0$.

So, $\alpha,\alpha^q,\alpha^{q^2},\ldots,\alpha^{q^{t-1}}$ are roots of f. Hence $\deg(f)\geq t$.

PROOF (cont'd)

iii) Let $m(y) = \prod_{\beta \in C(\alpha)} (y-\beta) = \sum_{i=0}^{t} m_i y^i$. Then $m(y) \in GF(q^m)[y]$.

We need to prove that $m(y) \in GF(q)[y]$.

Now, $m(y)^q = \prod_{\beta \in C(\alpha)} (y-\beta)^q = \prod_{\beta \in C(\alpha)} (y^q - \beta^q) = \prod_{\beta \in C(\alpha)} (y^q - \beta)$

$= m(y^q) = \sum_{i=0}^{t} m_i y^{iq}$. (*)

Also, $m(y)^q = \left(\sum_{i=0}^{t} m_i y^i \right)^q = \sum_{i=0}^{t} m_i^q y^{iq}$. (**)

Comparing coefficients of y^{iq} of (*) and (**) yields $m_i^q = m_i$ for $0 \le i \le t$. Thus, $m_i \in GF(q)$, and so $m(y) \in GF(q)[y]$.

iv) We conclude that $m(y)$ is a monic polynomial of smallest degree in $GF(q)[y]$ that has α as a root. $\square$

EXAMPLE Consider $GF(2^4) = \mathbb{Z}_2[x]/(x^4+x+1)$. Find the minimal polynomial of $\beta = x^3+x^2$ over $\mathbb{Z}_2$. (Here, $q=2$, $m=4$).

SOLUTION When doing computations by hand, it's useful to have a generator α of $GF(2^4)^*$, and a table of powers of α. It turns out that $\alpha = x$ is a generator of $GF(2^4)^*$.

Now, $\beta = \alpha^6$. Hence $C(\beta) = \{\alpha^6, \alpha^{12}, \alpha^9, \alpha^3\}$ (so $t=4$).

Thus,
$$
\begin{aligned}
m_\beta(y) &= (y-\alpha^6)(y-\alpha^{12})(y-\alpha^9)(y-\alpha^3) \\
&= [y^2-(\alpha^6+\alpha^{12})y+\alpha^{18}][y^2-(\alpha^9+\alpha^3)y+\alpha^{12}] \\
&= [y^2+\alpha^4 y+\alpha^3][y^2+\alpha y+\alpha^{12}] \\
&= y^4+(\alpha+\alpha^4)y^3+(\alpha^{12}+\alpha^5+\alpha^3)y^2+(\alpha^{16}+\alpha^4)y+\alpha^{15} \\
&= \underline{y^4+y^3+y^2+y+1}.
\end{aligned}
$$

$$
\boxed{
\begin{aligned}
\alpha^0 &= 1 \\
\alpha^1 &= \alpha \\
\alpha^2 &= \alpha^2 \\
\alpha^3 &= \alpha^3 \\
\alpha^4 &= \alpha+1 \\
\alpha^5 &= \alpha^2+\alpha \\
\alpha^6 &= \alpha^3+\alpha^2 \\
\alpha^7 &= \alpha^3+\alpha+1 \\
\alpha^8 &= \alpha^2+1 \\
\alpha^9 &= \alpha^3+\alpha \\
\alpha^{10} &= \alpha^2+\alpha+1 \\
\alpha^{11} &= \alpha^3+\alpha^2+\alpha \\
\alpha^{12} &= \alpha^3+\alpha^2+\alpha+1 \\
\alpha^{13} &= \alpha^3+\alpha^2+1 \\
\alpha^{14} &= \alpha^3+1 \\
\alpha^{15} &= 1
\end{aligned}
}
$$

V6C FACTORING x^n-1 OVER $GF(q)$ [Part 1]

GOAL Describe the factorization of x^n-1 over $GF(q)$. From this, we will see how canonical generators $g(x)$ can by chosen so that we have a non-trivial lower bound on the distance of the cyclic code generated by $g(x)$.

PRELIMINARIES Let p be the characteristic of $GF(q)$. If $\gcd(n,q)\neq 1$, then write $n=\bar{n}p^{\ell}$ where $\ell\geq 1$ and $\gcd(\bar{n},q)=1$.

Then $x^n-1 = x^{\bar{n}p^{\ell}}-1 = (x^{\bar{n}}-1)^{p^{\ell}}$. So, WLOG, we shall assume $\gcd(n,q)=1$.

NOTATION Let m be the smallest positive integer such that $q^m\equiv 1 \pmod{n}$, i.e. $n\mid(q^m-1)$. [FACT: such an m exists.]

Let α be a generator of $GF(q^m)^*$.

Let $\beta=\alpha^{(q^m-1)/n}$, and note that $\beta\in GF(q^m)$.

- Also, $\mathrm{ord}(\beta)=n$, and so $1, \beta, \beta^2, \ldots, \beta^{n-1}$ are distinct.
  Furthermore, $(\beta^i)^n = (\beta^n)^i = 1^i = 1$ for each $0 \le i \le n-1$.
  Hence, $1, \beta, \beta^2, \ldots, \beta^{n-1}$ are roots of x^n-1. So, the complete factorization of x^n-1 over $GF(q^m)$ is $x^n-1 = (x-1)(x-\beta)(x-\beta^2)\cdots(x-\beta^{n-1})$.

- However, we seek the factorization of x^n-1 over $GF(q)$.

- Consider β^i, where $0 \le i \le n-1$.
  Since β^i is a root of x^n-1, we have $m_{\beta^i}(x) \mid (x^n-1)$.
  Also, the roots of $m_{\beta^i}(x)$ are $C(\beta^i) = \{\beta^i, \beta^{iq}, \beta^{iq^2}, \ldots, \beta^{iq^{t-1}}\}$, where t is the smallest positive integer such that

$$\boxed{iq^t \equiv i \pmod{n}.}$$

CYCLOTOMIC COSETS

- The discussion on the previous slides motivates the following definition.

DEFINITION Suppose that $\gcd(n,q)=1$, and let $0 \le i \le n-1$. The cyclotomic coset of q mod n containing i is

$$C_i = \{i,\ iq \bmod n,\ iq^2 \bmod n, \ldots,\ iq^{t-1} \bmod n\},$$

where t is the smallest positive integer such that $iq^t \equiv i \pmod{n}$.
Also, $C = \{C_i : 0 \le i \le n-1\}$ is the set of cyclotomic cosets of q mod n.

- **EXAMPLE** The cyclotomic cosets of 2 mod 15 ($q=2$, $n=15$) are:

$C_0 = \{0\}$, $C_1 = \{1,2,4,8\} = C_2 = C_4 = C_8$,
$C_3 = \{3,6,12,9\} = C_6 = C_{12} = C_9$, $C_5 = \{5,10\} = C_{10}$,
$C_7 = \{7,14,13,11\} = C_{14} = C_{13} = C_{11}$. Hence $C = \{C_0, C_1, C_3, C_5, C_7\}$.

- As the example suggests, $\boxed{\text{if } j \in C_i, \text{ then } C_j = C_i.}$

- **NOTE:** $m_{\beta^i}(x) = (x-\beta^i)(x-\beta^{iq})(x-\beta^{iq^2})\cdots(x-\beta^{iq^{t-1}}) = \prod_{j \in C_i} (x-\beta^j)$

  is a monic irreducible factor of $x^n - 1$ over $GF(q)$ of degree $|C_i|$.

- This proves the following theorem.

THEOREM Suppose that $\gcd(n,q)=1$.

1) The number of monic irreducible factors of x^n-1 over $GF(q)$ is equal to the number of (distinct) cyclotomic cosets of q mod n.
2) The number of monic irreducible factors of degree d is equal to the number of (distinct) cyclotomic cosets of q mod n of size d.

V6d FACTORING x^n-1 OVER $GF(q)$ [Part 2]

THEOREM Suppose $\gcd(n,q)=1$. Let m be the smallest positive integer such that $q^m \equiv 1 \pmod{n}$, and let $\beta \in GF(q^m)$ be an element of order n. Then the monic irreducible factors of x^n-1 over $GF(q)$ are $\{m_{\beta^i}(x) : 0 \le i \le n-1\}$, where

$$\boxed{m_{\beta^i}(x) = \prod_{j \in C_i} (x-\beta^j).}$$

NOTE: If $j \in C_i$, then $m_{\beta^j}(x) = m_{\beta^i}(x)$.

EXAMPLE Factor $x^{15}-1$ over $\mathbb{Z}_2$. (Here $q=2$, $n=15$.)

SOLUTION • The cyclotomic cosets of 2 mod 15 are $C_0=\{0\}$, $C_1=\{1,2,4,8\}$, $C_3=\{3,6,12,9\}$, $C_5=\{5,10\}$, $C_7=\{7,14,13,11\}$. So, $x^{15}-1$ has 5 irreducible factors over $\mathbb{Z}_2$, one of degree 1, one of degree 2, and three of degree 4.

• The smallest m for which $2^m \equiv 1 \pmod{15}$ is $m=4$.

• We need an element $\beta \in GF(2^4)$ of order 15. see slide 145

Let's take $\beta=\alpha$, since α is a generator for $GF(2^4)=\mathbb{Z}_2[\alpha]/(\alpha^4+\alpha+1)$.

• We then compute:

$$m_{\beta^0}(x) = x+1 \quad C_0=\{0\}$$

$$m_{\beta}(x) = x^4+x+1 \quad C_1=\{1,2,4,8\}$$

See slide 145

$$m_{\beta^3}(x) = x^4+x^3+x^2+x+1 \quad C_3=\{3,6,12,9\}$$

$$m_{\beta^5}(x) = x^2+x+1 \quad C_5=\{5,10\}$$

$$m_{\beta^7}(x) = x^4+x^3+1 \quad C_7=\{7,14,13,11\}.$$

• Thus, $\underline{x^{15}-1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)}$.

EXAMPLE Determine the number of cyclic subspaces of $V_{90}(\mathbb{Z}_3)$.

SOLUTION • First, we observe that $x^{90}-1=(x^{10}-1)^9$.

• To determine the factorization pattern of $x^{10}-1$ over $\mathbb{Z}_3$, we find the cyclotomic cosets of $q=3$ modulo $n=10$:

$$C_0=\{0\},\quad C_1=\{1,3,9,7\},\quad C_2=\{2,6,8,4\},\quad C_5=\{5\}.$$

• Thus, $x^{90}-1=[f_0\cdot f_1\cdot f_2\cdot f_5]^9$, where $f_0, f_1, f_2, f_5 \in \mathbb{Z}_3[x]$ are monic irred. polynomials over $\mathbb{Z}_3$, and $\deg(f_0)=1$, $\deg(f_1)=4$, $\deg(f_2)=4$, $\deg(f_5)=1$.

• Hence, the number of monic factors of $x^{90}-1$ over $\mathbb{Z}_3$ is $10\times10\times10\times10=\underline{10000}$. This is also the number of cyclic subspaces of $V_{90}(\mathbb{Z}_3)$.

NOTE $f_i(x)=m_{\beta^i}(x)$, where β is an element of order 10 in $GF(3^4)$.
In fact, $\underline{x^{10}-1=(x+1)(x+2)(x^4+x^3+x^2+x+1)(x^4+2x^3+x^2+2x+1)}$.

V6e BCH Codes: Definition

- Discovered in 1960 by R.C. Bose and D. Ray-Chaudhuri, and independently in 1959 by A. Hocquenghem.

- A BCH code is a cyclic code that is constructed so that a non-trivial lower bound is known on its distance.

SETUP Suppose $\gcd(n,q)=1$.

- Let m be the smallest positive integer such that $q^m \equiv 1 \pmod{n}$.
- Let α be a generator of $GF(q^m)^*$, and let $\beta = \alpha^{(q^m-1)/n}$ (so $\mathrm{ord}(\beta)=n$).
- Let $m_{\beta^i}(x)$ denote the minimal polynomial of β^i over $GF(q)$, for $0 \le i \le n-1$. Recall that $m_{\beta^i}(x) \mid (x^n-1)$.
- We will let $m_{\beta^i}(x) = m_{\beta^{i \bmod n}}(x)$ for $i \ge n$ (since $\beta^i = \beta^{i \bmod n}$).

DEFINITION A BCH code C over $GF(q)$ of length n and designed distance δ is a cyclic code of length n over $GF(q)$ with canonical generator

$$g(x) = \operatorname{lcm}\{m_{\beta^i}(x) : a \le i \le a+\delta-2\}, \quad \text{for some integer } a.$$

NOTES 1) $\operatorname{lcm}\{3,3,5,7,7,7,11,11\} = 3 \times 5 \times 7 \times 11.$

2) Since each $m_{\beta^i}(x)$ is a monic irreducible factor of $x^n - 1$, it follows that $g(x)$ is a monic divisor of $x^n - 1$. Hence $g(x)$ is indeed the canonical generator for a cyclic code of length n over $GF(q)$.

3) Among the roots of $g(x)$ are the $\delta - 1$ consecutive powers of β:

$$\beta^a, \beta^{a+1}, \beta^{a+2}, \ldots\ldots, \beta^{a+\delta-2}.$$

4) BCH bound : $d(C) \geq \delta$. [Proof in V6f]

5) If $a=1$, the BCH code is narrow-sense.

EXAMPLE (BCH code) Let $q=3$, $n=13$. Then $m=3$ since $3^3 \equiv 1 \pmod{13}$.

- Consider $GF(3^3) = \mathbb{Z}_3[\alpha]/(\alpha^3+2\alpha^2+1)$.
- Then α is a generator of $GF(3^3)^*$ (see next slide).
- Also, $\beta = \alpha^2$ has order 13.
- Compute the cyclotomic cosets of $q=3$ mod $n=13$:

$C_0 = \{0\}$ —— $m_{\beta^0}(x) = x+2$.

$C_1 = \{1,3,9\}$ —— $m_{\beta}(x) = x^3+2x^2+2x+2$.

$C_2 = \{2,6,5\}$ —— $m_{\beta^2}(x) = x^3+2x+2$.

$C_4 = \{4,12,10\}$ —— $m_{\beta^4}(x) = x^3+x^2+x+2$.

$C_7 = \{7,8,11\}$ —— $m_{\beta^7}(x) = x^3+x^2+2$.

$\longrightarrow$

EXAMPLE (cont'd)

- $m_{\beta^2}(x) = (x-\beta^2)(x-\beta^6)(x-\beta^5)$

$$= (x-\alpha^4)(x-\alpha^{12})(x-\alpha^{10})$$
$$= [(x^2-(\alpha^4+\alpha^{12})x+\alpha^{16}][x-\alpha^{10}]$$
$$= [x^2+\alpha^{10}x+\alpha^{16}][x+\alpha^{23}]$$
$$= x^3+(\alpha^{10}+\alpha^{23})x^2+(\alpha^{16}+\alpha^{33})x+\alpha^{39}$$
$$= \underline{x^3+2x+2}.$$

Sample minimal polynomial calculation

$\alpha^0=1$	$\alpha^{13}=2$
$\alpha^1=\alpha$	$\alpha^{14}=2\alpha$
$\alpha^2=\alpha^2$	$\alpha^{15}=2\alpha^2$
$\alpha^3=2+\alpha^2$	$\alpha^{16}=1+2\alpha^2$
$\alpha^4=2+2\alpha+\alpha^2$	$\alpha^{17}=1+\alpha+2\alpha^2$
$\alpha^5=2+2\alpha$	$\alpha^{18}=1+\alpha$
$\alpha^6=2\alpha+2\alpha^2$	$\alpha^{19}=\alpha+\alpha^2$
$\alpha^7=1+\alpha^2$	$\alpha^{20}=2+2\alpha^2$
$\alpha^8=2+\alpha+\alpha^2$	$\alpha^{21}=1+2\alpha+2\alpha^2$
$\alpha^9=2+2\alpha+2\alpha^2$	$\alpha^{22}=1+\alpha+\alpha^2$
$\alpha^{10}=1+2\alpha+\alpha^2$	$\alpha^{23}=2+\alpha+2\alpha^2$
$\alpha^{11}=2+\alpha$	$\alpha^{24}=1+2\alpha$
$\alpha^{12}=2\alpha+\alpha^2$	$\alpha^{25}=\alpha+2\alpha^2$
	$\alpha^{26}=1$

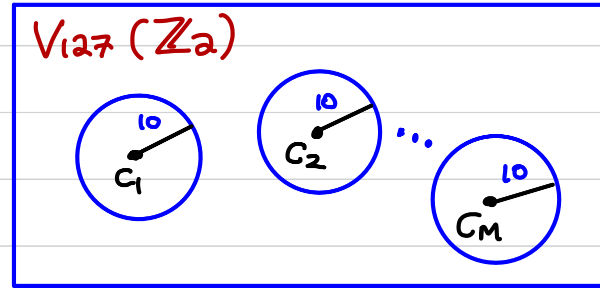
- Let $g(x) = m_{\beta^0}(x)\cdot m_{\beta^1}(x)\cdot m_{\beta^2}(x)$

$$= \underline{x^7+x^6+2x^5+x^4+2x+2}.$$

- The roots of $g(x)$ are $\beta^0, \beta^1, \beta^3, \beta^9, \beta^2, \beta^6, \beta^5$.
  Among these roots are $\beta^0, \beta^1, \beta^2, \beta^3$, so
  $\delta = 5 \Rightarrow d \geq 5$.
- Thus, <u>$g(x)$ is the canonical generator for a $(13,6)$-BCH code over $GF(3)$ of distance at least 5.</u>

V6f BCH BOUND

EXAMPLE Does there exist a block code with parameters $q=2$, $n=127$, $M=2^{64}$, $d \geq 21$? [slide 25]



The corresponding sphere packing problem is: Can we place $M=2^{64}$ spheres of radius $e=\lfloor \frac{21-1}{2} \rfloor = 10$ in $V_{127}(\mathbb{Z}_2)$ so that no two spheres overlap?

SOLUTION YES! We will describe a BCH code with parameters $q=2$, $n=127$, $k=64$, $\delta=21$.

We have $m=7$ since $2^7 \equiv 1 \pmod{127}$.

EXAMPLE (cont'd) The cyclotomic cosets of 2 mod 127 are:

$C_0 = \{0\}$

$C_1 = \{1, 2, 4, 8, 16, 32, 64\}$

$C_3 = \{3, 6, 12, 24, 48, 96, 65\}$

$C_5 = \{5, 10, 20, 40, 80, 33, 66\}$

$C_7 = \{7, 14, 28, 56, 112, 97, 67\}$

$C_9 = \{9, 18, 36, 72, 17, 34, 68\}$

$C_{11} = \{11, 22, 44, 88, 49, 98, 69\}$

$C_{13} = \{13, 26, 52, 104, 81, 35, 70\}$

$C_{15} = \{15, 30, 60, 120, 113, 99, 71\}$

$C_{19} = \{19, 38, 76, 25, 50, 100, 73\}$

$\vdots$

- Let β be an element of order 127 in $GF(2^7)^*$.
- Then $g(x) = m_\beta(x) \cdot m_{\beta^3}(x) \cdot m_{\beta^5}(x) \cdot m_{\beta^7}(x)$
  $\cdot m_{\beta^9}(x) \cdot m_{\beta^{11}}(x) \cdot m_{\beta^{13}}(x) \cdot m_{\beta^{15}}(x) \cdot m_{\beta^{19}}(x)$

  is a degree-63 monic divisor of $x^{127}-1$ over $GF(2)$.
- The roots of $g(x)$ include β^i, $1 \le i \le 20$.
- Thus, $g(x)$ is the canonical generator for a (127, 64)-binary BCH code with designed distance $\delta = 21$ (so distance ≥ 21).

VANDERMONDE MATRICES

DEFINITION A Vandermonde matrix over a field F is a matrix of the form
$$A(x_1,x_2,\dots,x_t)=\begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_t \\ x_1^2 & x_2^2 & \cdots & x_t^2 \\ \vdots & \vdots & & \vdots \\ x_1^{t-1} & x_2^{t-1} & \cdots & x_t^{t-1} \end{bmatrix}_{t\times t},$$
where $x_1,x_2,\dots,x_t\in F$.

THEOREM $\det(A(x_1,x_2,\dots,x_t))\neq 0$ iff $x_1,x_2,\dots,x_t$ are distinct.

PROOF Perform the following row operations on A:

$$\left\{\begin{array}{l} R_t\leftarrow R_t-x_1R_{t-1} \\ \quad\vdots \\ R_3\leftarrow R_3-x_1R_2 \\ R_2\leftarrow R_2-x_1R_1 \end{array}\right.$$
to get
$$A_1=\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & x_2-x_1 & x_3-x_1 & \cdots & x_t-x_1 \\ 0 & x_2^2-x_1x_2 & x_3^2-x_1x_3 & \cdots & x_t^2-x_1x_t \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & x_2^{t-1}-x_1x_2^{t-2} & x_3^{t-1}-x_1x_3^{t-2} & \cdots & x_t^{t-1}-x_1x_t^{t-2} \end{bmatrix}.$$

Now compute $\det(A_1)$ by expanding along the first column: $\longrightarrow$

PROOF (cont'd)

$$\det(A) = \det(A_1) = (x_2 - x_1)(x_3 - x_1)\cdots(x_t - x_1)\cdot \det \underbrace{\begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_2 & x_3 & \cdots & x_t \\ x_2^2 & x_3^2 & \cdots & x_t^2 \\ \vdots & \vdots & & \vdots \\ x_2^{t-2} & x_3^{t-2} & \cdots & x_t^{t-2} \end{bmatrix}}_{(t-1)\times(t-1)}.$$

By induction, $\det(A) = \prod_{1 \le i < j \le t} (x_j - x_i)$.

Thus, $\det(A) \neq 0$ iff $x_1, x_2, \ldots, x_t$ are distinct. $\square$

COROLLARY The Vandermonde matrix $A(x_1, x_2, \ldots, x_t)$ is non-singular iff $x_1, x_2, \ldots, x_t$ are distinct.

THEOREM (BCH bound)

Let C be an (n,k)-BCH code over $GF(q)$ with designed distance δ. Then $d(C) \geq \delta$.

PROOF • Let $g(x)$ be the canonical generator for C. For simplicity, we'll assume that C is narrow-sense (so $a=1$). Hence,

$$g(x) = \operatorname{lcm}\{m_{\beta^i}(x) : 1 \leq i \leq \delta-1\},$$

where $\beta \in GF(q^m)$ has order n.

• Now, let $r \in V_n(GF(q))$.

Then $\boxed{r \in C} \iff g(x) \mid r(x) \iff m_{\beta^i}(x) \mid r(x) \;\; \forall\, 1 \leq i \leq \delta-1 \iff \boxed{r(\beta^i) = 0 \;\; \forall\, 1 \leq i \leq \delta-1.}$

PROOF (cont'd) • Let $H_1 = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^2 & (\beta^2)^2 & \cdots & (\beta^2)^{n-1} \\ 1 & \beta^3 & (\beta^3)^2 & \cdots & (\beta^3)^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta^{\delta-1} & (\beta^{\delta-1})^2 & \cdots & (\beta^{\delta-1})^{n-1} \end{bmatrix}_{(\delta-1)\times n}$.

• Now, $r \in C \iff r(\beta^i) = 0 \ \forall\, 1 \le i \le \delta-1 \iff H_1 r^T = 0$.

• Furthermore, no $t = \delta-1$ columns of H_1 are linearly dependent over $GF(q^m)$ since

$$\det \begin{bmatrix} \beta^{i_1} & \beta^{i_2} & \cdots & \beta^{i_t} \\ (\beta^2)^{i_1} & (\beta^2)^{i_2} & \cdots & (\beta^2)^{i_t} \\ \vdots & \vdots & & \vdots \\ (\beta^{\delta-1})^{i_1} & (\beta^{\delta-1})^{i_2} & \cdots & (\beta^{\delta-1})^{i_t} \end{bmatrix} = \beta^{i_1}\beta^{i_2}\cdots\beta^{i_t}\cdot \det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \beta^{i_1} & \beta^{i_2} & \cdots & \beta^{i_t} \\ \vdots & \vdots & & \vdots \\ (\beta^{i_1})^{\delta-2} & (\beta^{i_2})^{\delta-2} & \cdots & (\beta^{i_t})^{\delta-2} \end{bmatrix}$$

$$= \left(\prod_{j=1}^{t} \beta^{i_j} \right) \cdot \det \big(\underbrace{A(\beta^{i_1}, \beta^{i_2}, \dots, \beta^{i_t})}_{\text{Vandermonde matrix}} \big) \neq 0, \text{ since } \beta^{i_1}, \beta^{i_2}, \dots, \beta^{i_t} \text{ are distinct.}$$

PROOF (cont'd)

- Since $GF(q) \subseteq GF(q^m)$, we also have that no $\delta-1$ columns of H_1 are linearly dependent over GF(q).
- Now, if $c \in C$, $c \neq 0$, $\omega(c) < \delta$, then $H_1 c^T = 0$ gives 0 as a non-trivial linear combination over $GF(q)$ of $\delta-1$ (or fewer) columns of contradicting what we just proved.
- Hence, every nonzero codeword in C has weight $\geq \delta$.
- Thus, $d(C) \geq \delta$. $\square$

V6g Examples of BCH Codes

EXAMPLE #1 • Let $q=2$, $n=2^r-1$ where $r\geq 2$. Then $\gcd(n,q)=1$ and $m=r$.

- Let β be a generator of $GF(2^r)^*$.
- The cyclotomic cosets of 2 mod n are $C_0=\{0\}$, $C_1=\{1,2,4,\ldots,2^{r-1}\}$, ...
- Let $g(x)=m_\beta(x)=(x-\beta)(x-\beta^2)(x-\beta^4)\cdots(x-\beta^{2^{r-1}})$.
- Then $g(x)$ is the canonical generator for a $(2^r-1,\, 2^r-1-r)$-binary BCH code C with designed distance $\delta=3$. So, $d(C)\geq 3$.

- A PCM for C must look like $H=\underbrace{\begin{bmatrix} | & | & | & | & \cdots & | \\ | & | & | & | & & | \\ | & | & | & | & & | \end{bmatrix}_{r\times(2^r-1)}}_{\text{all nonzero vectors in } V_r(\mathbb{Z}_2)}$.

So, C is a cyclic binary Hamming code (and $d(C)=3$).

- Hence, all binary Hamming codes are cyclic, up to equivalence.

EXAMPLE #2 • Let $q=2$ and $n=23$. Then $m=11$ $[2^{11}\equiv 1 \pmod{23}]$.

• The cyclotomic cosets of 2 mod 23 are:

$C_0=\{0\}$, $C_1=\{1,2,4,8,16,9,18,13,3,6,12\}$, $C_5=\{5,10,20,17,11,22,21,19,15,7,14\}$.

In fact $x^{23}-1=(x+1)(x^{11}+x^9+x^7+x^6+x^5+x+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)$.

• Let β be an element of order 23 in $GF(2^{11})^*$. Let $g(x)=m_\beta(x)$.
Then $g(x)$ is the canonical generator for a (23,12)-binary BCH code C of designed distance $\delta=5$. Hence $d(C)\geq 5$.
Furthermore, $g(x)\in C$, so $d(C)\leq 7$.

• **FACT** C is equivalent to the binary Golay code C_{23}.
So, C_{23} is equivalent to a cyclic code.

EXAMPLE #3 • Let $q=2$, $n=2^{16}-1=65535$. Then $\gcd(n,q)=1$ and $m=16$.

• Let $GF(2^{16})=\mathbb{Z}_2[\alpha]/(\alpha^{16}+\alpha^5+\alpha^3+\alpha^2+1)$.

• **FACT:** α is a generator of $GF(2^{16})^*$. Let $\beta=\alpha$.

• The cyclotomic cosets of 2 mod 65535 are: $C_0=\{0\}$,
$C_1=\{1,2,4,8,16,\ldots\}$, $C_3=\{3,6,12,24,\ldots\}$, $C_5=\{5,10,20,\ldots\}$, $C_7=\{7,14,\ldots\}$,
$C_9=\{9,18,\ldots\}$, $C_{11}=\{11,22,\ldots\}$, $C_{13}=\{13,\ldots\}$, $C_{15}=\{15,\ldots\}$,
$C_{17}=\{17,\ldots\}$, $C_{19}=\{19,\ldots\}$, $C_{21}=\{21,\ldots\}$, $C_{23}=\{23,\ldots\}$, $\ldots\ldots$

• **FACT** $C_1, C_3, C_5, \ldots, C_{23}$ are distinct and have size 16.

• Let $g(x)=\displaystyle\prod_{i\in\{1,3,5,\ldots,23\}} m_{\beta^i}(x)$. Then $\deg(g)=12\times 16=192$.

• $g(x)$ is the canonical generator for a (65535, 65343)-binary BCH code C with $\delta=25$, so $d(C)\geq 25$.

→

EXAMPLE #3 (cont'd)

THEOREM (shortening a code) Let C be a systematic (n,k,d)-code over $GF(q)$, and let $t<k$. Let C' be the code obtained by "shortening" C in its first t coordinate positions, i.e. taking all codewords in C that have 0 in the first t coordinate positions, and then deleting those coordinates. Then C' is an $(n-t, k-t, d')$-code over $GF(q)$ with $d' \geq d$.

PROOF Let $G = \left[\begin{array}{cccccc|c} 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & A \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 1 & \end{array}\right]_{k\times n}$ be a standard-form GM for C.

Let G' be the matrix obtained by deleting the first t rows of G, and then deleting the first t columns. Then G' is a $(k-t)\times(n-t)$ GM for C' with $d' \geq d$. $\square$

EXAMPLE #3 (cont'd)

- C : $(65535, 65343)$-binary BCH code with $d \geq 25$.
- C is systematic, since C has a GM $G = \begin{bmatrix} g(x) & & & & \\ & g(x) & & & \\ & & g(x) & & \\ & & & \ddots & \\ & & & & g(x) \end{bmatrix}$.

- Consider the shortened code C' obtained by shortening C by $t = 33135$.
- Then C' is a $(32400, 32208)$-binary code with distance $d' \geq 25$.

- C' is used (together with an LDPC code) in the DVB-S2 standard for digital video broadcasting — satellite.

EXAMPLE #4 (QR codes)

1) • Let $q=2$ and $n=15$, so $\gcd(n,q)=1$ and $m=4$.
   • Let $GF(2^4)=\mathbb{Z}_2[\alpha]/(\alpha^4+\alpha+1)$ and $\beta=\alpha$. Then $\mathrm{ord}(\beta)=15$.
   • Let $g(x)=m_\beta(x)\cdot m_{\beta^3}(x)\cdot m_{\beta^5}(x)=x^{10}+x^8+x^5+x^4+x^2+x+1$. [See slide 151]
   • Then $g(x)$ is the canonical generator for a (15,5)-binary BCH code C with $\delta=7$ (since $\beta,\beta^2,\beta^3,\beta^4,\beta^5,\beta^6$ are roots of $g(x)$). In fact, $d(C)=7$.
   • C is used in QR codes to encode the "format data". [There are 32 formats]

2) • $g(x)=x^{11}+x^9+x^7+x^6+x^5+x+1$ is the canonical generator for a (23,12,7)-BCH code B_{23} that is equivalent to C_{23}.
   • Let E_{23} be the set of even-weight codewords in B_{23}. Then E_{23} is a (23,11,8)-binary cyclic code with canonical generator $g(x)\cdot(x+1)$.
   • Let S_{23} be the (18,6,8)-binary code obtained by shortening E_{23} by $t=5$.
   • S_{23} is used to encode the "version data". [There are 34 versions]

$\longrightarrow$

EXAMPLE #4 (cont'd)

3) A (255, 231, 25)-RS code over $GF(2^8)$ is used for the payload, more precisely a shortened (36, 12, 25)-code over $GF(2^8)$ ($t = 219$), and a shortened (37, 13, 25)-code over $GF(2^8)$ ($t = 218$). [see slide 175]

DECODING BCH CODES

Several efficient algorithms have been designed for decoding BCH codes. We don't have the time to study them. Instead, we'll study a decoding algorithm for a family of BCH codes called Reed-Solomon (RS) codes.