# Background on Binary BCH Codes

"Technical Lemma": Suppose $a(x), f(x) \in F[x]$, where $F$ is a field; also let $\alpha$ be a root (in an extension of $F$): $a(\alpha) = f(\alpha) = 0$.
If $a(x)$ is irreducible (over $F$) then $a(x) | f(x)$.

Pf: Set $b(x) = \gcd(a(x), f(x))$. Then $b(x)$ can be expressed as $u(x)a(x) + v(x)f(x)$. Therefore $b(\alpha) = 0$. Since $b(x) | a(x)$ and $b(x) \neq 1$, claim follows.

Example: $x^4 + x + 1$ is irreducible in $F_2[x]$.
Construct $F_{16}$ using $x^4+x+1$. If $\alpha \in F_{16}$ has $\alpha^4 + \alpha + 1$, then $\alpha^{15} + 1 = 0$ (Prop 3.6 in text)
Thus $(x^4+x+1) \mid (x^{15}+1)$.
In fact $x^{15}+1 = (x^4+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^2+x+1)(x+1)$

Text Thm 7.10 $x^{2^n-1} - 1$ is, in general, the product of all (binary) irreducibles of degree $m|n$.

Observe: $\alpha$ is primitive in $F_{16}$, so each $\alpha^i$ is a root of one of these factors

| | |
|---|---|
| $x^4+x+1=0$ | roots $\alpha^1, \alpha^2, \alpha^4, \alpha^8$ |
| $x^4+x^3+x^2+x+1=0$ | roots $\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$ |
| $x^4+x^3+1=0$ | roots $\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$ |
| $x^2+x+1=0$ | roots $\alpha^5, \alpha^{10}$ |
| $x+1=0$ | root $\alpha^0$ |

For binary polynomials $a(x^2) = (a(x))^2$; $a(\beta)=0 \Rightarrow a(\beta^2)=0$.
Given $n = 2^m - 1$, cyclotomic cosets $C_j = \{j\, 2^i \pmod n \mid i \geq 0\}$

(Binary) <u>cyclic Codes</u> Use the 1-1 correspondence:

$$(c_{n-1}, c_{n-2}, \ldots, c_1, c_0) \Leftrightarrow \sum_{i=0}^{n-1} c_i x^i = c(x) \in F_2[x]$$

<u>Suppose</u>: $n$ odd, $g(x) \mid (x^n - 1)$, $g(x) \in F_2[x]$

Form $C_g = \{c(x) \in F_2[x] \mid \deg(c(x)) < n,\ g(x) \mid c(x)\}$.

Corresponds to a linear code closed under cyclic shifts: $c(x) \in C \Rightarrow x\,c(x) \pmod{x^n - 1} \in C$

Basis: $\{g(x), xg(x), \ldots, x^{n-\deg(g(x))-1} g(x)\}$

$(n, n - \deg(g(x))$ linear code over $F_2$

BCH bound (see Prop 8.7): $F$ finite field and $n > 1$ with $\gcd(|F|, n) = 1$. Suppose $g(x) \in F[x]$, $g(x) \mid (x^n - 1)$. Form $C_g$ as above. If $g(\alpha^i) = 0$ for $1 \le i \le d-1$, then $C_g$ has minimum distance at least $d$.

<u>Example</u> $F = \{0,1\}$ $n = 15$

$g(x) = (1 + x + x^4) \longrightarrow (15, 11, 3)$ code (cyclic Hamming)

$g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \rightarrow (15, 7, d)$ code with $d \ge 5$

$g(x) = (x^4 + x + 1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1) \rightarrow (15, 5, d)$ code, $d \ge 7$.

1965 Dissertation by Elwyn Berlekamp (MIT E.E.)

Efficient, low-memory decoding for BCH codes $\rightarrow$ founder Cyclotomics

# Algebraic Decoding

Example: $(15,7,5)$ Binary BCH Code

$n=15$, $\alpha^4+\alpha+1=0$, $g(x)=(x^4+x+1)(x^4+x^3+x^2+x+1)=x^8+x^7+x^6+x^4+1$

Test: $a(x)\in C_g \Leftrightarrow \begin{Bmatrix}(x^4+x+1)\mid a(x)\\ (x^4+x^3+x^2+x+1)\mid a(x)\end{Bmatrix} \Leftrightarrow \begin{Bmatrix}a(\alpha)=0\\ a(\alpha^3)=0\end{Bmatrix}$ [Lemma]

Receive $\vec{r}=\vec{c}+\vec{e}$ with $1\le wt(\vec{e})\le 2$ Find $\vec{e}$

Form $s_1=r(\alpha)$, $s_3=r(\alpha^3)$ (c.f. text Ex 3.10 binary matrix)

$c(x)\in C_g$ so that $s_1=e(\alpha)$, $s_3=e(\alpha^3)$ (c.f. syndrome seq.)

Necessary Condition for $wt(\vec{e})=1$: $(s_1)^3=s_3$

Now suppose $e(x)=x^i+x^j$, and compute $(s_1)^3$

$(\alpha^i+\alpha^j)^2(\alpha^i+\alpha^j)=(\alpha^{2i}+\alpha^{2j})(\alpha^i+\alpha^j)=\alpha^{3i}+\alpha^{3j}+\alpha^{2i+j}+\alpha^{2j+i}$

$=s_3+(\alpha^i+\alpha^j)\alpha^{i+j}=s_3+s_1\alpha^{i+j}$. Hence $\alpha^{i+j}=\dfrac{s_3+(s_1)^3}{s_1}$.

Locator Poly $(z+\alpha^i)(z+\alpha^j)=z^2+s_1z+\dfrac{s_3+(s_1)^3}{s_1}$

Substitute $z=s_1y \rightarrow s_1^2y^2+s_1^2y+\dfrac{s_3+(s_1)^3}{s_1}$

Has the same roots as $y^2+y+\left(\dfrac{s_3}{s_1^3}+1\right)$.

Summary: Decode from $\begin{Bmatrix}s_1\\ s_3\end{Bmatrix}$

$s_1=s_3=0 \Rightarrow$ assume no error

$s_3=(s_1)^3\neq 0 \rightarrow$ assume one error @ $i \Leftrightarrow s_1=\alpha^i$

$s_3\neq(s_1)^3\neq 0 \Rightarrow$ two errors from table

DECODE FAILURE CONDITIONS

Observe $s_1=0$, $s_3\neq 0 \Rightarrow \vec{e}\neq\vec{0}$ and $\vec{e}$ in Hamming code $(15,11,3)$ $wt(\vec{e})\ge 3$

$s_3/(s_1)^3$ not in table

Ex: Decode $(000000000011100)$ $r(x)=x^4+x^3+x^2$

$s_1=\alpha^2+\alpha^3+\alpha^4=\alpha^{12}$ $s_3=\alpha^6+\alpha^9+\alpha^{12}=\alpha^{14}$

$s_3/(s_1)^3=\alpha^{14}/\alpha^6=\alpha^8 \Leftrightarrow$ Two errors $\{i+3, i+14\}$

$=\{12+3, 12+14\}=\{0,11\}$

$c=(000000000011100)+(000100000000001)$

$\Leftrightarrow$ cyclic shift of $g(x)$

Decoding table Derivation for (15, 7, 5) BCH Code:

Set $S_1 = \alpha^i$. When $wt(e) = 1$, we saw that $S_3 = (S_1)^3 \neq 0$, which means $S_3/(S_1)^3 = 1$, with the error location being the exponent $i$.

For $S_3 \neq (S_1)^3 \neq 0$, again set $S_1 = \alpha^i$

The exponents of the roots of the Error-Locator $z^2 + S_1 z + \frac{S_3 + S_1^3}{S_1} = 0$ give the two error locations. This is done in two steps: find roots of $y^2 + y + (\frac{S_3}{S_1^3} + 1) = 0$, using a table; then use $z = \alpha^i y$ to convert to the roots in $z$-polynomial

Since coef of $y$ is 1, the roots $\alpha^j, \alpha^k$ must sum to 1, and $\alpha^j \cdot \alpha^k = 1 + S_3/(S_1)^3$.

For example, if $\alpha^3$ is a root, the other is $1 + \alpha^3 = \alpha^{14}$. Their product is $\alpha^2$, making $S_3/(S_1)^3 = 1 + \alpha^2 = \alpha^8$. So $\alpha^8$ is paired with $3+i$ and $14+i$.

<u>Remarks</u>: ① When $S_3/S_1^3$ is a value <u>not</u> in the table, $wt(e) > 2$, a Decode Failure.

② This method requires $n = 2^m - 1$, so that all computations (assuming errors) result in a power of $\alpha$, the primitive $n^{th}$ root.