Extensions of Finite Fields

Let Z is a field

Consider $Z^n = \{(z_1, \dots z_n) : z_i \in Z\}$

Z^n is a linear space over Z

Take a polynomial over Z

$$P(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_n x^n$$

where $c_i \in Z$; $\deg P(x) = n$

$P(x)$ is irreducible if $P(x)$ cannot be represented as $S(x) R(x)$

($\deg S(x) > 1$, $\deg R(x) > 1$)

$P(x)$ is primitive if $x^i \neq x^j$ for all $i, j = 0, 1, \dots, |Z|^n - 2$

④ If $P(x)$ is primitive $\Rightarrow$ it is irreducible (opposite is not correct)

(T2) For any Z and any n there exists at least one primitive polynomial $P(x)$

(T3) If $P(x)$ is primitive then Z^n is a field (called n-th <u>extension of</u> Z) if all vectors in Z^n are interpreted as polynomials and all operations in Z^n are modulo $P(x)$ i.e. $P(x)=0$; x is <u>primitive element</u> of Z^n (Z itself may be an extension of another field; e.g. $Z=Z_2^3 \Rightarrow Z^4=(Z_2^3)^4$)

(T4) For any finite field or its extension the number of elements is q^n (where q is a <u>prime</u>)

(T5) Any two fields with the same number of elements are isomorphic

CYCLIC HAMMING CODES.

Let $n = 2^r - 1$

CONSIDER $GF(2^r)$

LET α be primitive in $GF(2^r)$

$\alpha^i \neq \alpha^j \; ; \; i \neq j \; ; i, j = 0, 1, \ldots, 2^r - 2$

TAKE

$$H = \left[1 \; \alpha \; \alpha^2 \ldots \alpha^{2^r - 2}\right]$$

since $\alpha^i \neq \alpha^j$ H is a check matrix for a $(2^r - 1, 2^r - r - 1, 3)$ HAMMING code

$v \in V$ if

$v_0 + \alpha v_1 + \alpha^2 v_2 + \dots + \alpha^6 v^6 = 0$

Let

$$v(x) = v_0 + v_1 x + v_2 x^2 + \dots + v_6 x^6$$

polynomial representation of v

Then $v \in V$ iff

$v(\alpha) = 0$ α is a root of $v(x)$

For $v = (v_0, v_1, \dots, v_6)$

denote $y = Sh\, v = (v_6, v_0, v_1, \dots, v_5)$

Then in the polynomial form

$$y(x) = v_6 + v_0 x + v_1 x^2 + \dots + v_5 \cdot x^6$$

$$= v(x) \cdot x \quad \text{since } x^7 = x^0 = 1$$

there are no simple procedures to decide whether $P(x)$ is primitive over $\mathbb{Z}$

(irreducibility is a necessary condition for primitivity)

For $\mathbb{Z}_2^n$ there are good tables of primitive polynomials

EXAMPLE $\mathbb{Z} = \mathbb{Z}_2 = \{0,1\}$ $n=3$

BINARY	polynomial	exponential
000	0	–
001	x^2	x^2
010	x	x^1
011	x^2+x	x^4
100	1	x^0
101	x^2+1	x^6
110	$1+x$	x^3
111	$1+x+x^2$	x^5
$1\ x\ x^2$		

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

$x^3 = x+1$

$x^4 = x^2+x$

$x^5 = x^3+x^2$

$= x^2+x+1$

$x^6 = x^3+x^2+x$

$= x+1+x^2+x$

$= x^2+1$

$x^7 = x^3+x = 1$

$x^{2^n-1} = x^7 = 1$ $\quad |\mathbb{Z}_2^n| = 8$

$(101)(110) = x^6 \cdot x^3 = x^9 = x^2 = 001$

$111/110 = x^2 = 001$, $110/101 = x^3 = x^4 = 011$

Thus

if $y = sh\, v$ then

$$y(x) = x\, v(x)$$

If $v(\alpha) = 0 \iff v \in V$

$y(x) = x\, v(x) \iff y(\alpha) = 0$

$\iff sh\, v \in V$

Our code is <u>closed</u> for <u>circular shifts</u> $\Rightarrow$

cyclic code.

BINARY HAMMING CODES

(CONT'D)

$n = 2^r - 1$

Consider Z_2^r generated by $P(x)$

where $\deg P(x) = r$.

Let α is root of $P(x)$

$$P(\alpha) = 0$$

Take

$$H = \left[1\ \alpha\ \alpha^2\ \alpha^3 \ldots \alpha^{n-1}\right]\}r.$$

$v \in C$ - HAMMING CODE

IIf ~~$v \in$~~ $Hv = 0$

$$v(\alpha) = 0.$$

If. $v \in \mathbb{C} \Leftrightarrow$

$v(\alpha) = 0$

Consider

$$B(x) = v(x)\, w(x)$$

for any $w(x)$

Then $Q(\alpha) = v(\alpha) \cdot w(\alpha) = 0 \Rightarrow$

$Q \in \mathbb{C}$

If v is a codeword all multiples of v are codewords

Since $P(\alpha) = 0$, code $\mathbb{C}$ consists of all multiples of $P(x)$

For example for $n=3$

One can take $P(x)=x^3+x+1$

primitive

Then $P(x) \in \mathbb{C}$

$\Downarrow$

$(0\,0\,0\,1\,0\,1\,1) \in \mathbb{C}$

and code consists of all multiples of $P(x)=x^3+x+1$

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

$=x^5+x^3+x^2+x^3+x+1=$

$=x^5+x^2+x+1 \Rightarrow$

$0\,1\,0\,0\,1\,1\,1 \in \mathbb{C}$

<u>Remark:</u> $x^n=x^0$

Shortened Hamming codes with $n<2^r-1$ are <u>not</u> cyclic

Generating Matrices for Binary Hamming codes

Let $p(x)$ is used to construct

Z_2^r $\deg p(x) = r$

$p(x)$ primitive $p(\alpha)=0$

$p \in C$.

Then $x\,p(x) \in C$ since

$x\,p(x) = \text{Rot}\, p(x)$

$x^2 p(x) \in C$

$x^3 p(x) \in C$

and

the generating matrix G can be taken as

$$G = \begin{bmatrix} p(x) \\ x\,p(x) \\ x^2 p(x) \\ \vdots \\ x^{k-1} p(x) \end{bmatrix}$$

where $k = n - r = 2^r - 1 - r$

Example $n = 2^3 - 1 = 7 \quad r = 3$

$k = 4$

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

$$p = (0001011) \in C$$

$x\,p(x) = x^4 + x^2 + x$ or

in binary

0 0 1 0 1 1 0

For $x^2\,p(x) = x^5 + x^3 + x^2$ or

0 1 0 1 1 0 0

$x^3\,p(x) = x^6 + x^4 + x^3$

1 0 1 1 0 0 0

and $n = 7$

$$G = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \quad k = 4$$

(not in the standard form)

EXAMPLE $r=3$, x^3+x+1

$\alpha^3+\alpha+1=0$

$$H=\begin{bmatrix} 0&0&1&0&1&1&1 \\ 0&1&0&1&1&1&0 \\ 1&0&0&1&0&1&1 \end{bmatrix} \begin{matrix} \alpha^2 \\ \alpha \\ 1 \end{matrix}$$

α^5

$$H=[1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6]$$

(7,4,3) HAMMING code V

Let $v=(v_0,v_1,\dots,v_6)\in V$

then $Hv=0$

$$[1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6]\begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \end{bmatrix}=0$$