CHAPTER 3: Cyclic and convolution codes

Cyclic codes are special linear cods of interest and importance because

- They posses a rich algebraic structure that can be utilized in a variety of ways.
- They have extremely concise specifications.
- They can be efficiently implemented using simple ***shift registers***.
- Many practically important codes are cyclic.

Convolution codes allow to encode streams od data (bits).

IMPORTANT NOTE

In order to specify a binary code with 2^k codewords of length n one may need to write down

$$2^k$$

codewords of length n.

In order to specify a linear binary code with 2^k codewords of length n it is sufficient to write down

$$k$$

codewords of length n.

In order to specify a binary cyclic code with 2^k codewords of length n it is sufficient to write down

$$1$$

codeword of length n.

BASIC DEFINITION AND EXAMPLES

Definition A code C is cyclic if

(i) C is a linear code;

(ii) any cyclic shift of a codeword is also a codeword, i.e. whenever $a_0, \dots a_{n-1} \in C$, then also $a_{n-1} a_0 \dots a_{n-2} \in C$.

Example

(i) Code $C = \{000, 101, 011, 110\}$ is cyclic.

(ii) Hamming code $Ham(3, 2)$: with the generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

is equivalent to a cyclic code.

(iii) The binary linear code {0000, 1001, 0110, 1111} is not a cyclic, but it is equivalent to a cyclic code.

(iv) Is Hamming code $Ham(2, 3)$ with the generator matrix

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

(a) cyclic?

(b) equivalent to a cyclic code?

FREQUENCY of CYCLIC CODES

Comparing with linear codes, the cyclic codes are quite scarce. For, example there are 11 811 linear (7,3) linear binary codes, but only two of them are cyclic.

Trivial cyclic codes. For any field F and any integer $n >= 3$ there are always the following cyclic codes of length n over F:

- No-information code - code consisting of just one all-zero codeword.
- Repetition code - code consisting of codewords $(a, a, \ldots, a)$ for $a \in F$.
- Single-parity-check code - code consisting of all codewords with parity 0.
- No-parity code - code consisting of all codewords of length n

For some cases, for example for $n = 19$ and $F = GF(2)$, the above four trivial cyclic codes are the only cyclic codes.

EXAMPLE of a CYCLIC CODE

The code with the generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

has codewords

$$c_1 = 1011100 \qquad c_2 = 0101110 \qquad c_3 = 0010111$$

$$c_1 + c_2 = 1110010 \qquad c_1 + c_3 = 1001011 \qquad c_2 + c_3 = 0111001$$

$$c_1 + c_2 + c_3 = 1100101$$

and it is cyclic because the right shifts have the following impacts

$$c_1 \to c_2, \qquad c_2 \to c_3, \qquad c_3 \to c_1 + c_3$$

$$c_1 + c_2 \to c_2 + c_3, \qquad c_1 + c_3 \to c_1 + c_2 + c_3, \qquad c_2 + c_3 \to c_1$$

$$c_1 + c_2 + c_3 \to c_1 + c_2$$

POLYNOMIALS over GF(q)

A codeword **of a cyclic code is usually denoted**

$$a_0\, a_1 \ldots a_{n-1}$$

and to each such a codeword the polynomial

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}$$

will be associated.

NOTATION: $F_q[x]$ denotes the set of all polynomials over $GF(q)$.

deg (f(x)) = the largest m such that x^m has a non-zero coefficient in $f(x)$.

Multiplication of polynomials If f(x), g(x) $\in F_q[x]$, then

$$deg\,(f(x)\, g(x)) = deg\,(f(x)) + deg\,(g(x)).$$

Division of polynomials For every pair of polynomials a(x), b(x) $\neq 0$ in $F_q[x]$ there exists a unique pair of polynomials q(x), r(x) in $F_q[x]$ such that

$$a(x) = q(x)b(x) + r(x),\ deg\,(r(x)) < deg\,(b(x)).$$

Example Divide $x^3 + x + 1$ by $x^2 + x + 1$ in $F_2[x]$.

Definition Let f(x) be a fixed polynomial in $F_q[x]$. Two polynomials g(x), h(x) are said to be **congruent** modulo f(x), notation

$$g(x) \equiv h(x) \pmod{f(x)},$$

if g(x) - h(x) is divisible by f(x).

RING of POLYNOMIALS

The set of polynomials in $F_q[x]$ of degree less than *deg* (f(x)), with addition and multiplication modulo f(x) forms a ring denoted **$F_q[x]/f(x)$**.

Example Calculate $(x + 1)^2$ in $F_2[x] / (x^2 + x + 1)$. It holds

$$(x + 1)^2 = x^2 + 2x + 1 \equiv x^2 + 1 \equiv x \pmod{x^2 + x + 1}.$$

How many elements has $F_q[x] / f(x)$?

Result $| F_q[x] / f(x) | = q^{\deg (f(x))}$.

Example Addition and multiplication in $F_2[x] / (x^2 + x + 1)$

+	0	1	x	1 + x
0	0	1	x	1 + x
1	1	0	1 + x	x
x	x	1 + x	0	1
1 + x	1 + x	x	1	0

•	0	1	x	1 + x
0	0	0	0	0
1	0	1	X	1 + x
x	0	x	1 + x	1
1 + x	0	1 + x	1	x

Definition A polynomial f(x) in $F_q[x]$ is said to be reducible if f(x) = a(x)b(x), where a(x), b(x) $\in F_q[x]$ and

$$deg\ (a(x)) < deg\ (f(x)), \qquad deg\ (b(x)) < deg\ (f(x)).$$

If f(x) is not reducible, it is irreducible in $F_q[x]$.

Theorem The ring $F_q[x] / f(x)$ is a <u>field</u> if f(x) is irreducible in $F_q[x]$.

FIELD R_n, $R_n = F_q[x] / (x^n - 1)$

Computation modulo $x^n - 1$

Since $x^n \equiv 1 \pmod{(x^n - 1)}$ we can compute f(x) mod (x^n -1) as follows:

In f(x) replace x^n by 1, x^{n+1} by x, x^{n+2} by x^2, x^{n+3} by x^3, …

Identification of words with polynomials

$$a_0 a_1 \ldots a_{n-1} \leftrightarrow a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}$$

Multiplication by x in R_n corresponds to a single cyclic shift

$$x (a_0 + a_1 x + \ldots a_{n-1} x^{n-1}) = a_{n-1} + a_0 x + a_1 x^2 + \ldots + a_{n-2} x^{n-1}$$

Algebraic characterization of cyclic codes

Theorem A code C is cyclic if C satisfies two conditions

(i) $a(x), b(x) \in C \Rightarrow a(x) + b(x) \in C$

(ii) $a(x) \in C$, $r(x) \in R_n \Rightarrow r(x)a(x) \in C$

Proof

(1) Let C be a cyclic code. C is linear $\Rightarrow$ (i) holds.

(ii) Let $a(x) \in C$, $r(x) = r_0 + r_1 x + \ldots + r_{n-1}x^{n-1}$

$$r(x)a(x) = r_0 a(x) + r_1 x a(x) + \ldots + r_{n-1}x^{n-1}a(x)$$

is in C by (i) because summands are cyclic shifts of $a(x)$.

(2) Let (i) and (ii) hold

- Taking $r(x)$ to be a scalar the conditions imply linearity of C.
- Taking $r(x) = x$ the conditions imply cyclicity of C.

CONSTRUCTION of CYCLIC CODES

Notation If $f(x) \in R_n$, then

$$\langle f(x) \rangle = \{r(x)f(x) \mid r(x) \in R_n\}$$

(multiplication is modulo $x^n - 1$).

Theorem For any $f(x) \in R_n$, the set $\langle \mathbf{f(x)} \rangle$ is a cyclic code (generated by f).

Proof We check conditions (i) and (ii) of the previous theorem.

(i) If $a(x)f(x) \in \langle f(x) \rangle$ and also $b(x)f(x) \in \langle f(x) \rangle$, then

$$a(x)f(x) + b(x)f(x) = (a(x) + b(x))\, f(x) \in \langle f(x) \rangle$$

(ii) If $a(x)f(x) \in \langle f(x) \rangle$, $r(x) \in R_n$, then

$$r(x)\,(a(x)f(x)) = (r(x)a(x))\, f(x) \in \langle f(x) \rangle.$$

Example $C = \langle 1 + x^2 \rangle$, $n = 3$, $q = 2$.
We have to compute $r(x)(1 + x^2)$ for all $r(x) \in R_3$.

$$R_3 = \{0, 1, x, 1 + x, x^2, 1 + x^2, x + x^2, 1 + x + x^2\}.$$

Result

$$C = \{0, 1 + x, 1 + x^2, x + x^2\}$$

$$C = \{000, 011, 101, 110\}$$

Characterization theorem for cyclic codes

We show that all cyclic codes C have the form $C = \langle f(x) \rangle$ for some $f(x) \in R_n$.

Theorem Let C be a non-zero cyclic code in R_n. Then

- there exists unique monic polynomial $g(x)$ of the smallest degree such that
- $C = \langle g(x) \rangle$
- $g(x)$ is a factor of $x^n - 1$.

Proof

(i) Suppose $g(x)$ and $h(x)$ are two monic polynomials in C of the smallest degree. Then the polynomial $g(x) - h(x) \in C$ and it has a smaller degree and a multiplication by a scalar makes out of it a monic polynomial. If $g(x) \neq h(x)$ we get a contradiction.

(ii) Suppose $a(x) \in C$.

Then

$$a(x) = q(x)g(x) + r(x) \qquad (deg\ r(x) < deg\ g(x))$$

and

$$r(x) = a(x) - q(x)g(x) \in C.$$

By minimality

$$r(x) = 0$$

and therefore $a(x) \in \langle g(x) \rangle$.

Characterization theorem for cyclic codes

(iii) Clearly,

$$x^n - 1 = q(x)g(x) + r(x) \quad \text{with} \quad \mathit{deg}\ r(x) < \mathit{deg}\ g(x)$$

and therefore $r(x) \equiv -q(x)g(x) \pmod{x^n - 1}$ and

$$r(x) \in C \Rightarrow r(x) = 0 \Rightarrow g(x) \text{ is a factor of } x^n - 1.$$

GENERATOR POLYNOMIALS

Definition If for a cyclic code C it holds

$$C = \langle \mathbf{g}(\boldsymbol{x}) \rangle,$$

then g is called the **generator polynomial** for the code C.

IV054 **HOW TO DESIGN CYCLIC CODES?**

The last claim of the previous theorem gives a recipe how to get all cyclic codes of the given length n.

Indeed, all we need to do is to find all factors of

$$x^n - 1.$$

Problem: Find all binary cyclic codes of length 3.

Solution: Since

$$x^3 - 1 = \underbrace{(x+1)(x^2+x+1)}_{\text{both factors are irreducible in } GF(2)}$$

we have the following generator polynomials and codes.

Generator polynomials	Code in R_3	Code in $V(3,2)$
1	R_3	$V(3,2)$
$x + 1$	$\{0, 1 + x, x + x^2, 1 + x^2\}$	{000, 110, 011, 101}
$x^2 + x + 1$	$\{0, 1 + x + x^2\}$	{000, 111}
$x^3 - 1\ (= 0)$	$\{0\}$	{000}

Design of generator matrices for cyclic codes

Theorem Suppose C is a cyclic code of codewords of length n with the generator polynomial

$$g(x) = g_0 + g_1x + \dots + g_rx^r.$$

Then $dim\,(C) = n - r$ and a generator matrix G_1 for C is

$$G_1 = \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_r & 0 & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & g_2 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \dots & g_r & 0 & \dots & 0 \\ .. & .. & & & & & & & & .. \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & g_0 & \dots & g_r \end{pmatrix}$$

Proof

(i) All rows of G_1 are linearly independent.

(ii) The $n - r$ rows of G represent codewords

$$g(x),\ xg(x),\ x^2g(x), \dots,\ x^{n-r-1}g(x)$$

(*)

(iii) It remains to show that every codeword in C can be expressed as a linear combination of vectors from (*).

Inded, if $a(x) \in C$, then

$$a(x) = q(x)g(x).$$

Since $deg\ a(x) < n$ we have $deg\ q(x) < n - r$.

Hence

$$\begin{aligned} q(x)g(x) &= (q_0 + q_1x + \dots + q_{n-r-1}x^{n-r-1})g(x) \\ &= q_0g(x) + q_1xg(x) + \dots + q_{n-r-1}x^{n-r-1}g(x). \end{aligned}$$

EXAMPLE

The task is to determine all ternary codes of length 4 and generators for them.

Factorization of $x^4 - 1$ over $GF(3)$ has the form

$$x^4 - 1 = (x - 1)(x^3 + x^2 + x + 1) = (x - 1)(x + 1)(x^2 + 1)$$

Therefore there are $2^3 = 8$ divisors of $x^4 - 1$ and each generates a cyclic code.

Generator polynomial	Generator matrix
1	I_4
$x-1$	$\begin{bmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}$
$x + 1$	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$
$x^2 + 1$	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$
$(x - 1)(x + 1) = x^2 - 1$	$\begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$
$(x - 1)(x^2 + 1) = x^3 - x^2 + x - 1$	[-1 1 -1 1]
$(x + 1)(x^2 + 1)$	[1 1 1 1]
$x^4 - 1 = 0$	[0 0 0 0]

Check polynomials and parity check matrices for cyclic codes

Let C be a cyclic $[n,k]$-code with the generator polynomial $g(x)$ (of degree $n - k$). By the last theorem $g(x)$ is a factor of $x^n - 1$. Hence

$$x^n - 1 = g(x)h(x)$$

for some $h(x)$ of degree k (where $h(x)$ is called the check polynomial of C).

Theorem Let C be a cyclic code in R_n with a generator polynomial $g(x)$ and a check polynomial $h(x)$. Then an $c(x) \in R_n$ is a codeword of C if $c(x)h(x) \equiv 0$ – (this and next congruences are all modulo $x^n – 1$).

Proof Note, that $g(x)h(x) = x^n - 1 \equiv 0$

(i) $c(x) \in C \Rightarrow c(x) = a(x)g(x)$ for some $a(x) \in R_n$

$$\Rightarrow c(x)h(x) = a(x)\underbrace{g(x)h(x)}_{\equiv 0} \equiv 0.$$

(ii) $c(x)h(x) \equiv 0$

$$c(x) = q(x)g(x) + r(x),\ deg\ r(x) < n – k = deg\ g(x)$$

$$c(x)h(x) \equiv 0 \Rightarrow r(x)h(x) \equiv 0 \pmod{x^n - 1}$$

Since $deg\ (r(x)h(x)) < n – k + k = n$, we have $r(x)h(x) = 0$ in $F[x]$ and therefore

$$r(x) = 0 \Rightarrow c(x) = q(x)g(x) \in C.$$

POLYNOMIAL REPRESENTATION of DUAL CODES

Since *dim* (⟨h(x)⟩) = $n - k$ = *dim* ($C^{\perp}$) we might easily be fooled to think that the check polynomial h(x) of the code C generates the dual code $C^{\perp}$.

Reality is “slightly different":

Theorem Suppose C is a cyclic [n,k]-code with the check polynomial

$$h(x) = h_0 + h_1 x + \ldots + h_k x^k,$$

then

(i) a parity-check matrix for C is

$$H = \begin{pmatrix} h_k & h_{k-1} & \ldots & h_0 & 0 & \ldots & 0 \\ 0 & h_k & \ldots & h_1 & h_0 & \ldots & 0 \\ .. & .. & & & & & \\ 0 & 0 & \ldots & 0 & h_k & \ldots & h_0 \end{pmatrix}$$

(ii) $C^{\perp}$ is the cyclic code generated by the polynomial

$$\bar{h}(x) = h_k + h_{k-1}x + \ldots + h_0 x^k$$

i.e. the reciprocal polynomial of h(x).

POLYNOMIAL REPRESENTATION of DUAL CODES

Proof A polynomial $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$ represents a code from C if $c(x)h(x) = 0$. For $c(x)h(x)$ to be 0 the coefficients at $x^k, \dots, x^{n-1}$ must be zero, i.e.

$$c_0h_k + c_1h_{k-1} + \dots + c_kh_0 = 0$$
$$c_1h_k + c_2h_{k-1} + \dots + c_{k+1}h_0 = 0$$
$$\cdot\cdot \qquad\qquad\qquad \cdot\cdot$$
$$c_{n-k-1}h_k + c_{n-k}h_{k-1} + \dots + c_{n-1}h_0 = 0$$

Therefore, any codeword $c_0 c_1 \dots c_{n-1} \in C$ is orthogonal to the word $h_k h_{k-1} \dots h_0 00 \dots 0$ and to its cyclic shifts.

Rows of the matrix H are therefore in $C^\perp$. Moreover, since $h_k = 1$, these row-vectors are linearly independent. Their number is $n - k = dim\ (C^\perp)$. Hence H is a generator matrix for $C^\perp$, i.e. a parity-check matrix for C.

In order to show that $C^\perp$ is a cyclic code generated by the polynomial

$$\bar{h}(x) = h_k + h_{k-1}x + \dots + h_0x^k$$

it is sufficient to show that $\bar{h}(x)$ is a factor of $x^n - 1$.

Observe that $\bar{h}(x) = x^k h(x^{-1})$ and since $h(x^{-1})g(x^{-1}) = (x^{-1})^n - 1$

we have that $x^k h(x^{-1}) x^{n-k} g(x^{-1}) = x^n(x^{-n} - 1) = 1 - x^n$

and therefore $\bar{h}(x)$ is indeed a factor of $x^n - 1$.

ENCODING with CYCLIC CODES I

Encoding using a cyclic code can be done by a multiplication of two polynomials - a message polynomial and the generating polynomial for the cyclic code.

Let C be an $[n,k]$-code over an field F with the generator polynomial

$g(x) = g_0 + g_1 x + \dots + g_{r-1} x^{r-1}$ of degree $r = n - k$.

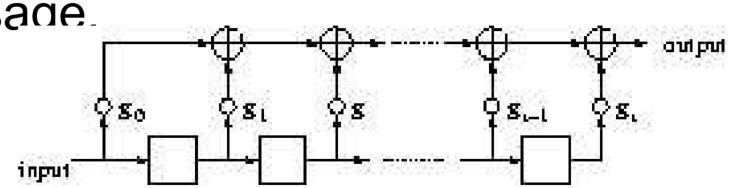
If a message vector m is represented by a polynomial $m(x)$ of degree k and m is encoded by

$$m \Rightarrow c = mG,$$

then the following relation between $m(x)$ and $c(x)$ holds

$$c(x) = m(x)g(x).$$

Such an encoding can be realized by the shift register shown in Figure below, where input is the k-bit message to be encoded followed by $n - k$ 0' and the output will be the encoded message.



Shift-register encodings of cyclic codes. Small circles represent multiplication by the corresponding constant, ⊕ nodes represent modular addition, squares are delay elements

Hamming codes as cyclic codes

Definition (Again!) Let r be a positive integer and let H be an $r * (2^r - 1)$ matrix whose columns are distinct non-zero vectors of $V(r,2)$. Then the code having H as its parity-check matrix is called binary **Hamming code** denoted by *Ham* $(r,2)$.

It can be shown that binary Hamming codes are equivalent to cyclic codes.

Theorem The binary Hamming code *Ham* $(r,2)$ is equivalent to a cyclic code.

Definition If $p(x)$ is an irreducible polynomial of degree r such that x is a primitive element of the field $F[x] / p(x)$, then $p(x)$ is called a primitive polynomial.

Theorem If $p(x)$ is a primitive polynomial over $GF(2)$ of degree r, then the cyclic code $\langle p(x) \rangle$ is the code *Ham* $(r,2)$.

Hamming codes as cyclic codes

Example Polynomial $x^3 + x + 1$ is irreducible over $GF(2)$ and x is primitive element of the field $F_2[x] / (x^3 + x + 1)$.

$$F_2[x] / (x^3 + x + 1) =$$

$$\{0, x, x^2, x^3 = x + 1, x^4 = x^2 + x, x^5 = x^2 + x + 1, x^6 = x^2 + 1\}$$

The parity-check matrix for a cyclic version of *Ham* $(3,2)$

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

PROOF of THEOREM

The binary Hamming code *Ham* (r,2) is equivalent to a cyclic code.

It is known from algebra that if p(x) is an irreducible polynomial of degree r, then the ring $F_2[x]$ / p(x) is a field of order 2^r.

In addition, every finite field has a primitive element. Therefore, there exists an element α of $F_2[x]$ / p(x) such that

$$F_2[x] / p(x) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2r-2}\}.$$

Let us identify an element $a_0 + a_1 + \ldots a_{r-1}x^{r-1}$ of $F_2[x]$ / p(x) with the column vector

$$(a_0, a_1, \ldots, a_{r-1})^T$$

and consider the binary r * (2^r -1) matrix

$$H = [\, 1 \;\; \alpha \;\; \alpha^2 \; \ldots \; \alpha^{2^\wedge r-2} \,].$$

Let now C be the binary linear code having H as a parity check matrix.

Since the columns of H are all distinct non-zero vectors of $V(r,2)$, C = *Ham* (r,2).

Putting $n = 2^r - 1$ we get

$$C = \{f_0 f_1 \ldots f_{n-1} \in V(n, 2) \mid f_0 + f_1 \alpha + \ldots + f_{n-1} \alpha^{n-1} = 0 \qquad (2)$$

$$= \{f(x) \in R_n \mid f(\alpha) = 0 \text{ in } F_2[x] / p(x)\} \qquad (3)$$

If f(x) $\in$ C and r(x) $\in$ R_n, then r(x)f(x) $\in$ C because

$$r(\alpha)f(\alpha) = r(\alpha) \bullet 0 = 0$$

and therefore, by one of the previous theorems, this version of *Ham* (r,2) is cyclic.

IV054 BCH codes and Reed-Solomon codes

To the most important cyclic codes for applications belong BCH codes and Reed-Solomon codes.

Definition A polynomial p is said to be ***minimal*** for a complex number x in Z_q if $p(x) = 0$ and p is irreducible over Z_q.

Definition A cyclic code of codewords of length n over Z_q, $q = p^r$, p is a prime, is called BCH code[1] of distance d if its generator $g(x)$ is the least common multiple of the minimal polynomials for

$$\omega^{l}, \omega^{l+1}, \ldots, \omega^{l+d-2}$$

for some l, where

ω is the primitive n-th root of unity.

If $n = q^m - 1$ for some m, then the BCH code is called primitive.

Definition A Reed-Solomon code is a primitive BCH code with $n = q - 1$.

Properties:

- Reed-Solomon codes are self-dual.

[1]BHC stands for Bose and Ray-Chaudhuri and Hocquenghem who discovered these codes.

CONVOLUTION CODES

Very often it is important to encode an infinite stream or several streams of data – say of bits.

Convolution codes, with simple encoding and decoding, are quite a simple generalization of linear codes and have encodings as cyclic codes.

An *(n,k)* convolution code (CC) is defined by an *k x n generator matrix, entries of which are polynomials over* F_2.

For example,

$$G_1 = [x^2 + 1, x^2 + x + 1]$$

is the generator matrix for a (2,1) convolution code CC_1 and

$$G_2 = \begin{pmatrix} 1 + x & 0 & x + 1 \\ 0 & 1 & x \end{pmatrix}$$

is the generator matrix for a (3,2) convolution code CC_2

ENCODING of FINITE POLYNOMIALS

An (n,k) convolution code with a k x n generator matrix G can be used to encode a k-tuple of plain-polynomials (polynomial input information)

$$I=(I_0(x), I_1(x),\ldots,I_{k-1}(x))$$

to get an n-tuple of crypto-polynomials

$$C=(C_0(x), C_1(x),\ldots,C_{n-1}(x))$$

As follows

$$C= I . G$$

EXAMPLES

EXAMPLE 1

$$(x^3 + x + 1).G_1 = (x^3 + x + 1)\ .\ (x^2 + 1, x^2 + x + 1]$$
$$= (x^5 + x^2 + x + 1, x^5 + x^4 + 1)$$

EXAMPLE 2

$$(x^2 + x, x^3 + 1).G_2 = (x^2 + x, x^3 + 1).\begin{pmatrix} 1+x & 0 & x+1 \\ 0 & 1 & x \end{pmatrix}$$

ENCODING of INFINITE INPUT STREAMS

The way infinite streams are encoded using convolution codes will be Illustrated on the code CC_1.

An input stream $I = (I_0, I_1, I_2, \ldots)$ is mapped into the output stream $C = (C_{00}, C_{10}, C_{01}, C_{11} \ldots)$ defined by

$$C_0(x) = C_{00} + C_{01}x + \ldots = (x^2 + 1)\, I(x)$$

and

$$C_1(x) = C_{10} + C_{11}x + \ldots = (x^2 + x + 1)\, I(x).$$

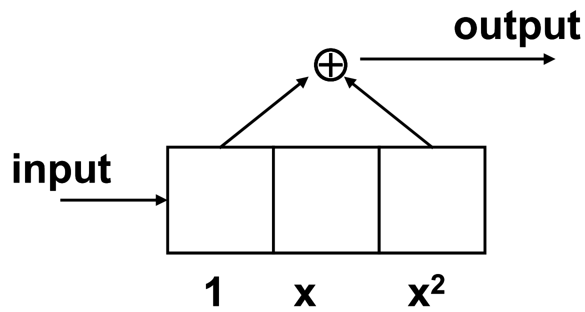
The first multiplication can be done by the first shift register from the next figure; second multiplication can be performed by the second shift register on the next slide and it holds

$$C_{0i} = I_i + I_{i+2}, \qquad C_{1i} = I_i + I_{i-1} + I_{i-2}.$$

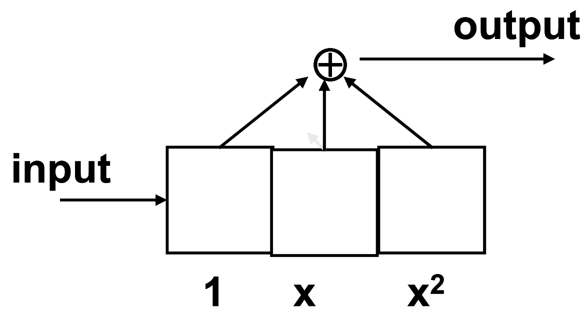
That is the output streams C_0 and C_1 are obtained by convolving the input stream with polynomials of G_1.

 ENCODING

The first shift register

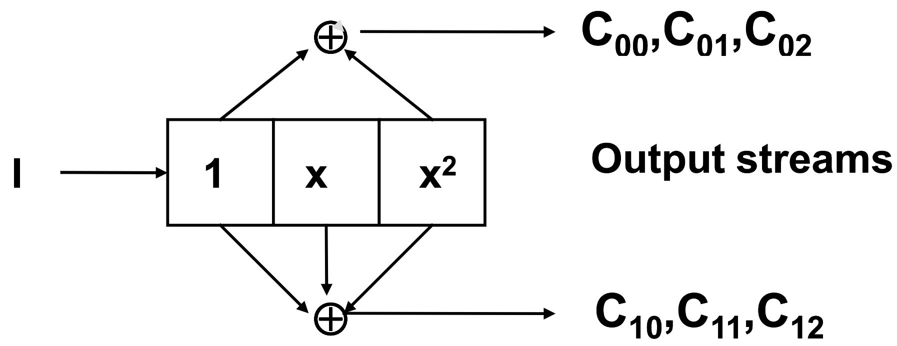


will multiply the input stream by x^2+1 and the second shift register



will multiply the input stream by x^2+x+1.

The following shift-register will therefore be an encoder for the code CC_1



For encoding of the convolution codes so called

Viterbi algorithm

Is used.