CONVOLUTION CODES

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

$$C= I \cdot G$$

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

$$(x^2 + x, x^3 + 1).G_2 = (x^2 + x, x^3 + 1).\begin{pmatrix} 10 & x+1 \\ 01 & x \end{pmatrix}$$

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

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

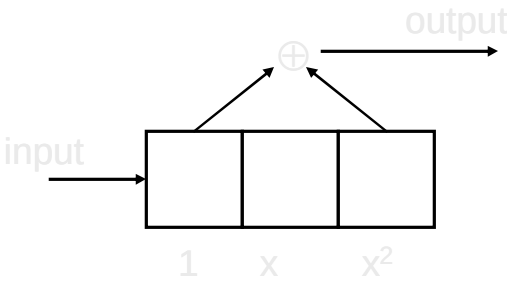
The first multiplication can be done by the first shift register from the next figure; second multiplication can be performed by the second shift register on the next slide and it holds

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

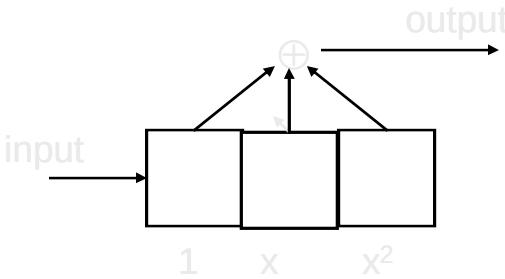
That is the output streams C_0 and C_1 are obtained by convolving the input stream with polynomials of G_1,

ENCODING

The first shift register



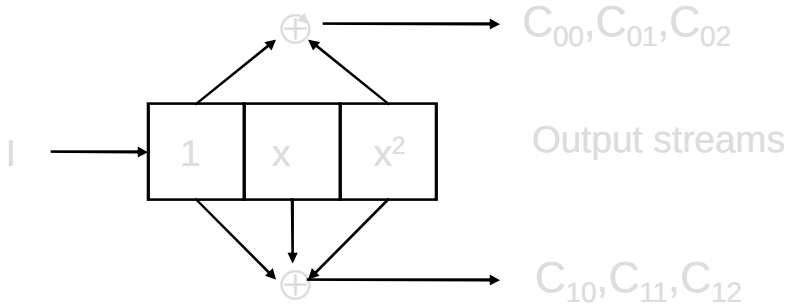
will multiply the input stream by x^2+1 and the second shift register



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

ENCODING and DECODING

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



For encoding of convolution codes so called

Viterbi algorithm

Is used.