Communications Theory and Engineering

Master's Degree in Electronic Engineering

Sapienza University of Rome

A.A. 2019-2020

Block codes and convolutional codes

Parity check matrix

Soft and hard decoders find codewords closest (in Euclidean or Hamming distances) to the received block.

Implementation becomes difficult for large and k and n, since there are 2^k distances that need to be computed and compared.

For hard decoding it is possible to implement efficient decoding techniques

Parity check matrix

Consider a systematic linear *(n, k)* block code, which has a generator matrix of the form

$$G = \left[I_k \mid P \right]$$

Given a row vector b of k bits, the corresponding codeword is $c=bG$, a row vector which can be written

$$c = \left[b \quad a \right]$$

where $a=bP$ is a row vector with n-k parity-check bits and one has

$$bP \oplus a = 0$$

$$\left[b \quad a \right] \begin{bmatrix} P \\ I_{n-k} \end{bmatrix} = 0$$

Parity check matrix

$$bP \oplus a = 0$$

$$\begin{bmatrix} b & a \end{bmatrix} \begin{bmatrix} P \\ I_{n-k} \end{bmatrix} = 0$$

or

$$cH' = 0 \quad with$$

$$H = \begin{bmatrix} P' | I_{n-k} \end{bmatrix}$$

H is called the parity-check matrix

H can be used to check if a vector c is a codeword

Example: the code for parity control *(k + 1, k)*

For the parity check code *(k + 1, k)* the parity check matrix is

$$H = \begin{bmatrix} 1 & 1 & 1 & . & . & . & 1 & 1 \end{bmatrix}$$

One can check in fact if a bit vector is a codeword by summing (modulo-two) all of the bits and checking if the sum is zero.

Example - Hamming code (7,4)

The parity-check matrix for the *(7,4)* Hamming code is

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

c_2 =[0110101], is not a codeword and c_2H'= [100]

while c = [0110001] is a code word since cH'=0

Syndrome

A parity check matrix can be found for all linear codes even though they are non-systematic block

The parity check matrix is a compact representation of a code

For a received vector c_r a transmitted codeword c_t and the error pattern e, one has:

$$c_r = c_t \oplus e$$

And the syndrome is defined

$$s = c_r H' = c_t H' + eH' = eH'$$

The syndrome is zero if c_r is a codeword, which occurs if and only if e is a codeword (recall that 0 is always a codeword of a linear code). Efficient decoders use the syndrome to flag the position of an error, which can then be corrected

Hamming codes

For any positive integer m there exists a Hamming code with

$$(n,k) = (2^m - 1, 2^m - 1 - m)$$

The parity-check matrix has n columns each with n–k bits

For a Hamming code, the parity-check matrix is constructed by letting the $n=2^m-1$ columns be all possible binary vectors with m=n-k elements, except the zero vector

Cyclic codes

The most practical block codes are cyclic codes

An (n,k) linear block code is said to be cyclic if any cyclic shift of a codeword produces another codeword

Some Hamming codes are cyclic codes

The algebraic properties of cyclic codes permit collapsing the information contained by the generator matrix into a single polynomial, called the generator polynomial, or by the dual parity polynomial

BCH and Reed-Solomon codes

The most important cyclic codes are the BCH codes

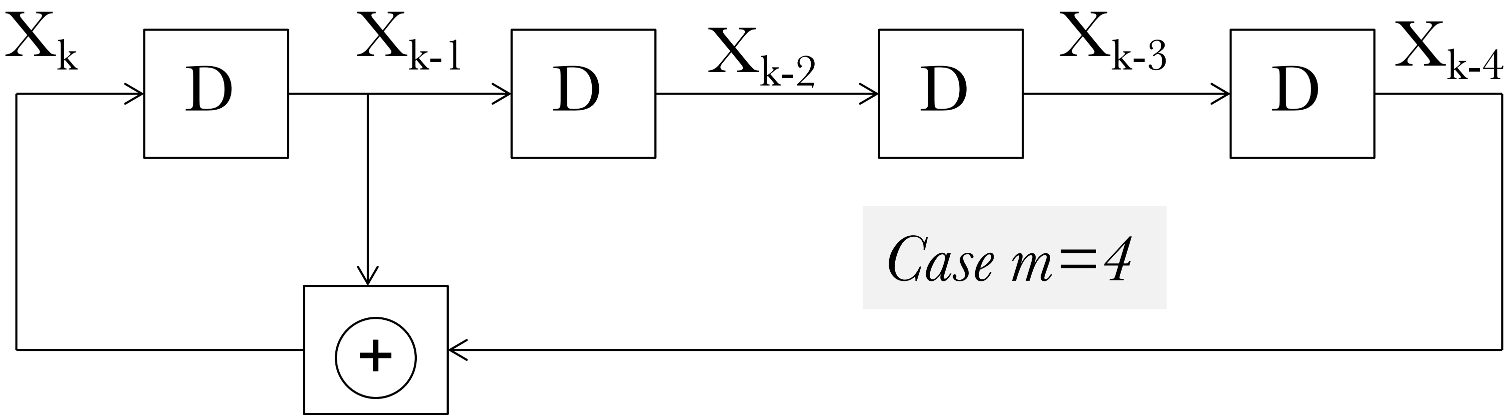
Bose, Ray-Chaudhuri, Hocquenghem, 1960

These are very efficient codes that allow the correction of multiple errors (satellite communications, CDs, DVDs)

A subset of these codes are the very famous Reed-Solomon codes (Voyager, CD, Blueray, QRcodes, Wimax, DSL, DVB)

Maximal-Length Shift Register Codes

Maximal-length shift register codes



The shift register is loaded with *4* bits and clocked 2^m*-1* times

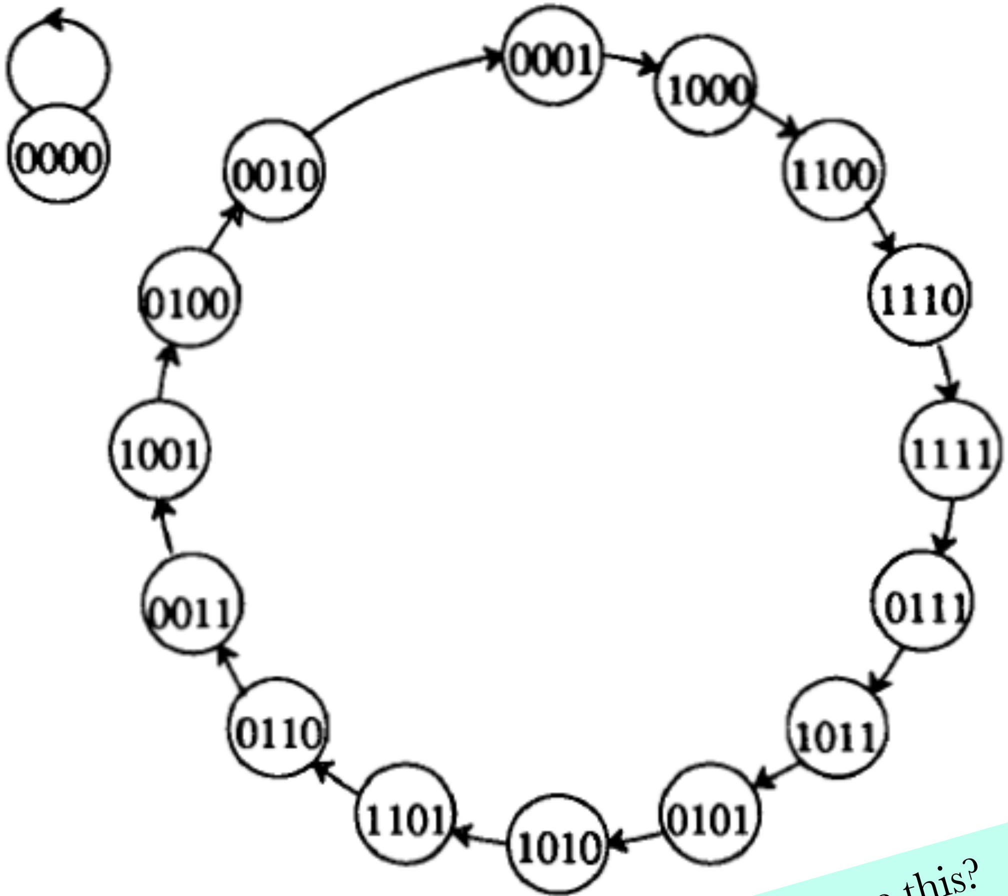
The output forms the 2^m*-1* length code

The result is an $(n,k)=(2^m-1, m)$ block code

The output is periodic with period 2^m-1

The code is cyclical

Example: state transition matrix for the m=4 maximal-length shift register



This is a cyclic code *(15,4)* in the case *m=4*

$$t = \left\lfloor \frac{d_{H,\min} - 1}{2} \right\rfloor$$

The Hamming weight is 2^{m-1}

Can you prove this?

The minimum Hamming distance is *8*

Correction capacity: *3* bit errors

Convolutional codes

A convolutional coder is a finite memory system (rather than a memoryless system, as in the case of the block coder).

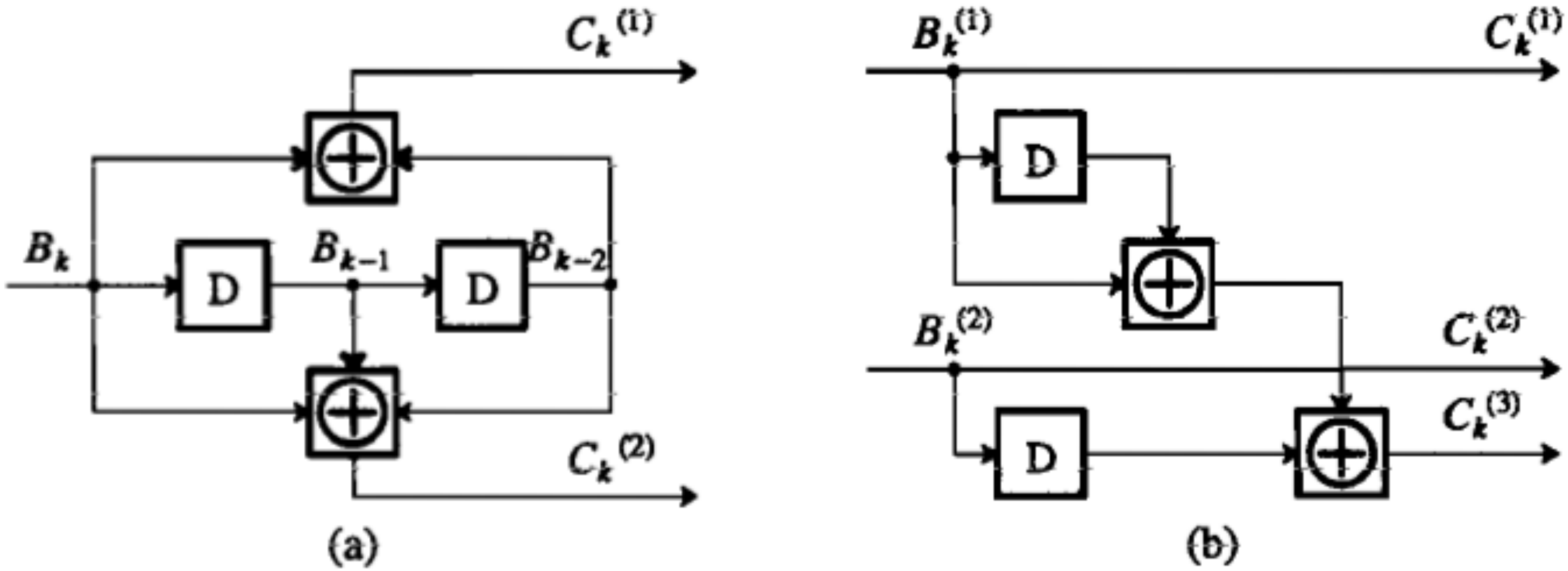
The name refers to the fact that the added redundant bits are generated by modulo-two convolutions

Convolutional codes are widely used because they provide better performance than block codes

A good part of their performance is attributable to the availability of practical soft decoding techniques.

As for block codes, linear convolutional coders are constructed using modulo-two adders with the addition of delay elements.

Example of convolutional codes



Conv*(1/2)*
Rate *1/2*

Conv*(2/3)*
Rate *2/3*
Note: it is systematic

Generator matrix

Example of the conv*(1/2)* case

$$G(D) = \left[1 \oplus D^2, 1 \oplus D \oplus D^2\right]$$

Example of the conv*(2/3)* case

$$G(D) = \begin{bmatrix} 1 & 0 & 1 \oplus D \\ 0 & 1 & D \end{bmatrix}$$

Parity check matrix

Example
conv*(2/3)*

$$G(D)=\begin{bmatrix} 1 & 0 & 1\oplus D \\ 0 & 1 & D \end{bmatrix}=\left[I_k \mid P\right]$$

$$H=\left[P' \mid I_{n-k}\right]=\left[1\oplus D, D, 1\right]$$

Verify that for all codewords one has

$$C(D)H'(D)=0$$

$$C_k^{(1)}\oplus C_{k-1}^{(1)}\oplus C_{k-1}^{(2)}=C_k^{(3)}$$

$$\Rightarrow C^{(3)}(D)=(1\oplus D)C^{(1)}(D)\oplus DC^{(2)}(D)$$

$$\Rightarrow (1\oplus D)C^{(1)}(D)\oplus DC^{(2)}(D)\oplus C^{(3)}(D)=0$$

$$\Rightarrow C(D)H'(D)=0$$

Length of a convolutional code

The constraint length of a convolutional code is defined as *1+* the maximum degree of the polynomials in the generator matrix

$$M = 1 + \max_{i,j}\left[\deg\left(g_{ij}(D)\right)\right]$$

For conv*(1/2)*, *M=3*

For conv*(2/3)*, *M=2*