Cyclic Codes

The cyclic property of code words is that any cyclic-shift of a code word is also a code word. Cyclic codes follow this cyclic property.

For a linear code **C**, if every code word i.e., **C =** C1,C2,......CnC1,C2,......Cn from C has a cyclic right shift of components, it becomes a code word. This shift of right is equal to **n-1** cyclic left shifts. Hence, it is invariant under any shift. So, the linear code **C**, as it is invariant under any shift, can be called as a **Cyclic code**.

Cyclic codes are used for error correction. They are mainly used to correct double errors and burst errors.

Hence, these are a few error correcting codes, which are to be detected at the receiver. These codes prevent the errors from getting introduced and disturb the communication. They also prevent the signal from getting tapped by unwanted receivers.

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 a0, . . . an−1 ∈ C, then also an−1a0 . . . an–2 ∈ C and a1a2 . . . an−1a0 ∈ C.

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

(ii) Hamming code Ham(3, 2): with the generator matrix G = 2 6 6 4 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 3 7 7 5 is equivalent to a cyclic code.

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

(iv) Is Hamming code Ham(2, 3) with the generator matrix » 1 0 1 1 0 1 1 2

Cyclic codes form a subclass of linear block codes. Indeed, many of the important linear block codes discovered to date are either cyclic codes or closely related to cyclic codes. An advantage of cyclic codes over most other types of codes is that they are easy to encode. Furthermore, cyclic codes possess a well-defined mathematical structure, which has led to the development of very efficient decoding schemes for them. A binary code is said to be a *cyclic code* if it exhibits two fundamental properties:

PROPERTY 1 **Linearity Property**

The sum of any two codewords in the code is also a codeword.

PROPERTY 2 **Cyclic Property**

Any cyclic shift of a codeword in the code is also a codeword.

Property 1 restates the fact that a cyclic code is a linear block code (i.e., it can be described as a parity-check code). To restate Property 2 in mathematical terms, let the *n*-tuple denote a codeword of an linear block code. The code is a cyclic code if the *n*-tuples

$cn - 2 \; cn - 1 + cn - 3$

$c1 \; c2 + cn - 1 \; c0$

are all codewords in the code.

To develop the algebraic properties of cyclic codes, we use the elements of a codeword $\mathbf{c}+X+ \; c0 \; c1X \; c2X2 + cn \; 1 - Xn - 1$to define the code polynomial where X is an indeterminate. Naturally, for binary codes, the coefficients are 1s and 0s. Each power of X in the polynomial represents a one-bit *shift* in time. Hence, multiplication of the polynomial by X may be viewed as a shift to the right. The key question is: How do we make such a shift *cyclic*? The answer to this question is addressed next.

Let the code polynomial in (10.27) be multiplied by Xi, yielding

$$\mathbf{C}+X+ \; c0 \; c1X \; c2X2 + cn \; 1 - Xn - 1$$

where X is an indeterminate. Naturally, for binary codes, the coefficients are 1s and 0s. Each power of X in the polynomial represents a one-bit *shift* in time. Hence, multiplication of the polynomial by X may be viewed as a shift to the right If $\mathbf{c}(X)$ is a code polynomial, then the polynomial is also a code polynomial for any cyclic shift i; the term mod is the abbreviation for modulo

Reed-Solomon Codes:

Reed Solomon (R-S) codes form an important sub- class of the family of Bose-Chaudhuri-Hocquenghem (BCH) codes and are very powerful linear non-binary block codes capable of correcting multiple random as well as burst errors. They have an important feature that the generator polynomial and the code symbols are derived from the same finite field. This enables to reduce the complexity and also the number of computations involved in their implementation. A large number of R-S codes are available with different code rates.

An R-S code is described by a generator polynomial g(x) and other usual important code parameters such as the number of message symbols per block (k), number of code symbols per block (n), maximum number of erroneous symbols (t) that can surely be corrected per block of received symbols and the designed minimum symbol Hamming distance (d). A parity-check polynomial h (X) of order k also plays a role in designing the code. The symbol x, used in polynomials is an indeterminate which usually implies unit amount of delay.

For positive integers m and t, a primitive (n, k, t) R-S code is defined as below: Number of encoded symbols per block: n = 2m – 1 Number of message symbols per block: k Code rate: R= k/n Number of parity symbols per block: n – k = 2t Minimum symbol Hamming distance per block: d = 2t +1. It can be noted that the block length n of an (n, k, t) R-S code is bounded by the corresponding finite field GF(2m). Moreover, as n – k = 2t, an (n, k, t) R-S code has optimum error correcting capability.

APPLICATIONS of REED-SOLOMON CODES

- Reed-Solomon codes have been widely used in mass storage systems to correct the burst errors caused by media defects.
- Special types of Reed-Solomon codes have been used to overcome unreliable nature of data transmission over erasure channels.
- Several bar-code systems use Reed-Solomon codes to allow correct reading even if a portion of a bar code is damaged.
- Reed-Solomon codes were used to encode pictures sent by the Voyager spacecraft. Modern versions of concatenated Reed-Solomon/Viterbi decoder convolution coding were and are used on the Mars Pathfinder, Galileo, Mars exploration Rover and Cassini missions, where they performed within about 1-1.5dB of the ultimate limit imposed by the shannon capacity