FORWARD ERROR CORRECTION SCHEMES FOR DIGITAL COMMUNICATIONS

VIJAY K. BHARGAVA

THE utility of coding was demonstrated by the work of Shannon in 1948. Shannon's work established that the ultimate limit of performance set by the noise on the channel is not the accuracy, but the rate at which data can be reliably transmitted.

A block diagram which describes the digital communication process using forward error correction (FEC) is shown in Fig. 1. This paper shall not be concerned with error control coding schemes which involve some type of detection and retransmission—the so-called automatic repeat request (ARQ) procedures [1].

Encoder—Decoder (CODEC)

Historically, the coding systems have been separated into block and convolutional error-correcting techniques.

In an (n,k) linear block code a sequence of k information bits is algebraically related to n-k parity bits to give an overall encoded block of n bits. Usually modulo-2 arithmetic is used, which is simply the EXCLUSIVE-OR operation in logic. In this arithmetic $1 \oplus 1 = 0$ and there are never any "carries." Hence, an odd number of 1's sums to 1. Linear codes form a linear vector space and have the very important property that two code words can be added to produce a third code word. The code rate is $r = k/n$, and n is called the block length. Note that the introduction of error-control coding requires more capacity; this can be in the form of wider bandwidth, longer bursts in time division multiple access (TDMA) systems, or a higher "chip" rate (and hence a higher bandwidth) in spread spectrum systems, if the same processing gain is needed.

The Hamming weight of a code word $\underline{c}$, denoted $w(\underline{c})$, is defined to be the number of nonzero components of $\underline{c}$. For example, if $\underline{c} = (110101)$, then $w(\underline{c}) = 4$. The Hamming distance between two code words $\underline{c}_1$ and $\underline{c}_2$, denoted $d(\underline{c}_1, \underline{c}_2)$, is the number of positions in which they differ. For example if $\underline{c}_1 = (110101)$ and $\underline{c}_2 = (111000)$ then $d(\underline{c}_1, \underline{c}_2) = 3$. Clearly, $d(\underline{c}_1, \underline{c}_2) = w(\underline{c}_1 \oplus \underline{c}_2) = w(\underline{c}_3)$, where $\underline{c}_3$, for linear codes, is a code word. Therefore, the distance between any two code words equals the weight of one of the code words and the minimum distance d for a linear block code equals the minimum weight of its nonzero code words.

A code can correct all patterns of t or fewer random errors and detect all patterns having no more than s errors, provided that $s + t + 1 \leqslant d$. Only if the code is used for error correction can the code correct all patterns of t or fewer random errors, provided that $2t + 1 \leqslant d$.

Convolutional codes are a subset of the so-called tree codes. A convolutional code of rate $1/v$ may be generated by a K stage shift register and v modulo-2 adders. A simple example is the rate 1/2 convolutional encoder shown in Fig. 2.

Information bits are shifted in at the left, and for each information bit the output of the modulo-2 adders provide two channel bits. The constraint length of the code expressed in information bits is defined as the number of shifts over which a single information bit can influence the encoder output. For the simple binary convolutional code, the constraint length is equal to K, the length of the shift register.

The decoder uses the redundancy introduced in the process of encoding and sometimes the reliability (defined below) of

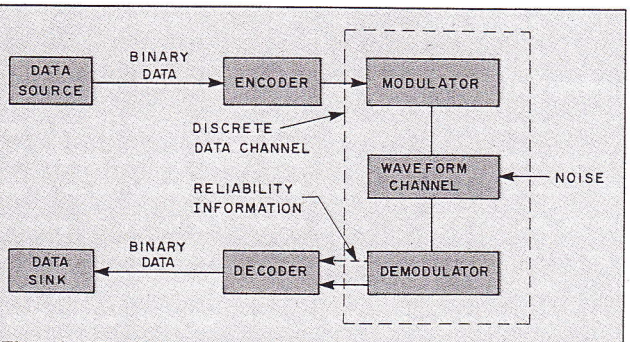

Fig. 1. Digital communication process using forward error correction.

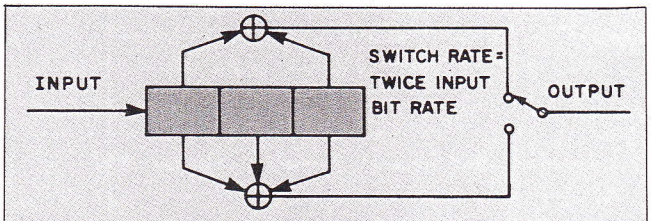

Fig. 2. Encoder for a rate ½, constraint length −3 convolutional code.

0163-6804/83/0100-0011 $01.00 © 1983 IEEE

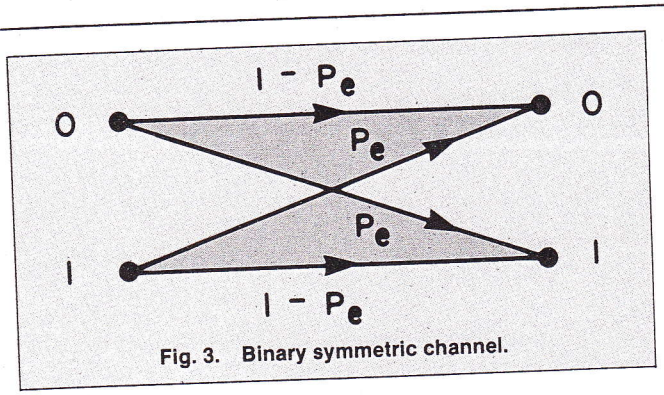

Fig. 3. Binary symmetric channel.

the received information to decide which information bit was actually sent.

Modulator—Demodulator (MODEM)

The encoded sequence is suitably modulated and transmitted over the noisy channel. In systems where coherent demodulation is possible (that is, where a carrier reference can be obtained), phase shift keying (PSK) is often used. In binary PSK an encoded 1 is represented by the wave form $s_1(t) = A\cos \omega_c t$, while an encoded 0 is represented by the antipodal signal $s_0(t) = -s_1(t) = A\cos(\omega_c t + \pi)$, the waveforms changing at discrete times T_s seconds (symbol duration) apart.

The physical channel or the waveform channel consists of all the hardware (for example, filtering and amplification) and the physical media that the waveform passes through in going from the output of the modulator to the input of the demodulator.

The demodulator estimates which of the possible symbols was transmitted, based upon an observation of the received signal. For PSK with white Gaussian noise and perfect phase tracking, the optimum receiver is a correlator or matched filter receiver which is sampled each T_s seconds to determine its polarity. It is easily shown that the voltage z, at the matched filter output at the sample time is a Gaussian random variable with mean $\pm\sqrt{E_s}$, (depending upon whether a 1 or 0 was transmitted) and variance $\sigma^2 = N_o/2$. In the above E_s is the energy per symbol (what we pay) and N_o denotes the one sided noise spectral density (what we must combat). When a symbol differs from a bit (that is, when we use coding) we will denote the energy per bit by E_b.

Hard Decisions, Soft Decisions

In practical communication systems, we rarely have the ability to process the actual analog voltages z_i (the values taken by the random variable z). The normal practice is to quantize these voltages. If a binary quantization is used, we say that a *hard decision* has been made on the correlator output as to which level was actually sent. In this case, we have the so-called binary symmetric channel (BSC) with probability of error P_e, shown in Fig. 3. For example, in coherent PSK with equally likely transmitted symbols, the optimum threshold is at zero. Then the demodulator output is a zero if the voltage z at the matched filter output is negative. Otherwise, the output is a one.

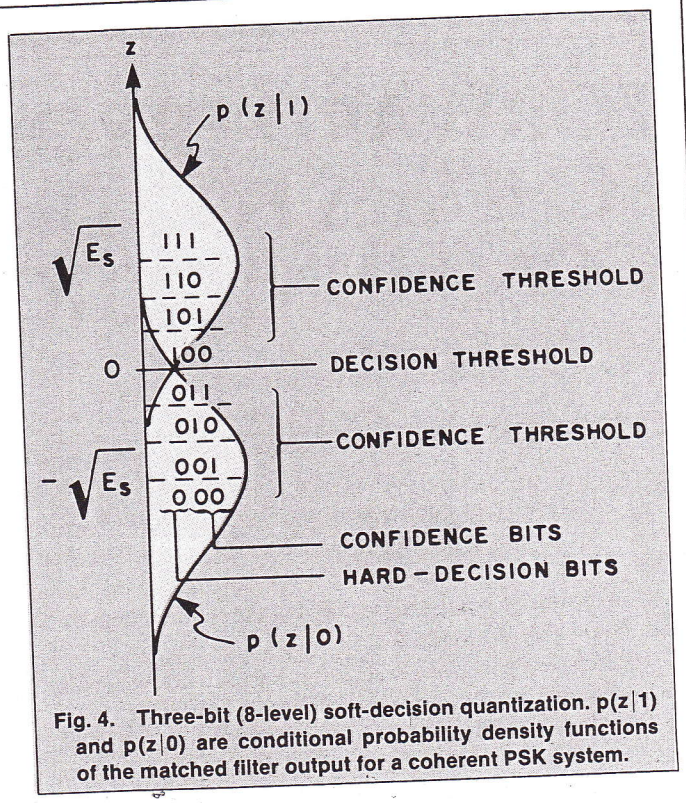

Fig. 4. Three-bit (8-level) soft-decision quantization. p(z|1) and p(z|0) are conditional probability density functions of the matched filter output for a coherent PSK system.

With coding, it is desirable to keep an indication of how reliable the decision was. A *soft-decision* demodulator first decides whether the output voltage is above or below the decision threshold, and then computes a "confidence" number which specifies how far from the decision threshold the demodulator output is. This number in theory could be an analogue quantity, but in most practical applications a three-bit (eight-level) quantization is used.

An example of three-bit quantization is shown in Fig. 4. The input to the demodulator is binary, while the output is 8-ary, delineated by one decision threshold and three pairs of confidence thresholds. The information available to the decoder is increased considerably and translates as an additional gain of 2 dB in most instances [2]. The receiver complexity is increased as an AGC will probably be needed, and three bits will have to be manipulated for every channel bit. The channel resulting from three-bit quantization on a Gaussian channel is called the binary input, 8-ary output, discrete memoryless channel (DMC), and is shown in Fig. 5.

Coding Gain

Before we start our study of codes, consider a Gaussian memoryless channel with one-sided noise spectral density N_o and under no bandwidth limitation. Let E_b denote the received energy per bit. Then it can be shown that for E_b/N_0 greater than -1.6 dB, there exists some coding scheme which allows us to communicate with zero error, while reliable communication is not generally possible at lower signal-to-noise ratios. On the other hand, it is well known that uncoded PSK over the same channel will require about 9.6 dB to achieve a bit error rate of 10^{-5}. Thus, as shown in Fig. 6, a potential coding gain of 11.2 dB is theoretically possible. Coding gain is defined as

the difference in values of E_b/N_o required to attain a particular error rate without coding and with coding.

It must be stressed that this coding gain is obtained at the expense of an increase in the necessary transmission bandwidth. The bandwidth expansion is the reciprocal of the coding rate. Thus, for a rate-1/2 code, the transmitted symbol energy E_s is 3 dB less than E_b. We also point out that coding gain is a useful concept only when one can obtain performance improvements by increasing the power. In certain communication links at high signal-to-noise ratios, there is a floor on performance that can not be overcome by simply increasing the power. The use of coding might considerably reduce the floor or make it disappear altogether. In such a situation one might be tempted to say that the coding gain is infinite, but this tends to be a meaningless statement. The fact is that without coding the desired performance could never have been obtained [2].

While another revolution in coding may be needed to deliver the theoretically possible coding gain of 11.2 dB, it is safe to say that coding systems (delivering 2-6 dB) will be used routinely in digital communication links as hardware costs decrease and system complexity increases. There are several reasons for this [9]:

1. Phenomenal decrease in the cost of digital electronics.
2. Significant improvement in various decoding algorithms.
3. Much slower (or no) decrease in the cost of analog components, such as power amplifier, antenna and so on.

Asymptotic coding gain, a figure of merit for a particular code, depends only on the code rate and the minimum distance. To define it, consider a t-error correcting code with rate r and minimum distance $d \geq 2t + 1$. If we use the code with a hard decision PSK demodulator, it can be shown that the bit error rate P_b is [2]

$$P_{b,h} \geq Q(\sqrt{2E_b r(t+1)/N_o})$$

where $Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-y^2/2}\, dy.$

With a soft-quantized PSK demodulator, we have

$$P_{b,s} \geq Q(\sqrt{2E_b rd/N_o}).$$

Recall that for uncoded PSK

$$P_b = Q(\sqrt{2E_b/N_o})$$

Thus, the asymptotic coding gain G_a for the two cases is:

$$G_a \leq r(t+1) = 10 \log r(t+1),\ dB \text{ (hard decision)}$$
$$G_a \leq rd = 10 \log rd,\ dB \text{ (soft decision)}$$

The above indicates that soft decision decoding is about 3 dB more efficient than hard decision decoding at very high E_b/N_o. A figure of 2 dB is more likely at realistic values of E_b/N_o.

Block Codes and Their Decoding

We shall illustrate the idea of a block code by the following example:

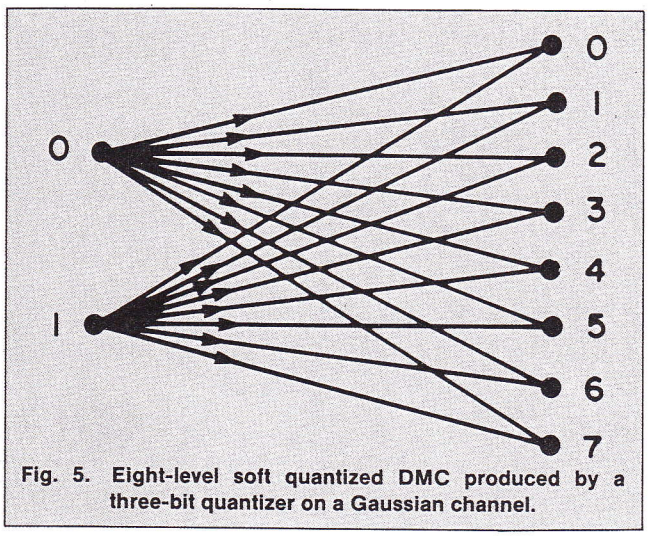

Fig. 5. Eight-level soft quantized DMC produced by a three-bit quantizer on a Gaussian channel.

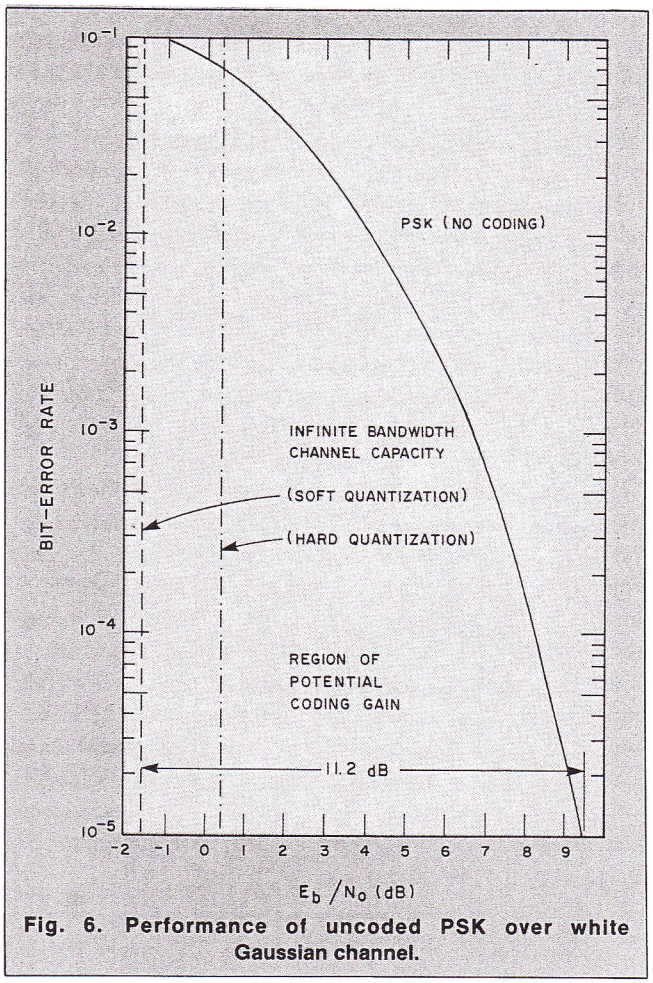

Fig. 6. Performance of uncoded PSK over white Gaussian channel.

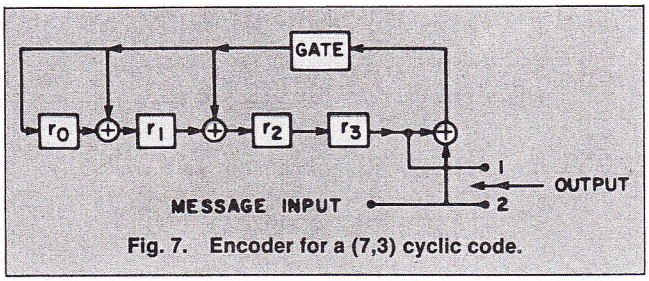

Fig. 7. Encoder for a (7,3) cyclic code.

Example 1

Consider the set of code words (000000), (001101), (010011), (011110), (100110), (101011), (110101) and (111000). These $2^3 = 8$ code words form a vector space of dimension three and thus a (6,3) code. The minimum weight (of nonzero code words) is 3 and hence the minimum distance is 3. Thus, the code is single-error correcting.

Block codes are also called parity check codes, for if $\underline{c} = (c_1,c_2,c_3,c_4,c_5,c_6)$ is a code word in the code of Example 1, then knowing c_1,c_2,c_3 allows one to solve for the other three bits by using the following parity check equations:

$$c_1 \oplus c_3 = c_4$$
$$c_1 \oplus c_2 = c_5$$
$$c_2 \oplus c_3 = c_6$$

The code of this example is said to be in the systematic form; the first three bits in any code word can be considered as the message bits while the last three bits, which are calculated from the first three bits, are the redundant or parity bits.

Cyclic Codes

It is perhaps a remarkable fact that many of the important block codes found to date can be reformulated to be cyclic codes or closely related to cyclic codes. For such codes, if an n tuple $\underline{c} = (c_0,c_1,c_2,\ldots,c_{n-1})$ is a code word, the n tuple $\underline{c}' = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ obtained by shifting $\underline{c}$ cyclically one place to the right is also a code word. This class of codes can be easily encoded using linear shift registers with feedback. Further, because of their inherent algebraic structure, the decoding has been greatly simplified, both conceptually and in practice.

Examples of cyclic and related codes include the Bose-Chaudhuri-Hocquenhem (BCH), Reed-Solomon, Hamming, maximal-length, Reed-Müller, Golay, quadratic residue, projective geometry, Euclidean geometry, difference sets, Goppa, and quasi-cyclic codes. The classes form overlapping sets so that a particular code may be a BCH code and also a quadratic residue code. Recent applications of codes from this family to digital communication include a (31,15) Reed-Solomon code for the joint tactical information distribution system (JTIDS), a (127,112) BCH code for the INTELSAT V system, and a (7,2) Reed-Solomon code for the air force satellite communications (AFSATCOM) wideband channels [1].

Example

Consider the encoder of Fig. 7, which generates a (7,3) cyclic code. Suppose we wish to encode (010). With the gate turned on and the switch in position 2, information bits shift into register and into the channel sequentially, and the contents of the shift register are as follows:

	r_0	r_1	r_2	r_3
Initial state	0	0	0	0
First shift	0	0	0	0
Second shift	1	1	1	0
Third shift	0	1	1	1

The gate is then turned off, the switch is thrown to position 1 and the four parity bits (0111) are shifted to obtain the encoded word as

(0111 010)

The Concept of Syndrome and Error Detection

The basic element of the decoding procedure consists of computing the syndrome defined according to the following operation: re-encode the received information bits to compute a parity sequence in exactly the same fashion as the encoder; compare these parity bits to the corresponding parity bits actually received using a modulo-2 adder whose output forms the syndrome.

Clearly, when no errors have occurred, the parity bits computed at the decoder will be identical to those actually received, and the syndrome bits will be zero. If the syndrome bits are not zero, then errors have been detected.

For error correction the syndrome is processed further. Thus, error correction is substantially more involved than error detection.

Summary of Important Classes of Block Codes

In this section we discuss the characteristics of some important classes of block codes. Most of them are cyclic (or related to cyclic codes). Further, we limit ourselves to only binary codes.

Bose-Chaudhuri-Hocquenghem (BCH) Codes

The BCH codes are the best constructive codes for channels in which errors affect successive symbols independently. These codes are cyclic and have the following parameters:

Block length: $n = 2^m - 1$, $m = 3,4,5,\ldots$
Number of information bits: $k \geq n - mt$
Minimum distance: $d \geq 2t + 1$

Reed-Solomon Codes

Each symbol here can be represented as m bits. These codes have the parameters:

Symbols: m bits per symbol
Block length: $n = 2^m - 1$ symbols $= m(2^m - 1)$ bits
Number of parity symbols: $(n - k) = 2t$ symbols $= m \cdot 2t$ bits
Minimum distance: $d = 2t + 1$ symbols

Example 2

Let $t = 1$ and $m = 2$. Denoting the symbols as 0, 1, 2, and 3,

we can write their binary representation as

$$0 = 00$$
$$1 = 01$$
$$2 = 10$$
$$3 = 11$$

and we have a code with the following parameters:

$$n = 2^2 - 1 = 3 \text{ symbols} = 6 \text{ bits}$$
$$(n - k) = 2 \text{ symbols} = 4 \text{ bits}$$

This code can correct any inphase burst (i.e. spanning a symbol) of length 2.

For example, suppose the code word (1,2,3) was transmitted. We write it as (01 10 11). Since the code is one-symbol error correcting, it will decode any inphase burst error of length 2. In general, a t symbol error correcting Reed-Solomon code can correct t inphase bursts of length m bits in each code word.

For any (n,k) code with minimum distance d, it can be shown that $d \leqslant n - k + 1$. Since $d = n - k + 1$ for RS codes, they are called maximum distance separable. Reed-Solomon codes are now commercially available with development spurred by military tactical communication.

Reed-Solomon codes are extremely well suited for burst-error correction and for use as outer codes in a powerful coding system known as the concatenated coding system [2]. The basic idea of concatenation is to factor the channel encoder and decoder in a way shown in Fig. 8. By choosing an inner code (block or convolutional) appropriately and taking a Reed-Solomon code as the outer code, lower decoding complexity and larger coding gains are possible compared to an unfactored system.

Golay Code

This is a very special three-error correcting (23,12) cyclic code with minimum distance 7 and is based on the following tantalizing number theoretic fact: $1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2048 = 2^{11}$, which makes the code a "perfect" code. The code has been widely used as a (24,12) code with minimum distance 8 by adding an extra parity bit which is a parity check over the other 23 bits. Unfortunately, the Golay code does not generalize to other combinations of n and k.

Hamming Codes

These are cyclic codes having the following parameters:

Block length: $n = 2^m - 1$
Number of parity bits: $k = m$
Minimum distance: $d = 3$

Maximum-Length Codes

These are cyclic codes with the following parameters:

Block length: $n = 2^m - 1$
Number of information bits: $k = m$
Minimum distance: $d = 2^m - 1$

These codes are related to maximal-length sequences used extensively in spread spectrum communications and for closed-loop time-division multiple-access synchronization, to name two examples [1]. They are also called simplex codes, an intriguing contact between algebraic coding theory and the geometry of n dimensions [3].

Quadratic Residue Codes

The minimum distances of codes in this family are typically comparable to those of BCH codes of comparable lengths. The quadratic residue codes are cyclic codes with the following parameters:

Block length: $n = p$ a prime number of the form $8m \pm 1$
Number of information bits: $k = (p + 1)/2$
Minimum distance: $d > \sqrt{n}$

The above list is by no means an exhaustive list. For example, we have not mentioned codes based on the combinatorial configurations of finite geometries, Goppa codes, quasi-cyclic codes, to name a few [5].

Decoding of Block Codes

The algebraic structure imposed on block codes has produced a number of decoding techniques for these codes, and the theory is quite well developed. Thus, the various schemes will be touched upon only briefly. To use many of these techniques requires the use of binary quantization (hard decisions) at the demodulator output. The first step is to form the syndrome. In medical parlance, a syndrome is a pattern of symptoms that aids in the diagnosis of a disease. Here the "disease" is the error pattern and a "symptom" is a parity check failure. This felicitous coinage is due to Hagelbarger [3]. To correct errors, the syndrome is processed further using any one of the following methods:

Table look up decoding—It can be shown that there is a unique correspondence between the 2^{n-k} distinct syndromes and the correctable error patterns. Thus, for codes with small redundancy we can store the error patterns in a read-only memory (ROM) with the syndrome of the received word forming the address. The error pattern would then be added modulo-2 to the received sequence to produce the transmitted code word.

Example 3

For the code of Example 1, the following correspondence can be established:

Fig. 8. Concatenated coding system.