International Journal of Computer Applications in Engineering Sciences
[VOL I, ISSUE II, JUNE 2011] [ISSN: 2231-4946]

Error Control Techniques and Their Applications

Rubal Chaudhary[1], Vrinda Gupta[2]

[1, 2]*Dept of Electronics and Communication Engineering*
NIT, Kurukshetra

[1]`rubal39@gmail.com`
[2]`vrindag16@yahoo.com`

***Abstract* -This paper is an introduction to the subject of error-control coding. Undesirable disturbances like noise, EMI, crosstalk can occur across the communication channel, causing the received information to be different from the original information sent. So to remove this we need some methods to detect as well as correct errors. This paper presents in a tutorial form a survey of the old and recent, powerful error correcting coding techniques. These techniques ensure receiving system to detect and possibly correct errors caused by corruption from the channel and the receiver by enabling the decoder to correct errors without requesting retransmission of the original information. The usual mathematical approach is bypassed to appeal to wider readers. The operation, proper use, and limitations of error-control codes are described.**

***Keywords* - error correction, error detection, coding theory, types of codes, encoding schemes, ARQ**

I. INTRODUCTION

A transmission channel is the physical medium through which the information is transmitted, such as telephone lines, or atmosphere in the case of wireless communication. Undesirable disturbances (noise) can occur across the communication channel, causing the received information to be different from the original information sent. Coding theory deals with detection and correction of the transmission errors caused by the noise in the channel. The primary goal of coding theory is efficient encoding of information, easy transmission of encoded messages, fast decoding of received information and correction of errors introduced in the channel. Coding Theory is used all the time: in reading CDs, receiving transmissions from satellites, or in cell phones [1]. The key challenge coding theorists face is to construct "good" codes and efficient algorithms for encoding and decoding them. Encoding introduces redundancy into a stream of data, and decoding uses the redundancy to correct errors and extract the original data. This paper will focus on the analysis, design, and applications of the important class of codes.

Error-correcting codes are more sophisticated than error detecting codes and require more redundant bits. The number of bits required correcting multiple bits or burst error is so high that in most of the cases it is inefficient to do so. For this reason, most error correction is limited to one, two or at the most three-bit errors. Different error coding schemes are chosen depending on the types of errors expected, the communication medium's expected error rate, and whether or not data retransmission is possible [2].

In section second and third two basic strategies for dealing with errors are described. One way is to include enough redundant information along with each block of data sent to enable the receiver to deduce what the transmitted character must have been. The other way is to include only enough redundancy to allow the receiver to deduce that error has occurred, but not which error has occurred and the receiver asks for a retransmission. The former strategy uses Error-Correcting Codes and latter uses Error-detecting Codes. Further in section four error control technique ARQ is explained and in section five some forward error correction codes are discussed along with their uses in day to day technology. Finally, in section five we provide summary of various codes and discuss scope of future extensions.

II. ERROR DETECTION SCHEMES

In telecommunication, all error detection codes transmit more bits than were in the original data. Most codes are "systematic" i.e. the transmitter sends a fixed number of original data bits, followed by fixed number of check bits which are derived from the data bits by some deterministic algorithm. The receiver applies the same algorithm to the received data bits and compares its output to the received check bits; if the values do not match, an error has occurred at some point during the transmission. Now we will discuss some error detection codes along with their uses and limitations.

A. *Repetition Codes*

One simplest possible solution to this problem is to repeat the transmission several times so as to increase the probability of receiving the correct message. This is called a repetition code. Perhaps the most popular repetition code is "triple modular redundancy", sending the same message 3 times. Let's say we have a repeated message of 3 bits that is sent 3 times. When it is received, each message is different:

101 001 100

Because we didn't receive exactly the same message all 3 times, we have detected that some errors occurred. We can see that the middle bit is certainly a 0, because it is the same in all messages and first and the last digit are likely to be a 1 because 2 out of 3 of the messages say that these values are 1. The transmitted message then was most likely 101.

The advantage of repetition codes is that they are extremely simple, and are in fact used in some transmissions of numbers stations [3]. Due to the simplicity of the channel encoding and decoding for repetition codes, they find applications in fading channels and non-AWGN environments. Repetition codes are one of the few known codes whose code rate can be automatically adjusted to varying channel capacity, by sending more or less parity information as required to overcome the channel noise.

B. Parity Check Codes

Another error detection scheme is called the parity check or check bit. A parity check is the process of counting the number of ones in a binary sequence. The parity check bit is a bit that is added to make the sequence even or odd. It can be calculated via an XOR sum of the bits, yielding 0 for even parity and 1 for odd parity

If an odd number of bits (including the parity bit) are transmitted incorrectly, the parity bit will be incorrect and thus indicates that an error occurred in transmission. The parity bit is only suitable for detecting errors; it cannot correct any errors, as there is no way to determine which particular bit is corrupted. The data must be discarded entirely, and re-transmitted from scratch [3]. An even number of flipped bits will make the parity bit appear correct even though the data is erroneous. However, parity has the advantage that it uses only a single bit and requires only a number of XOR gates to generate. Extensions and variations on the parity bit mechanism are horizontal redundancy checks, vertical redundancy checks, and "double," "dual," or "diagonal" parity (used in RAID-DP).

C. Checksum

A checksum or hash sum is a fixed size datum computed from an arbitrary block of digital data for the purpose of detecting accidental errors that may have been introduced during its transmission or storage. Check digits and parity are special cases of checksums, appropriate for small blocks of data (such as social Security bank account numbers, social security no., computer words, single bytes, etc.).

The simplest checksum algorithm is the so-called longitudinal parity check, which breaks the data into "words" with a fixed number n of bits, and then computes the exclusive or of all those words. The result is appended to the message as an extra word. To check the integrity of a message, the receiver computes the XOR of all its words, including the checksum; if the result is not a word with n zeros; the receiver knows that a transmission error occurred.

D. Cyclic Redundancy Check (CRC)

Cyclic codes have favorable properties in that they are well suited for detecting burst errors. CRCs are particularly easy to implement in hardware, and are therefore commonly used in digital networks and storage devices such as hard disk drives. A CRC-enabled device calculates a short, fixed-length binary sequence, known as the check value or improperly the CRC, for each block of data to be sent or stored and appends it to the data, forming a codeword. The idea behind CRC calculation is to look at the data as one large binary number. This number is divided by a certain value and the remainder of the calculation is called the CRC. When a codeword is received or read, the device either compares its check value with one freshly calculated from the data block, or equivalently, performs a CRC on the whole codeword and compares the resulting check value with an expected residue constant. If the check values do not match, then the block contains a data error [4] and the device may seize corrective action such as rereading or requesting the block is sent again, otherwise the data is assumed to be error-free. CRCs are so called because the check (data verification) code is a redundancy (adds zero information to the message) and the algorithm is based on cyclic codes. CRCs are popular because they are simple to implement in binary hardware, are easy to analyze mathematically, and are particularly good at detecting common errors caused by noise in transmission channels.

III. ERROR CORRECTION SCHEMES

The techniques that we have discussed so far can detect errors, but do not correct them. Error Correction can be handled in two ways:

A. *Backward Error Correction:* In this scheme, when an error is discovered; the receiver has a back channel to request the sender to retransmit the entire data unit, also known as ARQ.

B. *Forward error correction:* In this, receiver can use an error-correcting code, which automatically corrects certain errors.

Applications that require low latency (such as telephone conversations) cannot use Automatic Repeat request (ARQ) [6]; they must use Forward Error

Correction (FEC). By the time an ARQ system discovers an error and re-transmits it, the re-sent data will arrive too late to be any good. Applications where the transmitter immediately forgets the information as soon as it is sent (such as most television cameras) cannot use ARQ; they must use FEC because when an error occurs, the original data is no longer available [5]. This is also why FEC is used in data storage systems such as RAID and distributed data store.

IV. AUTOMATIC REPEAT REQUEST

Automatic Repeat reQuest (ARQ) is an error control method for data transmission that makes use of error-detection codes, acknowledgment and/or negative acknowledgment messages, and timeouts to achieve reliable data transmission. An acknowledgment is a message sent by the receiver to indicate that it has correctly received a data frame. Usually, when the transmitter does not receive the acknowledgment before the timeout occurs (i.e., within a reasonable amount of time after sending the data frame), it retransmits the frame until it is either correctly received. Three types of ARQ protocols are Stop-and-wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ.

ARQ is appropriate if the communication channel has varying or unknown capacity, such as is the case on the Internet [6]. However, ARQ requires the availability of a back channel, results in possibly increased latency due to retransmissions, and requires the maintenance of buffers and timers for retransmissions, which in the case of network congestion can put a strain on the server and overall network capacity.

V. FORWARD ERROR CORRECTION

An error-correcting code (ECC) or forward error correction (FEC) code is a system of adding redundant data, or parity data, to a message, such that it can be recovered by a receiver even when a number of errors (up to the capability of the code being used) were introduced, either during the process of transmission, or on storage. Since the receiver does not have to ask the sender for retransmission of the data, a back-channel is not required in forward error correction, and it is therefore suitable for simplex communication such as broadcasting. Error-correcting codes are frequently used in lower-layer communication, as well as for reliable storage in media such as CDs, DVDs, hard disks, and RAM.

Error-correcting codes are usually distinguished between convolutional codes and block codes:

- Convolutional codes are processed on a bit-by-bit basis. They are particularly suitable for implementation in hardware, and the Viterbi decoder allows optimal decoding.
- Block codes are processed on a block-by-block basis. They were followed by a number of efficient codes, RS codes [8], Turbo codes [13] and low density parity check code (LDPC) [11] are relatively new constructions that can provide almost optimal efficiency.

Shannon's theorem is an important theorem in forward error correction and describes the maximum information rate at which reliable communication is possible over a channel. This strict upper limit is expressed in terms of the channel capacity. More specifically, the theorem says that there exist codes such that with increasing encoding length the probability of error on a discrete memoryless channel can be made arbitrarily small, provided that the code rate is smaller than the channel capacity.

A. BCH Codes

BCH codes were invented in 1959 by Hocquenghem, and independently in 1960 by Bose and Ray-Chaudhuri. The codewords are formed by taking the remainder after dividing a polynomial representing our info bits by a generator polynomial. The generator polynomial is selected to give the code its characteristics all codewords are multiple of generator polynomial.

The principal advantage of BCH codes is the ease with which they can be decoded, via an elegant algebraic method known as syndrome decoding [7]. This class of codes, is also highly flexible, allowing control over block length and acceptable error thresholds, thus a custom code can be designed to a given specification (subject to mathematical constraints). They have been widely used in communications and data storage systems, including satellite communications, cellular networks, CD Rom, Mass Storage Systems, wireless broadband, etc.

B. Hamming code

In telecommunication, a Hamming code is a linear error-correcting code named after its inventor, Richard Hamming. Hamming codes can detect up to two simultaneous bit errors, and correct single-bit errors; thus, reliable communication is possible when the Hamming distance between the transmitted and received bit patterns is less than or equal to one[8]. This means it is suitable for transmission medium situations where burst errors do not occur. In particular, a single-error-correcting and double-error-detecting variant commonly referred to as SECDED.

TABLE I:
SHOWING WHICH PARITY BITS COVER WHICH TRANSMITTED BITS IN THE ENCODED CODE WORD

Bit#	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Sent Bit	$\mathbf{P_1}$	$\mathbf{P_2}$	$\mathbf{D_1}$	$\mathbf{P_3}$	$\mathbf{D_2}$	$\mathbf{D_3}$	$\mathbf{D_4}$
$\mathbf{P_1}$	Y	N	Y	N	Y	N	Y

P_2	N	Y	Y	N	N	Y	Y
P_3	N	N	N	Y	Y	Y	Y

Hamming Code (7, 4) adds three additional check bits to every four data bits of the message. Consider a message having four data bits which is to be transmitted as a 7-bit codeword by adding three error control bits. This would be called a (7, 4) code. The three bits to be added are three EVEN Parity bits, where the parity of each is computed on different subsets of the message bits as shown above in table 1, eg. , suppose the above message 1100110 is sent and a single bit error occurs such that the codeword 1110110 is received:

Transmitted message Received message
1 1 0 0 1 1 0 ⟹ 1 1 1 0 1 1 0
BIT: 7 6 5 4 3 2 1 BIT: 7 6 5 4 3 2 1

The above error (bit 5) can be corrected by examining which of the three parity bits was affected by the bad bit. Because of the simplicity of Hamming codes, they are widely used in computer memory (RAM).

C. Walsh-Hadamard code

In the field of mathematics, the Walsh-Hadamard code is an error correcting code over a binary alphabet that allows reconstruction of any codeword if less than half its bits are corrupted. Furthermore, the Walsh-Hadamard code is a locally decodable code [9] which provides a way to recover the original message with high probability. This gives rise to applications in complexity theory. It can also be shown that using list decoding; the original message can be recovered as long as less than 1/2 of the bits in the received word have been corrupted. In coding theory, the WH code is an example of a linear code over a binary alphabet that maps messages of length n to codewords of length 2^n. WH codes are mathematically orthogonal codes. As a result, a Walsh-encoded signal appears as random noise to a CDMA capable mobile terminal, unless that terminal uses the same code as the one used to encode the incoming signal. Walsh codes are used in direct sequence spread spectrum (DSSS) systems such as QUALCOMM's CDMA, IS-95 and in frequency hopping spread spectrum (FHSS) systems to select the target frequency for the next hop. Beside this, they are also used in power spectrum analysis, filtering, processing speech and medical signals, multiplexing and coding in communications, characterizing non-linear signals, solving non-linear differential equations, and logical design and analysis.

D. Reed–Solomon Codes

In coding theory, Reed–Solomon (RS) codes are non-binary cyclic error correcting codes invented by Irving S. Reed and Gustave Solomon in 1960. They described a systematic way of building codes that could detect and correct multiple random symbol errors. RS codes work by adding t check symbols to the data, an RS code can detect any combination of up to t erroneous symbols, and correct up to t/2 symbols. The choice of t is up to the designer of the code. RS codes are usually constructed as systematic codes. Instead of sending s(x) = p(x)g(x), the encoder will construct the transmitted polynomial s(x) such that it is evenly divisible by g(x) and p(x) is apparent in the codeword. Ordinarily, the construction is done by multiplying p(x) by x^t to make room for the t check symbols, dividing that product by g(x) to find the remainder, and then compensating for that remainder.

The above properties of RS codes make them especially well-suited to applications where errors occur in bursts [8]. RS codes prominently used in consumer electronics such as CDs, DVDs, Blue-ray Discs, in data transmission technologies such as DSL & WiMAX, in broadcast systems such as DVB and ATSC, and in computer applications such as RAID 6 systems.

E. Low Density Parity Check Code (LDPC)

LDPC codes provide performance very close to the channel capacity (the theoretical maximum) using an iterated soft-decision decoding approach, at linear time complexity in terms of their block length. Practical implementations can draw heavily from the use of parallelism [10].The construction of a specific LDPC code after this optimization falls into two main types of techniques:

a) Pseudo-random approaches
b) Combinatorial approaches

Construction [11] by a pseudo-random approach builds on theoretical results that, for large block size, a random construction gives good decoding performance. In general, pseudo-random codes have complex encoders; however pseudo-random codes with the best decoders can have simple encoders [12].Combinatorial approaches can be used to optimize properties of small block-size LDPC codes or to create codes with simple encoders.

LDPC codes are now used in many recent high-speed communication standards, such as DVB-S2 (Digital video broadcasting), WiMAX, High-Speed Wireless LAN (IEEE 802.11n), 10GBase-T Ethernet (802.3an) and G.hn/G.9960 (ITU-T Standard for networking over power lines, phone lines and coaxial cable). Since 2009, LDPC codes are also part of the Wi-Fi 802.11 standard as an optional part of 802.11n, in the High Throughput (HT) PHY specification.

F. Turbo Codes

Turbo coding is an iterated soft-decoding scheme that combines two or more relatively simple convolutional codes and an interleaver to produce a block code that can perform to within a fraction of a decibel of the Shannon limit. The first turbo code, based on convolutional encoding, was introduced in 1993 by Berrou et al. Predating LDPC codes in terms of practical application, they now provide similar performance. One of the earliest commercial applications of turbo coding was the CDMA2000 1x digital cellular technology specifically for Internet access, 1xEV-DO (TIA IS-856). Turbo codes find their major applications in field of telecommunications [13]:

- Turbo codes are used extensively in 3G and 4G mobile telephony standards e.g. in HSPA, EV-DO and LTE.
- MediaFLO, terrestrial mobile television system from Qualcomm.
- The interaction channel of satellite communication systems, such as DVB-RCS.
- New NASA missions such as Mars Reconnaissance Orbiter now use turbo codes, as an alternative to RS-Viterbi codes.
- Turbo coding such as block turbo coding and convolutional turbo coding are used in IEEE 802.16 (WiMAX), a wireless metropolitan network standard.

Turbo codes are used for pictures, video, and mail transmissions. For voice transmission, however, convolutional codes are used, because the decoding delay, the time it takes to decode the data, is a major drawback to turbo codes. The several iterations required by turbo decoding make the delay unacceptable for real-time voice communications and other applications that require instant data processing, like hard disk storage and optical transmission.

VI. CONCLUSION

A general overview of the various error correction and detection methods is briefed in this paper. Different error coding schemes are chosen depending on the types of errors expected, the communication medium's expected error rate, and whether or not data retransmission is possible. Faster processors and better communications technology make more complex coding schemes, with better error detecting and correcting capabilities, possible for smaller embedded systems, allowing for more robust communications. However, tradeoffs between bandwidth and coding overhead, coding complexity and allowable coding delay between transmissions, must be considered for each application [14].If errors are introduced during transmission, they will likely be detected during the decoding process at the destination because the code word would be transformed into an invalid bit string. It should be noted that although there is no single best technique. Never mind, it does not matter. We can run many techniques in parallel (independently, with no communication overhead) and thus combine strength of different techniques. Combinations of the above techniques, such as FEC with automatic repeat request (ARQ) [14], RS with hamming [8] have also been tried and reported. Though hybrid schemes [2] work better than individual techniques, they still suffer with the basic problem of individual techniques. Consequently, it is possible to run several techniques in parallel.

REFERENCES

[1] Litwin, L. Ramaswamy, K. **"**Error control coding", Potentials, IEEE Vol: 20, pp: 26 – 28, 2001.

[2] Zhen Zhang "Some Recent Progresses in Network Error Correction Coding Theory"; Theory and Applications Network Coding, pp 1-5, 2008.

[3] Wicker, Stephen B. "Error Control Systems for Digital Communication and Storage". Englewood Cliffs NJ: Prentice-Hall.,1995

[4] Code Jun Jin Kong; Parhi, K.K.; "Interleaved cyclic redundancy check (CRC)" IEEE Conference on Signals, Systems and Computers, Vol: 2, Pp: 2137 – 2141, 2003.

[5] Babiker, A.E.; Zakaria, M.N.B "An Efficient Energy two Mode Error Correction technique in Underwater Wireless Sensor Networks" IEEE 2010 International Symposium in Information Technology (ITSim), Vol: 2, Pp: 580 – 585, 2010.

[6] Gonzalez, O.; Kohno, R.; "Performance of a spread slotted CDMA/ALOHA with hybrid ARQ system with variations on the FEC code capabilities" IEEE Vehicular Technology Conference Proceedings, Pp: 2262 - 2266, vol.-3, 2000.

[7] Sarnin, Suzi Seroja; Nairn, Nani Fadzlina; Muhamad, Wan Nor Syafizan W.; "Performance evaluation of phase shift keying modulation technique using BCH code, Cyclic code and Hamming code through AWGN channel model in communication system" ,3rd IEEE International Conference on Information Sciences and Interaction Sciences (ICIS), Page(s): 60 – 65 ,2010 .

[8] Sunwook Rhee;Changgeun Kim; Juhee Kim; Yong Jee; "Concatenated Reed-Solomon Code with Hamming Code for DRAM Controller Second" IEEE International Conference on Computer Eng and Applications (ICCEA),Vol: 1 , Pp: 291-295,2010.

[9] Shaopeng Wang; Shihua Zhu; Guomei Zhang "Walsh-Hadamard coded spectral efficient full frequency diversity OFDM system"; IEEE Transactions on Communications, Vol: 58, pp-28-34,2010.

[10] Djordjevic, I.B.; Lei Xu; Ting Wang; "Multidimensional turbo product and generalized LDPC codes with component RS codes suitable for use in beyond 100 Gb/s optical transmission" 9th IEEE International Conference on Telecommunication in Modern Satellite, Cable, and Broadcasting Services, TELSIKS '09,pp 402 – 405 ,2009.

[11] Honary, B.; Heravi, B.M.; Kariyawasam, S.; Pandya, N.; "Design, implementation and applications of low-complexity LDPC codes", 2nd IEEE International Conference on Signal Processing and Communication Systems, ICSPCS, Pp: 1, 2008.

[12] Li, G.; Fair, I.J.; Krzymien, W.A.; "Low-density parity-check codes for space-time wireless transmission" IEEE Transactions on Wireless Communications, Vol: 5 , Pp 312 – 322,2006.

[13] Gracie, K.; Hamon, M.-H.; "Turbo and Turbo-Like Codes: Principles and Applications" IEEE Proceedings of in Telecommunications Vol: 95, Pp: 1228 – 1254, 2000.

[14] Mitra, S. McCluskey, E.J. "Which Concurrent Error Detection Scheme To Choose" IEEE Proceedings. International Test Conference, pp985 - 994, 2000.