Applications of Information Theory in Communication Engg

Prof. Sumita Chandak¹ Prof. Reena Mahe² Prof. Nileema Pathak³ Prof. Renuka Nagpure⁴ Prof. K Tejaswi⁵
¹,²,³,⁴,⁵Assistant Professor
¹,²,³,⁴,⁵Department of Information Technology
¹,²,³,⁴,⁵Atharva College of Engineering University of Mumbai, India

Abstract— Coding applications have grown rapidly in the past several years with cost-effective performance demonstrated to increase the efficiency and reliability of communication. An overview of the many practical applications of source coding and channel coding theory in the past are presented. The following application areas are included: text compression, audio and video compression, satellite communication, data transmission, data storage, mobile communication, files transfer, and digital audio/video transmission. Although no attempt is made to be comprehensive in our coverage, the examples chosen clearly illustrate the richness, variety, and importance of compression and error-control coding methods in modern digital applications.

Key words: Entropy, Huffman Coding, Arithmetic Coding, DCT, Quantization, JPEG, MPEG, Block Codes, Convolution Codes, Error Control Coding

I. INTRODUCTION

In 1948, Shannon published his paper “A Mathematical Theory of Communication” in the Bell Systems Technical Journal [1]. He has given mathematical model for measuring information and showed how information could be quantified with absolute precision, and demonstrated the essential unity of all information media. Telephone signals, text, radio waves, and pictures, essentially every mode of communication, could be encoded in bits. The paper provided a “blueprint for the digital age” It provides measurable quantities on:

- The amount of information issued by a discrete symbols source to increase the efficiency of communication.
- Maximum amount of information (or information rate) at which reliable communication can take place over a noisy channel.

In this paper applications on two concepts of information theory are discussed i.e source coding and channel coding. Source coding deals with representation of data efficiently. The basic objective of source coding is to remove redundancy in the information to make the message smaller i.e. compression of data. The channel coding is to protect the messages against disturbance of the channel, to make a noisy channel behave like a noiseless channel. The primary objective of coding is that the decoder can determine if the received word is a valid codeword, or if it is a codeword which has been corrupted by noise (i.e. detect one or more errors). Ideally the decoder should be able to decide which codeword was sent even if the transmitted codeword was corrupted by noise (i.e. error correction). Channel encoding inserts redundant bits (or symbols ) sequentially (convolutive codes) or per blocks(block codes) by a coding process designed to make the noisy received signal decodable.

II. SOURCE CODING

The source coding theorem will exhibit the entropy of a source as the fundamental limit in data compression. [1]

\[ H(X) = \sum_{i=0}^{n} p_i \log_2 \frac{1}{p_i} \]  

(1)

For the discrete source, data compression is used for encoding the source output at a smaller rate than the source entropy. And for a continuous source, the entropy is infinite so for encoding scalar and vector quantizes are used which results into lossy compression.

Most famous code is the Morse code. Invented by Samuel Morse in the 1840’s, it allows letters of the alphabet { a, b, … , z, “ space”, “ full stop”, “ comma”, … } to be sent as short electrical signals (dots) and long electrical signals (dashes). A code is said to be uniquely decipherable if any sequence of code word can be interpreted in only one way.

A. Huffman Algorithm [2] [3]:

This algorithm, invented in 1952 by D.A. Huffman, provides a prefix code whose construction can be achieved by a binary tree.

Here are the successive steps: The Huffman encoding algorithm starts by constructing a list of all the alphabet symbols in descending order of their probabilities. It then constructs, from the bottom up, a binary tree with a symbol at every leaf. This is done in steps, where at each step two symbols with the smallest probabilities are selected, added to the top of the partial tree, deleted from the list, and replaced with an auxiliary symbol representing the two original symbols. When the list is reduced to
Applications of Information Theory in Communication Engg

(IJSRD/Conf/NCTAA/2016/037)

just one auxiliary symbol (representing the entire alphabet), the tree is complete. The tree is then traversed to determine the codeword of the symbols.

Huffman coding supports for facsimile recommendations T3 and T4 used to encode run length. For PKZIP, GZIP, WINZIP (multichannel compression including text and other data types), JPEG, PNG, MPEG, MP3, AAC and also used in steganography for JPEG carrier compression.

B. Arithmetic Coding [2] [3]:
Unlike Huffman coding, arithmetic coding does not assign particular bit patterns to the source symbols. Instead, a single arithmetic codeword is assigned to the complete sequence of symbols. Arithmetic codewords consist of sub-intervals of the unit interval [0, 1). They are specified with sufficient bits to differentiate each sub-interval corresponding to a source symbol from other possible sub-intervals. Shorter codes are assigned to larger sub-intervals or more probable symbols. As the coding proceeds, the sub-intervals are refined, and bits are output as they are determined.

Supports to general purpose applications like PPM, PAQ, DjVu. For image JPEG2000, JBIG, MPEG For teleconferencing SKFYPE, FLASH Arithmetic coding is used.

C. LZW Algorithm [2] [3]:

Before starting the algorithm, the dictionary contains all the strings of length one.

As soon as the juxtaposition P + c are not in the dictionary, only the address of P is transmitted. Then, the string P + c are added to the dictionary and the character c is used to initialise the next string.

LZ77 supports PNG, GZIP

LZW supports GIF, V.42, and UNIX file compression

To compare the performances of some codes, the compression rates have been calculated after applying different algorithms to the same 6MB set of files divided into three parts:

- Text files
- Binary files
- Graphic files

Compression rate =1- size of the original file/ size of the compressed file

These files have been extracted from Dr Dobb’s journal February 1991 (source Mark Nelson).

<table>
<thead>
<tr>
<th>codes</th>
<th>graphic</th>
<th>binary</th>
<th>text</th>
<th>on average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Huffman</td>
<td>27.22%</td>
<td>24.79%</td>
<td>46.38%</td>
<td>31.04%</td>
</tr>
<tr>
<td>adaptive</td>
<td>32.59%</td>
<td>26.69%</td>
<td>40.72%</td>
<td>33.27%</td>
</tr>
<tr>
<td>Huffman</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LZW (fixed 12 bits)</td>
<td>20.61%</td>
<td>15.07%</td>
<td>50.32%</td>
<td>29.20%</td>
</tr>
<tr>
<td>LZW (variable 12 bits)</td>
<td>46.78%</td>
<td>36.61%</td>
<td>54.82%</td>
<td>45.81%</td>
</tr>
<tr>
<td>LZW (variable 15 bits)</td>
<td>48.44%</td>
<td>36.15%</td>
<td>58.28%</td>
<td>47.31%</td>
</tr>
</tbody>
</table>

Table 1: comparison of various coding technique

D. RLE- Run Length Encoding [2] [3]:
Repeated occurrence of the same character is called a run. Number of repetition is called the length of the run. Run of any length is represented by two characters

Ex: eeeeeettttttttt

Run length code- e71n8

It is supported by ITU-T T4 standard for facsimile, and also for Tiff, BMP, PCX, JPEG etc.

E. Image/Video Compression:

Intra frame coding and inter frame coding are two important concepts involved in video coding. Intra frame coding refers to the exploitation of redundancies within each individual frame in a sequence, or in effect coding still images. This effectively means exploiting the spatial correlations. On the other hand, inter frame coding is the process of eliminating the temporal redundancies, i.e the similarities between the successive frames. Three fundamental approaches are usually taken to accomplish this goal:

- Spatial redundancy reduction, exploiting the correlations of similar pixels within a frame e.g. DCT.
- Temporal redundancy reduction, exploiting the similarities between successive frames.
- Entropy coding, for reducing redundancies between compressed data symbols e.g. Huffman coding

1) Discrete Cosine Transform [2]:

In general, neighboring pixels within an image tend to be highly correlated. As such, it is desired to use a transform to concentrate randomness into fewer, decorrelated parameters. The Discrete Cosine Transform (DCT) has been shown to be near optimal for a large class of images in energy concentration and decorrelation. The DCT decomposes the signal into underlying
Applications of Information Theory in Communication Engg
(IJSRD/Conf/NCTAA/2016/037)

spatial frequencies, which then allow further processing techniques to reduce the precision of the DCT coefficients consistent with the Human Visual System (HVS) model.

The DCT transforms the data from the spatial domain to the frequency domain. The spatial domain shows the amplitude of the color as you move through space. The frequency domain shows how quickly the amplitude of the color is changing from one pixel to the next in an image file.

\[
S_{uv} = \frac{1}{4} C_u C_v \sum_{i=0}^{7} \sum_{j=0}^{7} S_{ij} \cos \left(\frac{(2i+1)\mu\pi}{16}\right) \cos \left(\frac{(2j+1)\nu\pi}{16}\right)
\]

2) Quantization [2]:
However due to the nature of most of the images, maximum energy (information) lies in low frequency as opposed to the high frequency. We can represent the high frequency components coarsely, or drop them altogether, without strongly affecting the quality of the resulting image reconstruction. This leads to a lot of compression (lossy).

3) Basic JPEG Algorithm [2] [5]:

“JPEG” stands for Joint Photographic Experts Group was approved in September 1992 as ITU-T Recommendation T.81. The source image is divided into 8x8 pixel input blocks. On each 8 x 8 block apply DCT results 64 elements in matrix form. The top left-hand corner is called the “DC” coefficient and the remaining 63 the “AC” coefficients. The “DC” coefficient is a measure of the average value of the 64 pixels of the input block. On DCT coefficients apply quantization matrix. Read quantization coefficients in a sequence using zigzag scanning. Apply run length coding and DPCM coding. Finally coefficients are converted into bit stream using Entropy coding technique.

Fig. 1: basic JPEG algorithm

JPEG standards are JPEG-LS, JPEG2000, and JPEG-XR etc for various image applications.

4) JBIG [2] [3]:
The JBIG image compression standard for bi-level images provides the user with the option of either sequential encoding, progressive encoding, or in between them. In sequential mode the pixels in the image are encoded and decoded in raster scan order and in the progressive mode image is first decomposed into images of varying resolution. According user request particular resolution image is available. JBIG2 standard is for document storage, archiving, wireless transmission, print spooling and coding images on web.

F. MPEG [2] [4]
The MPEG standards are an evolving set of standards for video and audio compression and for multimedia delivery developed by the Moving Picture Experts Group. There are many different redundancies present in the video signal data.

Such as spatial, Temporal, Psycho visual, Coding. Spatial redundancy occurs because neighboring pixels in each individual frame of a video signal are related. The pixels in consecutive frames of signal are also related, leading to temporal redundancy. The human visual system does not treat all the visual information with equal sensitivity, leading to psycho visual redundancy. Finally, not all parameters occur with the same probability in an image. As a result, they would not require equal number of bits to code them.

- MPEG-1 was designed for coding progressive video at a transmission rate of about 1.5 million bits per second. It was designed specifically for Video-CD and CD-i media. MPEG-1 audio layer-3 (MP3) has also evolved from early MPEG work.
- MPEG-2 was designed for coding interlaced images at transmission rates above 4 million bits per second. MPEG-2 is used for digital TV broadcast and DVD. An MPEG-2 player can handle MPEG-1 data as well.
- A proposed MPEG-3 standard, intended for High Definition TV (HDTV), was merged with the MPEG-2 standard when it became apparent that the MPEG-2 standard met the HDTV requirements.
MPEG-4 is a much more ambitious standard and addresses speech and video synthesis, fractal geometry, computer visualization, and an artificial intelligence (AI) approach to reconstructing images. MPEG-4 addresses a standard way for authors to create and define the media objects in a multimedia presentation, how these can be synchronized and related to each other in transmission, and how users are to be able to interact with the media objects.

III. CHANNEL CODING

Channel coding [6] deals with error control techniques. If the data at the output of a communications system has errors that are too frequent for the desired use, the errors can often be reduced by the use of a number of techniques. Coding permits an increased rate of information transfer at a fixed error rate, or a reduced error rate for a fixed transfer rate.

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.

The two main methods of error control are:
- Automatic Repeat Request (ARQ) when a receiver circuit detects errors in a block of data, it requests that the data is retransmitted.
- Forward Error Correction (FEC) the transmitted data is encoded so that the data can correct as well as detect errors caused by channel noise.

The choice of ARQ or FEC depends on the particular application. ARQ is often used where there is a full duplex (2-way) channel because it is relatively inexpensive to implement. FEC is used where the channel is not full duplex or where ARQ is not desirable because real time is required.

![Fig. 2: forward error codes tree](image)

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.

The two main categories of channel codes are:

A. **Block Codes:**

A block of \( k \) information bits is encoded to give a codeword of \( n \) bits (\( n > k \)). For each sequence of \( k \) information bits, there is a distinct codeword of \( n \) bits. Examples of block codes include Hamming Codes, RS Codes, BCH codes, Cyclic Codes and LDPC Codes. A Cyclic Redundancy Check (CRC) code can detect any error burst up to the length of the CRC code itself.

B. **LBC Codes:**

All the codewords can be obtained as linear combination of basis vectors designate as \( G \). \( G \) is a matrix consisting of \( k \) rows and \( n \) column. Since an \((n, k)\) linear block code has \(2^k\) valid codewords, it is a subspace of dimension \( k \). Consequently, the row of \( G \) must be linearly independent, i.e. they must be the basis for the \((n, k)\) code.

\[
G = \begin{bmatrix}
g_1 \\
g_2 \\
\vdots \\
g_k \\
\end{bmatrix} = \begin{bmatrix}
g_{11} & g_{12} & \cdots & g_{1m} \\
g_{21} & g_{22} & \cdots & g_{2m} \\
\vdots & \vdots & \ddots & \vdots \\
g_{k1} & g_{k2} & \cdots & g_{km} \\
\end{bmatrix}
\]

(4)

A linear block code is said to be a systematic code if the first \( k \) bits of the code words are the data bits and the following \( n - k \) bits are the parity check bits. Any generator matrix \( G \) can be reduced by row operations to the systematic form.
Where \( m \) is message, \( I \) is identity matrix, \( P \) are parity check bits and \( C \) is codeword.

At the receiver, the decoding operation of a linear block code involves a parity check matrix \( H \) that is used to detect and possibly correct bit errors.

\[
H = [P^T b_{-k}] 
\]

We denote the received data block as \( r \) and \( e \) as error vector is equal to

\[
r = c \oplus e \quad \text{and} \quad S = eH'
\]

\( S \) is known as the syndrome of the error pattern. The parity check results in \( S = 0 \) when no error detected, which is equivalent to \( e = 0 \). When errors are detected, \( S \) is nonzero and indicates the positions of the error bits. Hence the error bits can be corrected. In the cases of the number of errors exceeding the error correcting capacity of the code but within the detection capability, the syndrome indicates uncorrectable errors. There exist some rare error patterns that the syndrome reports no error.

**C. Convolutional Codes:**
The coded sequence of \( n \) bits depends not only on the present \( k \) information bits but also on the previous information bits. Turbo codes are relatively new constructions that can provide almost optimal efficiency.

**D. Convolution codes:**
Convolutional encoding of data is accomplished using a shift register and associated combinatorial logic that performs modulo-two addition. A convolutional code with constraint length \( N \) consists of an \( N \)-stage shift register (SR) and \( \nu \) modulo-2 adders.

\[
\text{Fig. 3: convolution coder with rate } \frac{1}{2} 
\]

Above figure 3 show convolutional coder with \( k =1, n = 2, (2, 1) \) Rate-1/2. Two-stage register (M=2). Each input bit influences the output for 3 intervals (K=3) where \( K = \text{constraint length of the code} = M + 1 \)

A convolutional code may be defined by a set of \( n \) generating polynomials for each input bit. For the circuit under consideration:

\[
g_1(D) = 1 + D + D^2 \quad \text{and} \quad g_2(D) = 1 + D^2
\]

The set \( \{g_i(D)\} \) defines the code completely. The length of the shift register is equal to the highest-degree generator polynomial.

**E. State Diagram Representation**
The output depends on the current input and the state of the encoder (i.e. the contents of the shift register).

\[
\text{Fig. 4: state diagram of convolution coder } \frac{1}{2} 
\]

**F. Trellis Diagram Representation**
It is expansion of state diagram in time.
G. Decoding

A message \( m \) is encoded into the code sequence \( c \). Each code sequence represents a path in the trellis diagram. According to Minimum Distance Decoding (MDD) after receiving the received sequence \( r \), search for the path that is closest (in Hamming distance) to \( r \). Popular algorithm for MDD is viterbi algorithm.

H. The Viterbi Algorithm

- Walk through the trellis and compute the Hamming distance between that branch of \( r \) and those in the trellis.
- At each level, consider the two paths entering the same node and are identical from this node onwards. From these two paths, the one that is closer to \( r \) at this stage will still be so at any time in the future. This path is retained, and the other path is discarded.
- Proceeding this way, at each stage one path will be saved for each node. These paths are called the survivors. The decoded sequence (based on MDD) is guaranteed to be one of these survivors.
- Each survivor is associated with a metric of the accumulated Hamming distance (the Hamming distance up to this stage).
- Carry out this process until the received sequence is considered completely. Choose the survivor with the smallest metric.

I. 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.

J. 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. Because of the simplicity of Hamming codes, they are widely used in computer memory (RAM).

K. 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] [14] which provide 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 Walshencoded 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.
L. Reed–Solomon Codes

In coding theory, Reed–Solomon (RS) codes are nonbinary 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 \( \frac{t}{2} \) symbols. RS codes especially well-suited to applications where errors occur in bursts [8][14]. 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.

M. Low Density Parity Check Code (LDPC)

LDPC [10][11] codes perform delivery 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:
- Pseudo-random approaches
- Combinatorial approaches

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.

N. Turbo Codes

Turbo coding [11][14] 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 earliest commercial applications of turbo coding were 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 realtime voice communications and other applications that require instant data processing, like hard disk storage and optical transmission.

IV. CONCLUSION

Information theory was created to find practical ways to make better, more efficient codes and find the limits on how fast computers could process digital signals. Every piece of digital information is the result of codes that have been examined and improved using Shannon's equation. It has provided the mathematical underpinning for increased data storage, compression and communication like Zip files, MP3s, JPEGs, internet, WiMAX, DVB etc. could not exist without it. And none of those high-definition videos online would have been possible without Shannon's mathematics. A general overview of the various compression and error control coding methods are briefed in this paper.

REFERENCES

[4] Hsin-Hui Chen, “Video Compression Tutorial”, Graduate Institute of Communication Engineering, National Taiwan University, Taipei, Taiwan, ROC.


