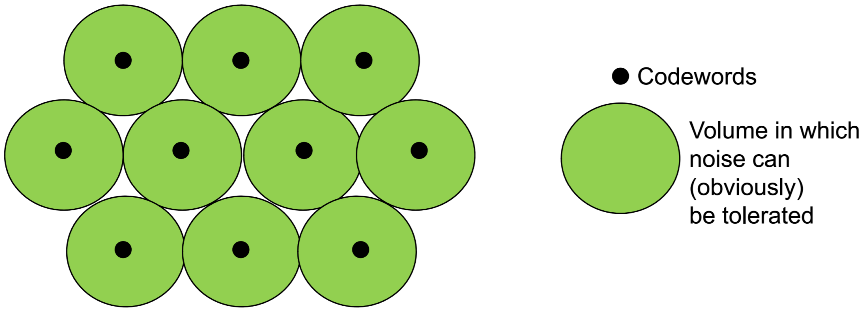
Error Correcting Codes - A Short Survey

Sanjeev Narayanan

April 10th, 2018

Introduction

The idea of redundant information is a well known phenomenon in reading a newspaper. Misspellings go usually unnoticed for a casual reader, while the meaning is still grasped. The art and science of deleting redundant information in a clever way such that it can be stored in less memory or space and still can be expanded to the original message, is called data compression or source coding [1].The idea in error-correcting codes is the converse. One adds redundant information in such a way that it is possible to detect or even correct errors after transmission [2]. This survey gives a brief overview on the principal elements studied or found quite often in an Error Correcting Code textbook.



An error correcting code selects a subset of the space to use as valid messages (codewords). Since the number of valid messages is smaller than the total number of possible messages, we have given up some communication rate in exchange for robustness. The size of each ball above gives approximately the amount of redundancy. The larger the ball (the more redundancy), the smaller the number of valid messages

Figure 1: Visualization of Error Correcting Codes

Block Codes

Adding a parity check such that the number of ones is even, is a well-known way to detect one error. But this does not correct the error. Error-correcting codes are used to reliably transmit digital data over unreliable communication channels subject to channel noise. When a sender wants to transmit a possibly very long data stream using a block code, the sender breaks the stream up into pieces of some fixed size. Each such piece is called message and the procedure given by the block code encodes each message individually into a codeword, also called a block in the context of block codes. The sender then transmits all blocks to the receiver, who can in turn use some decoding mechanism to (hopefully) recover the original messages from the possibly corrupted received blocks. The performance and success of the overall transmission depends on the parameters of the channel and the block code [1]. Formally, a block code is an injective mapping. The block length **n** of a block code is the number of symbols in a block. The rate of a block code is defined as the ratio between its message length and its block length. A large rate means that the amount of actual message per transmitted block is high. The distance or minimum distance d of a block code is the minimum number of positions in which any two distinct codewords differ. Examples of block codes are Reed–Solomon codes, Hamming codes, Hadamard codes, Expander codes, Golay codes, and Reed–Muller codes. These examples also belong to the class of linear codes, and hence they are called linear block codes. More particularly, these codes are known as algebraic block codes, or cyclic block codes, because they can be generated using boolean polynomials. Algebraic block codes are typically hard-decoded using algebraic decoders.

Linear Codes

Linear codes are used in forward error correction and are applied in methods for transmitting symbols (e.g., bits) on a communications channel so that, if errors occur in the communication, some errors can be corrected or detected by the recipient of a message block. The codewords in a linear block code are blocks of symbols that are encoded using more symbols than the original value to be sent. For example, the [7,4,3] Hamming code is a linear binary code which represents 4-bit messages using 7-bit codewords. Two distinct codewords differ in at least three bits. As a consequence, up to two errors per codeword can be detected while a single error can be corrected [3].

Low Density Parity Checking Codes

Low-density parity-check (LDPC) codes are a class of linear block codes. The name comes from the characteristic of their parity-check matrix which contains only a few 1's in comparison to the amount of 0's. Their main advantage is that they provide a performance which is very close to the capacity for a lot of different channels and linear time complex

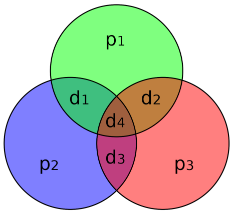


Figure 2: Hamming code - Graphical Representation

algorithms for decoding. Furthermore are they suited for implementations that make heavy use of parallelism [4].

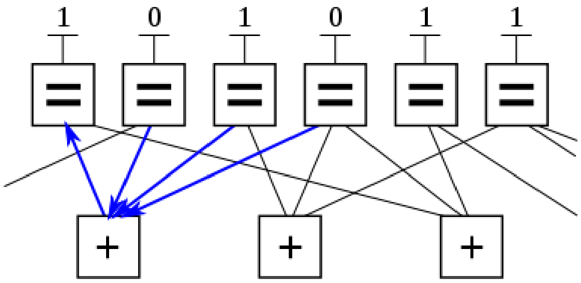


Figure 3: Graph fragment of an example LDPC code using Forney's factor graph notation

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. They described a systematic way of building codes that could detect and correct multiple random symbol errors. By adding t check symbols to the data. An RS code can detect any combination of up to t erroneous symbols, or correct up to $t/2$ symbols [5].

Cyclic Codes

Cyclic codes form an important subclass of linear codes [6]. These codes are attractive for two reasons -

1. Encoding and syndrome computation can be implemented easily by employing shift registers with feedback connections (or linear sequential circuits).
2. They have considerable inherent algebraic structure, and hence, it is possible to find various practical methods for decoding them.

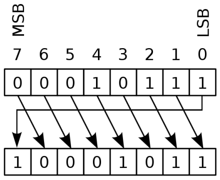


Figure 4: If 00010111 is a valid codeword, applying a right circular shift gives the string 10001011. If the code is cyclic, then 10001011 is again a valid codeword.

References

[1] Ruud Pellikaan, Xin-Wen Wu, Stanislav Bulygin, and Relinde Jurrius. Error-correcting codes. *preprint available at http://www. win. tue. nl/ruudp/courses/2WC09/2WC09-book. pdf*, 2015.

[2] William Wesley Peterson and Edward J Weldon. *Error-correcting codes.* MIT press, 1972.

[3] Aleksander Lodwich. Understanding error correction and its role as part of the communication channel in environments composed of self-integrating systems. *arXiv preprint arXiv:1612.07294*, 2016.

[4] M Pramodh kumarP and S Murali mohanP. Serial one-step majority logic decoder for eg-ldpc code.

[5] Manika Pandey and Vimal Kant Pandey. Comparative performance analysis of block and convolution codes. *International Journal of Computer Applications*, 119(24), 2015.

[6] V Pushpa, H Ranganathan, and M Palanivelan. Ber analysis of bpsk for block codes and convolution codes over awgn channel.