http://ijea.jctjournals.com/ ISSN(ONLINE):2320 – 0804

Volume-10, Issue-11, November, 2021
International Journal of Engineering Associates (IJEA)
Page Number: 01-06

A BIRD EYEVIEW ON VARIOUS GOLAY ENCODER DECODER AND GALOIS FIELD

Anil Dixit [1], Mr. Santosh Onkar [2]
[1]Research Scholar of of VLSI Design, [2]Assistant Professor
[1,2]Department of Electronics & Communication Engineering
[1,2]SAM College of Engineering & Technology, Bhopal (M.P), India
[1]anildixit534@gmail.com

***Abstract*— In The current world of digital communication secure data communication prime task. Data coding decoding explore a variety of applications of the theory of arithmetic and computation. In the fields of cryptography and cryptanalysis as well as in the field of digital communication. For the improvement of security of the codes using the Galious field (G.F.). Computation over finite fields (also called Galois fields) is an active area of research in number theory and algebra, and finds many applications in cryptography, error control coding and combination design. In this survey paper shows the literature review of golay code in digital communication. A bird eye review for Golay code is presented in this research work. A Golay code is presented addressing the error correcting phenomena. This is used in field programmable gate array (FPGA). There are various researchers presents there techniques for correcting the error check. This research work reviews that work.**

Keywords*— Field Programmable Gate Array (FPGA), Binary Code, Digital Communications, Gaussian White Noise Simulation (AWGN) etc.

I. INTRODUCTION

The Golay code was presented in [1] to address error correcting phenomena. The binary Golay code (G23) is represented as (23, 12, 7), while the extended binary Golay code (G24) is as (24, 12, 8). The extended Golay code has been used extensively in deep space network of JPL-NASA as well as in the Voyager

imaging system. In addition, Golay code plays a vital role in different applications like coded excitation for a laser and ultrasound imaging due to the complete sidelobe nullification property of complementary Golay pair. All these applications need generation of Golay sequence, which is fed as trigger to the laser modules. However, for generating Golay code an automatic pattern generator is used, which is of very high cost. To combat this problem, a hardware module programmed to yield a Golay encoded codeword may be used. Golay decoder is used extensively in communication links for forward error correction. Therefore, a high speed and high throughput hardware for decoder could be useful in communication links for forward error correction. Literature surveys were conducted, which deal with encoding methods for Golay code, but these are not suitable for hardware implementation due to complexity of the algorithms. Weng and Lee invented an encoding method for Golay code comprising of a linear feedback shift register (LFSR), an overall parity bit generator, a clock doubles, a five bit counter, and some switching logic. Conventionally, LFSR-based cyclic redundancy check (CRC) generation scheme is preferred for hardware implementation of encoding process, but it has several drawbacks like high latency and less throughput, hence making it unsuitable for high-speed applications.

Over the years, many decoding techniques [12]–[14],[17]–[19], [21], [22] for Golay code have been presented. Based on these algorithms several hardware architectures [10], [15], [16], [20], [23], [24] have been proposed for decoder. Most recently, Alimohammad and Fard implemented a novel architecture for Golay decoder based on imperfect maximum likelihood Manuscript received October 21, 2013; revised May 10, 2014; accepted July 16, 2014. The authors are with the Department of Electronics and Electrical Communication Engineering, IIT Kharagpur, Kharagpur 721302, Digital Object Identifier 10.1109/TVLSI.2014.2346712 decoding (IMLD) scheme, which is also considered in this brief for designing hardware. The rest of this brief is organized as follows. Section II gives an introduction on Golay code, encoding, and decoding schemes. The proposed algorithm, architecture for encoding Golay code and the hardware implementation results have

been illustrated in Section III, while Section IV depicts the proposed hardware architecture for implementing decoder using IMLD algorithm and the results of hardware implementation of proposed decoder module. Finally, conclusions are drawn in Section V.

A number of hard-decision algebraic decoding algorithms have been investigated over the years (see *e.g.*). In contrast to hard-decision decoders which operate on binary values, soft-decision decoders directly process unquantized (or quantized on more than two levels in practice) samples at the output of the matched filter, thereby avoiding the loss of information. Over the Additive White Gaussian Noise (AWGN) channel, soft-decision decoding may offer up to 3 dB coding gain over hard-decision decoding, but at the cost of increased computational complexity. Soft-decision decoding algorithms for the extended Golay code have also received a lot of attention (see [6] and references therein, or [7][8] for more recent results). Yet very few decoder architectures have been published ([6] is a notable exception). This paper addresses the challenging issue of designing a low-complexity (less than 5,000 gates) soft-decision decoder architecture with near-optimal performance for the (24,12,8) code.

II. LITERATURE SURVEY

Sarangi, S., & Banerjee, S. (2014))- This brief describes a coding scheme based on the verification of cyclic redundancy and presents an efficient implementation of the encoding algorithm in the field programmable gate array (FPGA) prototype for both the Golay (G_{23}) and The extended Golay binary code (G_{24}). High-speed, low-latency architecture was designed and implemented in Virtex-4 FPGA for the Golay encoder without incorporating a linear shift register. This memory also presents an optimized and low complexity decoding architecture for the extended binary Golay code (24, 12, 8) based on an incomplete maximum likelihood decoding scheme. The architecture proposed for the decoder occupies less area and has lower latency than some of the recent works published in this field. The encoder module operates at 238.575 MHz, while the proposed architecture for the decoder has an operating clock frequency of 195.028 MHz. The proposed hardware modules can be a good candidate for direct error correction in the communication link, which requires a high speed system. An efficient hardware architecture for the binary Golay encoder and the extended binary Golay encoder were designed and implemented after verifying the proposed algorithm. The results obtained from the simulation indicate that the hardware architecture proposed for the encoder replaces the conventional CRF generation systems based on LFSR. Similarly, the hardware module proposed for the decoder shows better performance in some of the recent publications, taking into account various performance measures. These hardware modules for encoder and decoder can be a good candidate for various applications in high speed communication links, photo spectroscopy and ultrasound. **[01]**

Alimohammad, A., & Fard, S. F. (2013) - This article presents the validation of the performances of the digital baseband communication systems (BER) on a field-programmable gate array (FPGA). The proposed BER tester integrates fundamental baseband signal processing modules from a conventional wireless communication system with a realistic fading channel simulator and a precise Gaussian noise generator on a single FPGA to provide a test environment Accelerated and repetitive in the laboratory. Using a developed graphical user interface, the error rate performance of single antenna and multi-antenna systems over a wide range of parameters can be quickly assessed. The BERT based on FPGA should reduce the need for time-consuming software simulations, thus increasing productivity. This FPGA-based solution is significantly more cost-effective than conventional performance measurements using expensive commercially available test equipment and channel simulators. Accelerated hardware validation is essential to accelerate the characterization of high-intensity, rapidly evolving wireless communication systems.**[02]**

Adde, P., & Le Bidan, R. (2012, December - The extended binary Golay code (24, 12, 8) is a well-known short linear block frequency error correction code with remarkable properties. This research work studies the design of a low decision decoding architecture for this code. A dedicated algorithm is introduced which takes advantage of the properties of the code to simplify the decoding process. The results of the simulation show that the proposed algorithm achieves a performance close to the maximum likelihood with a low computational cost. The architecture of the decoder is described and the results of the VLSI synthesis are presented. The soft-resolution decoding of the Golay codes has been studied and the architecture of the decoder has been described. The proposed approach relies on a dedicated decoding algorithm which exploits the properties of the code to obtain a performance close to the ML using a small number of error patterns. The simulation results and the hardware complexity of the prototype demonstrate the practicality and advantages of the proposed decoding algorithm.**[03]**

Adde, P., Toro, D. G., & Jego, C. (2012) - The maximum likelihood decoding of the linear block codes is

dealt with in this correspondence. A new algorithm based on the Chase-2 algorithm for the decoding of the codes of systematic binary blocks is detailed. A technique of double re-encoding in place of the classical algebraic decoding for the calculation of the list of candidate codewords is the main innovation of the proposed algorithm. This approach has been successfully applied to systematic block codes which have a code rate equal to 1/2 and a parity check matrix composed of a reversible submatrix for the redundancy part. The results of the simulation show a performance close to optimal maximal likelihood decoding for an excellent compromise between BER performance and computational complexity. Next, the problem of designing a decoder for a specific family of short codes of binary blocks, called Cortex codes, is also described. Three soft decoders for Cortex codes with a length of 32, 64 and 128 and a code equal to 1/2 have been designed. Next, all the decoders were successively implemented on a Field Programmable Circuit (FPGA) device. It shows that Cortex codes are a promising solution for digital communication standards requiring short FEC codes. **[04]**

Lin, T. C., Shih, P. Y., Su, W. K., & Truong, T. K. (2009, September) - In this research work, a new soft decision decoder of Golay extended binary code (24, 12, 8) is proposed up to six errors. First, by using the error pattern obtained from the hard decoder, the method of determining possible error patterns is developed. The emblematic probability value of each error pattern is then defined as the product of the individual bit error probabilities corresponding to the locations of the possible error patterns. The most probable of these error models is obtained by choosing the maximum of the emblematic probability values of the possible error patterns. Finally, the results of the Gaussian white noise simulation (AWGN) indicate that this decoder reduces the complexity of the decoding although it achieves a slight loss of coding gain than the modified algorithm of Chase II proposed by Hackett. The proposed modulated decision decoder for Golay code (24, 12, 8) reduces 30% of the decoding complexity in terms of CPU time with respect to the modified Chase II algorithm proposed by Hackett. It is known that Chase decoder II for this code can correct less than or equal to seven errors. Although the proposed decoder corrects the error patterns with a weight less than or equal to six, it achieves only a slight loss of coding gain.**[05]**

Huang, Y. W., & Li, Y. (2010) - A construction of 802.16e compatible uplink sounding sequences is proposed. Ideally, probe signals should have a low peak-to-peak power ratio (PAPR) and low cross-correlation. Existing probing sequences 802.16e are variations of the perforated subsequences of a Golay BPSK sequence with PAPR that may exceed 7dB. The proposed sequences are variations of Golay QPSK sequences that maintain a maximum PAPR of 3 dB and low cross correlation for various multiplexing options in all FFT sizes with full band probe. The proposed modulated decision decoder for Golay code (24, 12, 8) reduces 30% of the decoding complexity in terms of CPU time with respect to the modified Chase II algorithm proposed by Hackett. It is known that Chase decoder II for this code can correct less than or equal to seven errors. Although the proposed decoder corrects the error patterns with a weight less than or equal to six, it achieves only a slight loss of coding gain. It is expected that an extension of the idea proposed in this document will further improve performance.**[06]**

Su, S. Y., & Li, P. C. (2010, October - Photoacoustic imaging (AP) has the potential to image soft tissue with high contrast and high spatial resolution. Conventionally, a Q-switching Nd: YAG laser providing ns pulse duration and pulse energy mJ is suitable for PA applications. However, such a laser is typically cumbersome and expensive. On the other hand, a small diode laser with a low relative cost is potentially useful for performing PA imaging because it provides a PRF up to kHz, but the pulse energy of such a laser is generally too low for one Generation of effective PA. In this study, we proposed an excitation encoded by Golay using a diode laser to generate a PA signal. A high frequency 20 MHz PA transducer integrated into an optical fiber has been proposed to allow retrograde ultrasound and PA detection. The signal-to-noise ratio (SNR) of the generated PA signals of different Golay code lengths (i.e., 2, 4, 16 and 256 bits) was evaluated and pulse durations 25, 50, 100 and 200 ns). The results show that the SNR increases with the length of the code and reaches 30.8 to 37.0 dB of 256 bit code length with different pulse durations. In addition, SNR improvement has also been demonstrated.**[07]**

III. ENCODING THE (24,12,8) GOLAY CODE

The The binary (23,12,7) Golay code can be described in cyclic form as a quadratic residue code with generator polynomial g(x)=x11+ x9+ x7+ x6+ x5+ x+1 [4]. Thus a 11-stage shift-register followed by an accumulator can be used to perform systematic encoding of the (24,12,8) extended Golay code in 24 clock periods. Another approach directly implements with logic gates the product of the binary data vector d with the generator matrix G of the code.

Since the extended Golay code is a self-dual code, the generator matrix Gd in canonical form can be written as

$$Gd = [I12, P]$$

where I12 is the 12 12 identity matrix corresponding to the 12 information bits d, and where P is a 12 12 invertible binary matrix that generates the 12 paritycheck bits p. The corresponding codeword c then reads c = (d, p). From the self-dual property of the extended Golay code, P satisfies the property P-1 = Pt. Thus, in just the same way that the 12 information coordinate d are used to compute the parity bits p using the generator matrix Gs=[I12, P], the 12 parity. coordinates p may also be encoded using the alternative generator matrix Gp = P-1 Gd = [Pt, I12] to obtain the information vector d. A third method uses the Cortex construction. Cortex codes are a family of rate-1/2 self-dual linear block codes first introduced. As shown in Fig. 1, they combine a very short mother code *E* with a sequence of permutations to produce the parity bits. If the mother code is self-dual, the resulting Cortex code inherits from the self-dual property.

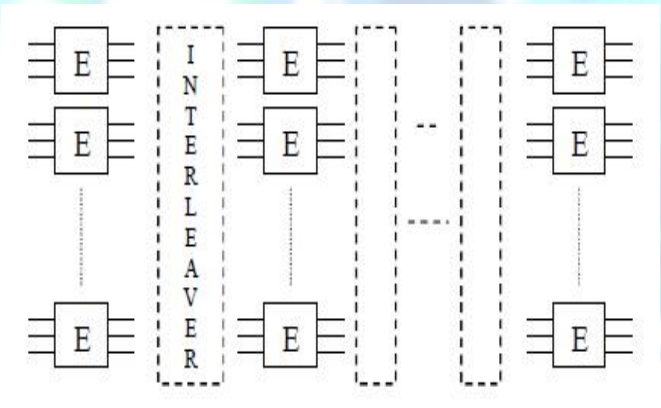

Fig.1: General Cortex encoding scheme build from elementary code E

The Cortex structure corresponding to the extended Golay code is shown in Fig. 2. It is based on the (8,4,4) extended Hamming code (denoted H). The 12 information bits d are divided into 3 blocks of 4 bits. Each block is encoded by the (8,4,4) code to produce 4 parity bits (systematic bits are discarded). The sequence of 12 parity bits is then shuffled by a suitable permutation function, and the whole process is repeated 3 times in order to generate the parity bits p. The codeword is finally obtained by concatenating the 12 systematic bits d with the 12 final parity bits p. Interestingly, the (8,4,4) extended Hamming code used as a building block for obtaining the extended Golay code in Cortex form may also be described as a Cortex code.

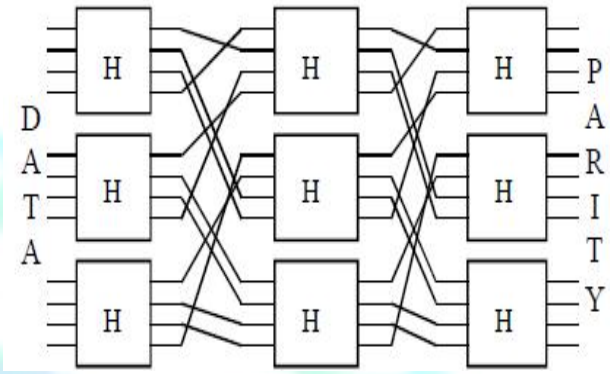

Fig.2: Cortex Architecture for the extended Golay Code

IV. SOFT-DECISION DECODER ARCHITECTURE

In In spite of its short block length, designing lowcomplexity soft-decision decoding architectures for the Golay code that are amenable to very high data rate remains a challenging issue. Here, we describe a digital implementation tailored to the soft-decision decoding algorithm investigated in the previous Section. The decoder operates on soft inputs quantized on q=3 bits (+ sign bit). A total of $VT = VTs+VTp$ = 24+24 = 48 candidate codewords is used to generate the decoder decision. The 2 24 error patterns are chosen so as to correct the most likely errors located in the $Lrs = Lrp$ = 5 least reliable positions in both the information and parity parts of the received vector. The corresponding architecture is inspired and is shown in Fig. 6. It consists of four main blocks: reception, processing, transmission and control. Inside the reception block, the n=24 soft symbols of the received word are processed sequentially. This block first identifies successively the *Lrs* and *Lrp* least reliable positions within the systematic and parity parts of the received word, respectively. In parallel, a serial-in parallel-out (SIPO) shift-register memorizes sequentially the 24 soft samples of the received word. The processing block comprises three main tasks. First, error patterns are generated from the sign bits of the received word by testing different combinations of 0s and 1s in the least reliable bit positions. Then, these error patterns are added (modulo-2) to the information/parity sequence and the resulting sequence is re-encoded to produce a codeword which is scored (correlation metric). Finally, a selection function (comparator) identifies the most likely codeword within the input list of 48 candidate codewords. Note that this process is realized in parallel for the information and the

parity parts of the received word. Moreover, the metric of each candidate codeword is computed on-the-fly from the 24 soft symbols provided by the SIPO shift register, Finally, the transmission block is composed solely of a parallel-in serial-out (PISO) shift register, used to deliver sequentially the decoded message (systematic bits of the decoder decision) at the decoder output.

V. CONCLUSION

In this survey paper discuss on Implementation Of Galois Field Encoder & Decoder. The important outcomes of this paper are shown in the section of comparative analysis.In this survey paper observe that the Implementation Of Galois Field Encoder & Decoder. Also most of the Encoder & Decoder. In future design a better Implementation Of Galois Field Encoder & Decoder. That can improve all these problems in this Galois Field Encoder & Decoder. In future try to Implementation Of Galois Field Encoder & Decoder.

References

[1]. SatyabrataSarangi and Swapna Banerjee, "Efficient Hardware Implementation of Encoder and Decoder for Golay Code" IEEE transactions on very large scale integration (VLSI) systems, vol. 23, no. 9, September 2015.

[2]. AmirhosseinAlimohammad and SaeedFouladiFard, "FPGA-Based Bit Error Rate Performance Measurement of Wireless Systems", IEEE transactions on very large scale integration (VLSI) systems, vol. 22, issue 7, pp.1583-1592, Jul. 2014.

[3]. P. Adde and R. Le Bidan, "A low-complexity soft-decision decoding architecture for the binary extended Golay code," in Proc. 19th IEEE International. Conference Electronics, Circuits, System. (ICECS), Dec. 2012, pp. 705–708.

[4]. Patrick Adde, Daniel Gomez Toro, and Christophe Jego,"Design of an Efficient Maximum Likelihood Soft Decoder for Systematic Short Block Codes", IEEE Transaction Signal Process., vol. 60, no. 7, pp. 3914–3919, Jul. 2012.

[5]. T.-C. Lin, H. –C. Chang, H. –P. Lee, and T.-K. Truong "On the decoding of the (24, 12, 8) Golay Code", International Science., vol. 180, no. 23, pp. 4729–4736 Dec. 2010.

[6]. Yen-Wen Huang and Ying Li, "802.16 Uplink Sounding via QPSK Golay Sequences" vol. 13, no.3PP.152-161, July, 2010.

[7]. S.-Y. Su and P.-C. Li, "Photoacoustic signal generation with Golay coded excitation," in Proc. IEEE Ultrason. Symp. (IUS), Oct. 2010, pp. 2151–2154.

[8]. Hehn, Thorsten, et al. "Multiple-bases belief-propagation decoding of high-density cyclic codes." IEEE transactions on communications 58.1 (2010): 1-8.

[9]. Adde, Patrick, et al. "Design and implementation of a soft-decision decoder for cortex codes." 2010 17th IEEE International Conference on Electronics, Circuits and Systems. IEEE, 2010.

[10]. M.-H. Jing, Y.-C. Su, J. –H. Chen, Z.-H. Chen, and Y. Chang, "High-Speed Low-Complexity Golay Decoder Based on Syndrome weight Determination" in Proc. 7th Int. Conf. Int., Communication , Signal Process, Dec. 2009, pp. 1-4.

[11]. Wong, Yin Sweet, et al. "Implementation of convolutional encoder and Viterbi decoder using VHDL." 2009 IEEE Student Conference on Research and Development (SCOReD). IEEE, 2009.

[12]. Hehn, Thorsten, et al. "Permutation decoding and the stopping redundancy hierarchy of cyclic and extended cyclic codes." IEEE Transactions on Information Theory 54.12 (2008): 5308-5331.

[13]. Chunjian, Deng, et al. "MCU Interface Based Golay Coder & Decoder in SoC Realization." 2008 Second International Symposium on Intelligent Information Technology Application. Vol. 2. IEEE, 2008.

[14]. X. –H. Peng, and P. G. Farrell, "On Construction of the (24, 12, 8) Golay Codes", IEEE Trans. Inf. Theory, vol. 52, no. 8, pp. 3669–3675, Aug. 2006

[15]. Chr, Ching-Lung, Szu-Lin Su, and Shao-Wei Wu. "Decoding the (23, 12, 7) Golay code using a low-complexity scheme." IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 89.8 (2006): 2235-2238

[16]. Murugan, Arul D., et al. "A unified framework for tree search decoding: Rediscovering the sequential decoder." IEEE Transactions on Information Theory 52.3 (2006): 933-953.

[17]. G. Campobello, G. Patane, and M. Russo, "Parallel CRC Realization" IEEE Trans. Comput., vol. 52, no. 10, pp. 1312-1319, Oct. 2003.

[18]. Engin, Nur, and Kees van Berkel. "Viterbi decoding on a coprocessor architecture with vector parallelism." 2003 IEEE Workshop on Signal Processing Systems (IEEE Cat. No. 03TH8682). IEEE, 2003.

[19]. Chang, Yaotsu, et al. "Algebraic decoding of (71, 36, 11),(79, 40, 15), and (97, 49, 15) quadratic residue codes." IEEE transactions on communications 51.9 (2003): 1463-1473.

[20]. Kwak, Jaeyoung, and Kwyro Lee. "Design of dividable interleaver for parallel decoding in turbo codes." Electronics Letters 38.22 (2002): 1362-1364.

[21]. Uchida, Yoshihiro, et al. "VLSI architecture of digital matched filter and prime interleaver for W-CDMA." 2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No. 02CH37353). Vol. 3. IEEE, 2002.

[22]. M. Spachmann, "Automatic generation of parallel CRC circuits", IEEE Des. Test. Comput., vol. 18, no. 3, pp. 108-114, May/Jun. 2001.

[23]. Winstead, Chris, et al. "Analog MAP decoder for (8, 4) Hamming code in subthreshold CMOS." Proceedings 2001 Conference on Advanced Research in VLSI. ARVLSI 2001. IEEE, 2001.

[24]. Fekri, Faramarz, et al. "Decoding of half-rate wavelet codes; Golay code and more." 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No. 01CH37221). Vol. 4. IEEE, 2001.

[25]. Solomon, G. "Golay encoding/decoding via BCH-Hamming." Computers & Mathematics with Applications 39.11 (2000): 103-108.

[26]. R. Nair, G. Ryan and F. Farzaneh"A Symbol Based Algorithm for Hardware Implementation of Cyclic Redundancy Check (CRC)," in Proc. VHDL Int. Users' Forum, Oct. 1997, pp. 82-87.

[27]. Cao, Weixun. "High-speed parallel VLSI-architecture for the (24, 12) Golay decoder with optimized permutation decoding." 1996 IEEE International Symposium on Circuits and Systems. Circuits and Systems Connecting the World. ISCAS 96. Vol. 4. IEEE, 1996.

[28]. A.Vardy and Y. Be'eg, "More Efficient Soft Decoding Of The Golay Codes," IEEE Trans. Inf. Theory, vol. 37, no. 3, pp. 667-672, May 1991.
[29]. S. –W. Wei and C. –H. Wei, "On High-speed Decoding of the (23,12,7) Golay Code," IEEE Trans. Inf. Theory, vol. 36, no. 3, pp. 692-695, May 1990.
[30]. J. Snyders and Be' ery, "Maximum likelihood soft decoding of binary block codes and decoders for the Golay codes," IEEE Trans. Inf. Theory, vol. 35, no. 5, pp. 963-975, Sep. 1989.