DVB-S2 IRA Code를 위한 최적 부호화 방법

정회원 황 승 오*, 종신회원 이 재 용**

Efficient Partial Parallel Encoders for IRA Codes in DVB-S2

Sung Oh Hwang *Regular Member**, Jaiyong Lee** *Lifelong Member*

요 약

갤러거와 맥케이에 의해 처음 소개된 LDPC(Low density parity check)부호는 성능의 우수함 및 간단한 복호 과정으로 많은 관심을 받아 왔으며, 특히 DVB-Satellite 2, DVB-Cable 2, DVB-Terrestrial 2 등의 차세대 방송 시스템에서 널리 사용되고 있다. LDPC 부호의 성능은 충분히 긴 길이의 부호어와 iterative decoder를 사용함으로서 샤논의 한계에 거의 근접하는 성능을 보여준다. 그러나, LDPC 부호는 현재 이동통신에서 널리 사용되고 있는 Turbo 부호와 비교해서 복잡한 부호화 과정이 단점으로 지적되고 있다. 본 논문에서는 IRA 부호기를 사용하여 DVB-S2 LDPC 부호기의 성능을 향상 시킬 수 있는 방안을 제안한다.

Key Words : LDPC, IRA, Accumulator, Partial Encoding, Parallel Encoding, DVB-S2

ABSTRACT

Low density parity check (LDPC) code, first introduced by Gallager and re-discovered by MacKay et al, has attracted researcher's interest mainly due to their performance and low decoding complexity. It was remarkable that the performance is very close to Shannon capacity limit under the assumption of having long codeword length and iterative decoder. However, comparing to turbo codes widely used in the current mobile communication, the encoding complexity of LDPC codes has been regarded as the drawback. This paper proposes a solution for DVB-S2 LDPC encoder to reduce the encoder latency. We use the fast IRA encoder that use the transformation of the parity check matrix into block-wise form and the partial parallel process to reduce the number of system clocks for the IRA code encoding. We compare the proposed encoder with the current DVB-S2 encoder to show that the performance of proposal is better than that of the current DVB-S2 encoder.

Ⅰ. Introduction

Low density parity check (LDPC) code, first introduced by Gallager and re-discovered by MacKay et al, has attracted researcher's interest mainly due to their performance and low decoding complexity[1-2]. It was remarkable that the performance is very close to Shannon capacity limit under the assumption of having long code word length and iterative decoder. However, comparing to turbo codes widely used in the current mobile communication, the encoding complexity of LDPC codes has been regarded as the drawback.

Irregular Repeat Accumulate (IRA) codes as the accumulator-based LDPC code were developed

※ This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency)" (NIPA-2010-(C1090-1011-0006))

* 삼성전자 DMC 연구소 Multimedia 표준 그룹(sungoh@samsug.com), ** 연세대학교 전기전자공학과 Ubinet LAB(jyl@yonsei.ac.kr)

논문번호 : KICS2010-08-414, 접수일자 : 2010년 8월 24일, 최종논문접수일자 : 2010년 11월 1일

to have the linear-complexity encoding method using rate-1 accumulator[3]. Even though IRA codes offer the advantage of linear-complexity encoding, their encoding latency due to generation of parity bits is not negligible since it requires 1 system clock per each parity bit. Especially, the latency increases dramatically when cordword length is long.

To reduce the encoding complexity of IRA codes, there have been a few technical proposals. Yokokawa *et al.*[4] proposed a partial parallel encoder structure for DVB-S2 LDPC codes, which is a special class of IRA codes[5] and Gomes *et al.*[6] also proposed high throughput encoder architecture for the DVB-S2 LDPC codes[6]. The DVB-S2 LDPC codes have the structured parity-check matrix(PCM) whose information part has the cyclic structure in every 360 columns. In [4], the encoder architecture has the efficient mechanism to compute the information part by using the quasi-cyclic structure of the DVB-S2 LDPC codes. However, it still requires many system clocks for generating parity bits part. Furthermore, the possible maximum value for the parallel encoding factor p is limited to 12. In [6], the authors use the quasi-cyclic structure and they proposed a partial parallel algorithm with factor 360 for generating parity bits. So, their encoder architecture supports the relatively low delay and high throughput. However, the fixed periodicity factor 360 may not be the optimal value for the parity part bit generation because it was selected only for the optimal generation of information part.

In this paper, we propose new encoder for DVB-S2 LDPC codes with the partial parallel encoding algorithm and also show how our proposal can enhance the existing encoders' performance including the encoder in [6].

Ⅱ. Irregular repeat-accumulate (IRA) Codes

Generally, LDPC codes are specified by PCM, which is divided into information and parity parts. IRA codes are developed for the simple encoding process by using of dual diagonal structure in the parity part. Assume that N is the code word length and K is the information length, the PCM of IRA codes is shown as:

$$H = [H_1 \;\; H_P] = \begin{bmatrix} & & & & \\ H_1 & & & & \\ & & & & \\ & & & & \end{bmatrix} \begin{vmatrix} 1 & & & 0 \\ 1 & 1 & & \\ & & \ddots & \\ 0 & & 1 & 1 \end{vmatrix}, \quad (1)$$

Where H_I is $(N-K)\times K$ matrix for information part and H_P is $(N-K)\times(N-K)$ square matrix for parity part.

We can specify codeword vector $\underline{c}$ with the information bit vector $\underline{s}$, the parity bit vector p, and H_p. It is shown in (2)

$$H \cdot \underline{c}^T = \underline{0} = H_1 \cdot \underline{s}^T + H_P \cdot \underline{p}^T \quad (2)$$

Assume that $\underline{v} = H_I \underline{s}^T$ and v_i, v_i are the ith elements of the vector v and $\underline{v}$, respectively. Since H_p has dual diagonal structure, the parity bit vector can be obtained recursively:

$$\begin{aligned} &p_0 = v_0, \\ &p_i = v_i \oplus p_{(i-1)}, \quad i = 1,2,...,N-K-1 \end{aligned} \quad (3)$$

As a result, a simple circuit such as rate-1 accumulator can be used for the implementation of IRA codes, as shown in Fig.1

As shown in Fig.1, the conventional IRA encoding requires every single system clock for a parity bit. Therefore, it requires $(N-K)$ clocks for the whole process. It can be more critical for the low code rate and the long code-length. For instance, the DVB-S2 LDPC code with

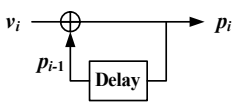

Fig 1. Rate-1 Accumulator

$N = 64000$ and 1/4 code rate requires 48,600 of systems clocks that causes the encoding delay and high clock chip-set.

Ⅲ. Efficient partial parallel encoding process

To overcome the drawback of the IRA encoding scheme, Sung Oh *at el.* proposed the partial parallel encoding process[7]. The first step for the parallel encoding process is the transformation of parity part of the PCM into a block-wise matrix, which bit wise one is used in (1).

3.1 Permutation preprocessing

Denote the row and column permutation matrices by P_R and P_c, respectively. P_R has the dimension $(N-K)\times(N-K)$ and its (i,j) entry is defined as

$$P_{ij}=\begin{cases}1 & \text{if } j\equiv\dfrac{(N-K)}{L}i+\left\lfloor\dfrac{i}{L}\right\rfloor \bmod(N-K),\ \ 0\le i,j<(N-K)\\ 0 & \text{otherwise.}\end{cases} \tag{4}$$

where L is a divisor of $(N-K)$. Furthermore, $N\times N$ martix P_C is defined as

$$P_{\mathrm{C}}=\begin{pmatrix} I_K & O_1 \\ O_1^T & P_{\mathrm{R}}^T \end{pmatrix}, \tag{5}$$

where I_K is $K\times K$ identify matrix and O_1 is $K\times(N-K)$ zero matrix. With P_R and P_C, the transformed block type PCM H_{RC} is given as

$$H_{\mathrm{RC}}=P_{\mathrm{R}}HP_{\mathrm{C}}=\left[P_{\mathrm{R}}H_1 \ \ P_{\mathrm{R}}H_{\mathrm{p}}P_{\mathrm{R}}^{\mathrm{T}}\right]=\left[H_{\mathrm{I,RC}} \ \ H_{\mathrm{P,RC}}\right]. \tag{6}$$

In addition, the new codeword $\underline{c'}$ corresponding to H_{RC} can be obtained as follows:

$$\begin{aligned}\underline{0}=H\cdot\underline{c}^T \Leftrightarrow \underline{0}&=P_{\mathrm{R}}\cdot H\cdot\underline{c}^T=(P_{\mathrm{R}}HP_{\mathrm{C}})\cdot(P_{\mathrm{C}}^T\cdot\underline{c}^T)\\ &=H_{\mathrm{RC}}\cdot\left[\underline{s}\ \ \underline{p}\cdot P_{\mathrm{R}}^T\right]^T=H_{\mathrm{RC}}\cdot\underline{c'}^T.\end{aligned} \tag{7}$$

From (7), we observe that the encoding process which calculates the codeword $\underline{c}$ is equivalent to obtain the new codeword $\underline{c'}$ from the transformed PCM H_{RC}, followed by the re-permutation in the parity bits. Therefore, the parity part of the transformed PCM is given as:

$$H_{\mathrm{P,RC}}=\begin{bmatrix} I_L & O & O & O & S \\ I_L & I_L & O & O & O \\ O & I_L & I_L & O & O \\ \vdots & & \ddots & \ddots & \vdots \\ O & O & O & I_L & I_L \end{bmatrix} \tag{8}$$

where I_L and O are the $L\times L$ identity and zero matrix, respectively, and S is $L\times L$ matrix whose (i,j) enrty $S_{(i,j)}$ is given as

$$S_{ij}=\begin{cases}1 & \text{if } i-1=j \text{ and } 1\le i,j<L,\\ 0 & \text{otherwise.}\end{cases} \tag{9}$$

Note that the parity part of the transformed PCM is represented in a block-wise form, which enables the partial parallel encoding with simple permutation.

The IRA code with the transformed PCM in (6) can be encoded by using a modified Richardson-Urbanke method[8]. Based on the Richardson-Urbanke method, the transformed PCM is further divided into 6 sub-matrixes as:

$$H_{\mathrm{RC}}=\left[H_{\mathrm{I,RC}} \ \ H_{\mathrm{P,RC}}\right]=\begin{bmatrix} A & E & S \\ B & T & C \end{bmatrix} \tag{10}$$

where the dimensions of sub-matrices are

$$\begin{aligned} &A: L\times K \quad B:(N-K-L)\times K \quad C:(N-K-L)\times L\\ &T:(N-K-L)\times(N-K-L) \quad E: L\times(N-K-L)\end{aligned} \tag{11}$$

and S is the same matrix in (9). According to [8], the encoding process can be expressed as the following equations.

$$B\,\underline{s}^T+T\,\underline{p}_1^T+C\,\underline{p}_2^T=\underline{0} \tag{12}$$

$$(ET^{-1}B+A)\underline{s}^T+(ET^{-1}C+S)\underline{p}_2^T=\underline{0} \qquad (13)$$

where $\underline{p}_1$ and $\underline{p}_2$ are the divided part of parity bits, which have the length of $N-K-L$ and L, respectively. Therefore, the proposed encoding process is calculating each part of parity bits $\underline{p}_1$ and $\underline{p}_2$, from the transformed PCM, and restoring the transformed parity bits into the original solution shown in (7). Note that each process can be constructed in a simple operation.

3.2 Encoding Process for calculation of $\underline{p}_2$

(13) can be expressed as

$$(ET^{-1}C+S)\underline{p}_2^T=(ET^{-1}B+A)\underline{s}^T \qquad (14)$$

Due to the property of sparse matrix, the right side of (14) can be easily calculated as introduced in [8]. Furthermore, it is easily shown that $ET^{-1}C$ becomes $L\times L$ identity matrix from (8) and (10). As a result, (14) becomes

$$(I+S)\underline{p}_2^T=(ET^{-1}B+A)\underline{s}^T=\underline{w}^T \qquad (15)$$

Since $(I+S)$ is the dual diagonal matrix, the solution of (15) can be obtained in a similar way like (3), using rate-1 accumulator. However, as the dimension of the solution was reduced to the block size L, the required system clock can be decreased as well.

3.3 Encoding process for calculation of $\underline{p}_1$

From(12), the first part of parity bits, $\underline{p}_1$ can be obtained as

$$T\underline{p}_1^T=B\underline{s}^T+C\underline{p}_2^T \qquad (16)$$

Note that the matrix T is the lower-left part of $H_{P,RC}$, shown in (8), which is composed of block-wise identity matrix I_L and the zero matrix O. Therefore, we can observe that the two adjacent bits within the same block of size L and $\underline{p}_1$ have no relevance to each other, and only two bits located in the same position of the neighboring blocks are relevant. No relevance of all L bits in the block enables the parallel processing with the factor of block size. Therefore, taking into account that the length of $\underline{p}_1$ is $N-K-L$, the total system clocks requires is equal to $(N-K)/L-1$, when the rate-1 accumulator circuit is used.

Ⅳ. Encoder Implementation

4.1 General Encoder Architecture

we showed the proposed encoder architecture at Figure 2. From the information vector and the particle matrices of transformed PCM, L bit parity vector $\underline{p}_2$ can be calculated first. Afterwards, the last part of parity vector $\underline{p}_1$ will be obtained in L branches of rate-1 accumulators. Then the overall parity vector $\underline{p}$ is obtained by

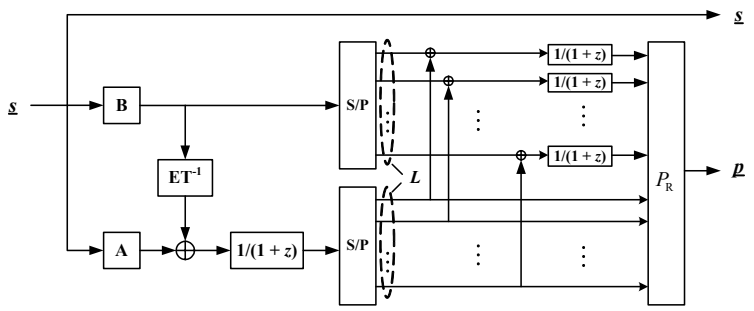

Fig 2. Architecture of proposed IRA encoder

re-permutation.

The computational complexity and required system clocks at each step in the proposed encoding procedure is shown in Table 1. In Table 1, the operation of information part is not considered because it depends on the structure of information part. What we focused on is the operation of the parity bits generation for any IRA codes. In Table 1, it is easily checked that the total system clocks required is $2(N-K)/L+L-1$. We can find its minimum value at $L \approx \sqrt{2(N-K)}$ from the inequality of arithmetic and geometric means. Note that the calculation for the inverse of T is not required in step 2 because ET^{-1} is identical to $[II\cdots I]$.

4.2 Enhanced DVB-S2 Encoder

In [6], Gomes *et al.* proposed the high throughput encoder architecture based on the quasi-cyclic structure, which is specialized for DVB-S2 LDPC codes. They fixed the parallel factor as 360 since they considered the periodicity factor 360 is the optimal value for the information part of all DVB-S2 LDPC codes[6]. Therefore, it is possible to support the efficient encoding for the information part, while its efficiency for generating parity bits may be decreased.

As a result of Table 1, we can find the

Table 1. Complexity of each sten in the proposed encoder

Encoding Step	Operation Complexity	# of System Clocks
1. compute $A\underline{s}$ and $B\underline{s}$	$O(N)$	-
2. compute $ET^{-1}B\underline{s}$ by using $ET^{-1}=[I\ I\ \cdots\ I]$	$(N-K-2L)$ XORs	$(N-K)/L-2$
3. addition of $A\underline{s}$ and $ET^{-1}B\underline{s}$	L XORs	1
4. compute $\underline{p_2}$in (12)	$(L-1)$ XORs	L
5. addition of $B\underline{s}$ and $C\underline{p_2}$in (13)	L XORs	1
6. compute $\underline{p_1}$ in(13)	$(N-K-L)$ XORs	$(N-K)/L-1$

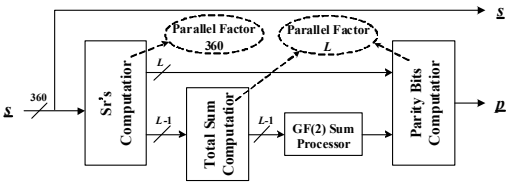

Fig 3. Enhanced Gomes' DVB-S2 Encoder

method to maximize the efficiency of Gomes' encoder. The proposed encoder structure is shown at Fig. 3. The main difference between Gomes' encoder and the proposed encoder is the flexible parallel factor for its computation. By applying parallel factor $L \approx \sqrt{2(N-K)}$ to them for each code rate, we can enhance the encoder performance in [6]. Even though the parallel factor is varying, the operation of each component is not basically changed. For example, in [6], the size of the binary matrix for storing S_r values is $(N-K)/360 \times 360$ and total sum computatior is carried out by 360 elements. On the other hand, we propose to rearrange the matrix for S_r into $(N-K)/L \times L$ and carry out total sum computatior by L elements with the same operation.

In Table 2, we present the number of required system clocks for generating parity bits based on the proposed encoding process for the DVB-S2 LDPC codes with N=16200. As shown at Table 2 L values that can minimize the number of clocks is closed to $\sqrt{2(N-K)}$. Therefore, we should use L value, which is smaller that 360 used in [6] to have the optimal encoder operation.

Table 2. Comparison of required system clocks for generating parity (N=16,200)

Code Rate	Conventional	Gomes at al[6]	Proposed encoder	
	# of clocks	# of clocks	L	# of clocks
1/5	12,960	429	160	321 (97.52%)
2/5	9,720	411	135	278 (97.14%)
3/5	6,480	393	108	227 (96.50%)
7/9	3,600	377	80	169 (95.31%)
8/9	1,800	367	60	119 (93.59%)

Note that we consider the system clocks for only total sum computatior, GF(2) sum processor, and parity bit computatior corresponding to equations (11), (12) and (14) in [6], respectively.

Ⅴ. Conclusion

We proposed the enhanced DVB-S2 encoder with IRA encoding process based on the efficient generation method for the parity bits part. We also showed that the proposal reduced the encoding latency. The additional benefits of proposal are we can apply it for any IRA codes because we don't used a fixed periodicity factor. Therefore, we can more easily use IRA coding for the real time stream data requiring a very short transmission delay.

References

〔1〕 R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inform. Theory*, Vol. IT-8, pp.21-28, Jan., 1962.

〔2〕 D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low-density parity-check codes," *IEE Electron. Lett.,* Vol.32, pp.1645-1646, Aug., 1996.

〔3〕 D. Divsalar, H. Jin, and R. J. McEliece, "Coding theorems for 'turbo-like' codes," in *Proc. 36th Allerton Conf. on Communication, Control, and Computing*, Allerton, Illinois, Sept., 1998, pp.201-210.

〔4〕 T. Yokokawa, M. Nakane, and M. Kan, "A low complexity and programmable encoder architecture of the LDPC codes for DVB-S2,"in *Proc. Turbo-Coding 2006,* Munich, Germany, April, 2006.

〔5〕 EN 302 307, *Digital video broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, news gathering and other broad-band satellite applications*, European Telecommunications Standards Institute (ETSI), 2003.

〔6〕 M. Gomes, G. Falcao, A. Sengo, and M. Falcao, "High throughput encoder architecture for DVB-S2 LDPC-IRA codes," in *Proc .IEEE International Conf. on Microelectronics (ICM)*, Cairo, Egypt, Dec., 2007, pp.271-274.

〔7〕 S.O. Hwang, S.H. Muyng, H.J. Lee, S.I. Park and J.Y Lee *"Partial Parallel Encoder for IRA codes"*, *IET Electron. Lett.*, Vol.46, Issue 2, pp.135-137, Jan., 2010.

〔8〕 T. J. Richardson and R. L. Urbanke, "Efficient encoding of low-density parity-check codes," *IEEE Trans. Inform .Theory*, Vol.47, pp.638-656, Feb., 2001.

황 승 오 (Sung Oh Hwang) 정회원

1997년 2월 한양대학교 전자통신공학과 학사
1999년 2월 한양대학교 전자통신공학과 석사
1999년 3월~현재 삼성전자 책임연구원
2005년 3월~현재 연세대학교 전기전자공학과 박사과정
2005년 3월 OMA BCAST WG 부의장
2006년 8월~현재 OMA BCAST WG 의장
<관심분야> 디지틀방송 응용계층/물리 계층, 휴대방송 응용 계층/물리 계층, Security, DRM, IPTV

이 재 용 (Jaiyong Lee) 종신회원

1977년 2월 연세대학교 전자공학과 학사
1984년 5월 IOWA State University 공학석사
1987년 5월 IOWA State University 공학박사
1987년 6월~1994년 8월 포항공과대학 교수
1994년 5월~현재 연세대학교 전자공학과 교수
<관심분야> Protocol Design for Wired/Wireless QoS Management, Ubiquitous Sensor Network, Wireless Multimedia Support Protocol, Mobile Multimedia Broadcasting service