Design of Encoder and Decoder for LDPC Codes Using Hybrid H-Matrix

Chanho Lee

Low-density parity-check (LDPC) codes have recently emerged due to their excellent performance. However, the parity check (H) matrices of the previous works are not adequate for hardware implementation of encoders or decoders. This paper proposes a hybrid parity check matrix which is efficient in hardware implementation of both decoders and encoders. The hybrid H-matrices are constructed so that both the semi-random technique and the partly parallel structure can be applied to design encoders and decoders. Using the proposed methods, the implementation of encoders can become practical while keeping the hardware complexity of the partly parallel decoder structures. An encoder and a decoder are designed using Verilog-HDL and are synthesized using a 0.35 μm CMOS standard cell library.

Keywords: Low-density parity-check (LDPC), semi-random, hybrid H-matrix, partly parallel structure.

I. Introduction

Wireless mobile communication now demands large data bandwidth to accommodate various multimedia services. The third generation mobile communication, IMT-2000, provides 144 kbps for a fast moving terminal, 384 kbps for walking conditions, and 2 Mbps for stationary conditions [1]. The current bandwidth of IMT-2000 will not be enough to satisfy the various future demands for real-time and high quality service, compared to wired communication services for fast moving stations. The specification of fourth generation (4G) mobile communication is being developed to overcome the limitation. 4G mobile communication is supposed to provide 100 Mbps for a fast moving station and 155 Mbps to 1 Gbps for slow moving and stationary conditions. Such a system requires a very high speed wireless transmission technique.

A wireless channel environment is more subject to noise than a wired channel because the signals are open to external disturbances such as path loss, shadowing, and fading. Therefore, channel coding is inevitable for wireless communication. Channel coding has been an important issue in communication systems. It has the ability to detect and correct errors caused by noise on a channel. The bit-error-rate (BER) can be reduced without increasing the signal power since the transmitted data carry redundancies that are used to detect and correct errors. This coding skill is useful in transmission on finite power channels such as general switched telephone networks [2]-[5].

Low-density parity-check (LDPC) codes [6] proposed by R. G Gallager in 1962 were too complex to implement and had almost been forgotten in spite of their powerful error-correcting capability. However, it was rediscovered by MacKay and Neal in the 1990s, who made significant improvements on BER

Manuscript received Jan. 13, 2005; revised May 12, 2005.

This work was supported by Soongsil University Research fund. The material in this work was presented in part at IT-SoC 2004, Seoul, Korea, Oct. 2004.

Chanho Lee (phone: + 82 2 820 0710, email: chlee@ssu.ac.kr) is with the School of Electronic Engineering, Soongsil University, Seoul, Korea.

performance [7]. Chung and others [8] showed that the threshold for an LDPC code of code rate 1/2 on an additive white Gaussian noise (AWGN) channel was within 0.0045 dB of the Shannon limit, and simulation results were within 0.04 dB of the Shannon limit at a BER of 10^{-6} using a block length of 10^7.

Compared with turbo codes, the LDPC codes exhibit better performance due to good distance properties and less complex and highly parallelizable decoding approaches [9]. Therefore, the LDPC codes have been widely considered as next-generation error-correcting codes for telecommunication. DVB-S2, the new European satellite broadcasting system, also employs a concatenated code composed of a LDPC code and BCH code [10].

However, the encoding complexity of LDPC codes is still too high, which is a major problem that needs to be solved for their implementation. There have been some studies to reduce the encoding complexity using specially formed matrices such as a lower triangular matrix [11] or semi-random matrix [12].

The encoding process of standard LDPC codes requires transferring a parity check matrix (H) into an equivalent systematic form, which can be accomplished by Gaussian elimination [12]. Gaussian elimination requires large memory and heavy calculation. The encoding process with a semi-random technique is much simpler than that using other matrices because it doesn't require Gaussian elimination [12]. Consequently, a linear time encoding is possible with very little memory.

The hardware implementation of LDPC decoders is another problem to be considered when we use the fully parallel decoding algorithm of LDPC codes [9]. Although the fully parallel decoders can achieve a very high decoding speed, it is too complex to implement practically [12]. One of the best solutions for the decoder architecture is to directly instantiate the belief propagation (BP) algorithm [14] in hardware [13]. In fully parallel decoding structures, all check nodes and variable nodes have their own processors and exchange messages between each check node and variable node at the same time. In order to lower the hardware complexity, the number of check node and variable node processors needs to be reduced. In partly parallel decoding structures, part of variable nodes and check nodes perform the message passing process in time-division multiplexing mode [15]. Therefore, there is trade-off between decoding throughput and hardware complexity in partly parallel structures.

Although the hardware complexity of LDPC decoders is reduced using the partly parallel structures, these structures have a potential problem of encoding complexity because their parity check matrices may not be suitable for an efficient encoding process.

In this paper, we propose a hybrid model that combines partly parallel decoder structures and a semi-random technique to have efficient encoding and decoding processes. The hybrid H-matrix has the advantages of both the partly parallel decoder structures and the semi-random technique. An encoder using the hybrid H-matrix has a similar hardware complexity of an encoder with the semi-random technique. A decoder using the hybrid H-matrix has similar operation characteristics and hardware complexity to a partly parallel decoder. The proposed hybrid H-matrix makes the practical implementation possible for both the encoders and decoders of LDPC codes. We show how to construct a hybrid H-matrix and generate an H-matrix with a 32 × 32 base matrix. Using the matrix, we implement a high performance LDPC encoder and decoder with practical throughput and hardware complexity.

II. Hybrid H-Matrix

1. Semi-random Technique

An H-matrix, generated using the semi-random technique, consists of two parts, H^d and H^p, H^d being a randomly generated form and H^p a deterministic form [12]. The matrix structure makes encoding processes simple because the deterministic form of H^p shown in Fig. 1 is a dual-diagonal square matrix.

$$H^p = \begin{bmatrix} 1 & 0 & 0 & \cdots & \cdots & 0 & 0 & 0 \\ 1 & 1 & 0 & \cdots & \cdots & 0 & 0 & 0 \\ 0 & 1 & 1 & \cdots & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \cdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \cdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & \cdots & 1 & 1 & 0 \\ 0 & 0 & 0 & \cdots & \cdots & 0 & 1 & 1 \end{bmatrix}$$

Fig. 1. A deterministic matrix in the semi-random technique.

Although an H^d-matrix is randomly generated, some efficient forms of matrices are preferred for better coding performance if possible. Once an H^d-matrix is generated, the H-matrix is constructed as $H = [H^d, H^p]$. When a codeword $C = [d, p]^t$, where d and p are information bits and parity bits, respectively, parity bits can be easily calculated according to the following equation of [12]:

$$\begin{aligned} p_1 &= \sum_j h_{1j}^d d_j, \\ p_i &= p_{i-1} + \sum_j h_{ij}^d d_j, \end{aligned} \tag{1}$$

where $p = \{p_i\}$ and $d = \{d_i\}$. Equation (1) can be easily implemented using an exclusive-OR gate and a flip-flop as shown in Fig. 2 [17].

The encoder structure can be constructed using an input buffer,

an interleaver, and a parity bit generator as shown in Fig 3. The H^d-matrix determines the interleaving operations, and the interleaver is the only part of the encoder blocks to be modified when a different H^d-matrix is applied. Therefore, we have to find a good H^d-matrix for efficient encoding. In the semi-random technique, the choice of a good H^d-matrix is a major point for good performance and efficient hardware implementation.

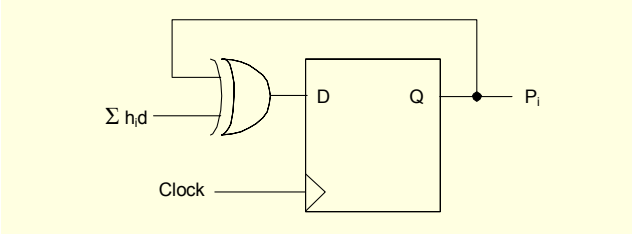

Fig. 2. Schematic of a parity bit generation circuit.

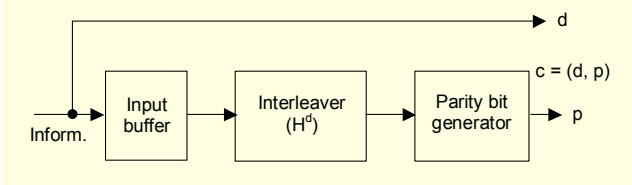

Fig. 3. Block diagram of an encoder using a semi-random technique.

2. Partly Parallel Structure

Partly parallel decoder structures were originally proposed by Zhang and others [18]. First, they designed a good partly parallel decoder structure. Then, a new parity check matrix form, which was constructed with shifted identity matrices, was generated based on the structure. However, their model does not support a flexible code rate or a degree distribution, which is required to achieve very good error-correcting performance [15]. A modified model, a matrix expansion method, is proposed to solve the problem of the original partly parallel decoder structure [15]. An expanded matrix is constructed using an ($M_s \times N_s$) base matrix and ($p \times p$) shifted identity matrices.

We need to apply a bit-filling algorithm to construct a base matrix [19]. Since the matrix generated by the bit-filling algorithm has a large girth, which can be a standard of good error correcting capability, we can avoid small cycles that make performance worse and can expect to have a matrix with a good error correcting capability. In Fig 4, we show a randomly expanded ($pM_s \times pN_s$) matrix after a base matrix with the bit-filling algorithm is generated [15]. Each 0 in the base matrix is expanded to a ($p \times p$) zero sub-matrix O, and 1's are expanded to a ($p \times p$) sub-matrix $T_{u,v}$. Sub-matrix $T_{u,v}$ is a ($p \times p$) identity matrix with a cyclic shift right by the number of randomly generated integers. The method of replacing and expanding 1's of a base matrix with identity matrices make the design flexible. When we implement decoder structures with the expanded matrices, all check nodes and variable nodes don't have to have their own computational units, and the time-division multiplexing mode can be applied [18].

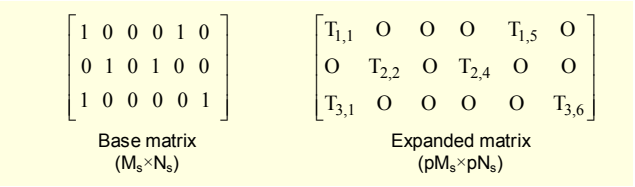

Fig. 4. Matrix expansion in a partly parallel algorithm [15].

As shown in Fig. 5 [15], the numbers of check node processor units (CNUs) and variable node processor units (VNUs) are M_s and N_s, respectively, which are the numbers of rows and columns of the base matrix. In fully parallel structures, $p \cdot M_s$ CNUs and $p \cdot N_s$ VNUs are required, and they are p times the number of the processor units in partly parallel structures. However, the partly parallel decoder completes a decoding iteration in 2p cycles, while the fully parallel decoder needs only 2 cycles for a decoding iteration.

The partly parallel decoding scheme still has the problem of encoding complexity, although the implementation of a decoder becomes efficient in its hardware size and flexible with the expanded matrices, which are constructed for partly parallel decoder structures.

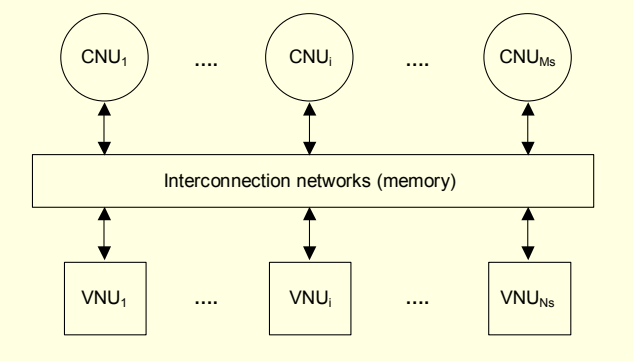

Fig. 5. The structure of a partly parallel decoder [15].

3. Structure of Hybrid H-Matrix

We investigated the implementation methods for the encoder and decoder of an LDPC code. The implementation methods still have problems. That is, the decoder structure according to the semi-random technique is very complex, while the encoder structure is simple. The partly parallel structure enables the simple decoder structure, while the encoder structure is complex.

We propose a hybrid H-matrix to solve the problem of the implementation methods for conventional LDPC codes. The hybrid H-matrix is constructed by combining the semi-random technique and the partly parallel structure. Figure 6 shows the structure of a hybrid H-matrix. The hybrid H-matrix has a systematic form of $[H^d | H^p]$, where H^d is a matrix according to the partly parallel structure and H^p is a dual diagonal matrix according to the semi-random technique. The hybrid H-matrix enables the implementation of a simple encoder according to the semi-random technique and a simple decoder according to the partly parallel structure. Therefore, both the encoder and the decoder can be implemented in hardware with practical hardware complexity.

The proposed LDPC code is regular since the hybrid H-matrix is constructed in a regular manner. The BER performance of the proposed LDPC code is similar to those of the other regular codes, while it is worse than those of irregular codes [9], [15], and [20].

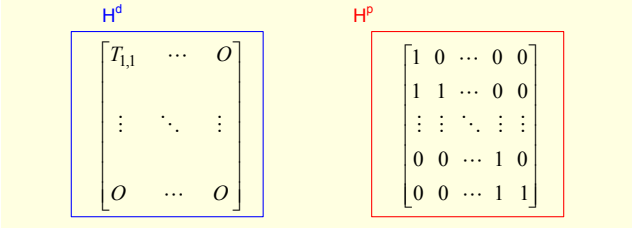

Fig. 6. The structure of a hybrid H-matrix.

4. Encoder Structure

Figure 7 shows the structure of an encoder for an LDPC code using the proposed hybrid H-matrix. It can be implemented in a simple manner using exclusive-OR gates, multiplexers, and memory as shown in the figure. The number of memory blocks is the same as that of the columns of the base matrix. The source information bits are stored and transmitted through port *d* shown in Fig. 7. The parities are calculated and transmitted through port *p* using the data in the memory after a block of information bits has been received. When the memory is filled with information bits, several information bits in memory corresponding to the non-zero elements of a column of the base matrix are selected using the select signals from the "MEM_LUT" which has the information of the base matrix. The selected bits are then shifted right by the amount that the non-zero elements of the base matrix represent. The numbers of shifts are stored in the "SHIFT_LUT." The results are used to calculate a parity bit.

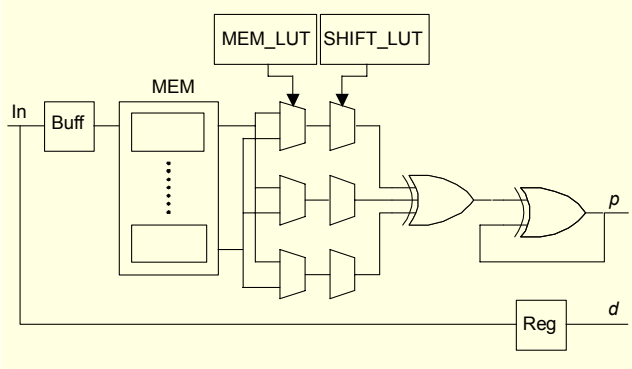

Fig. 7. The structure of an encoder using a hybrid H-matrix.

5. Decoder Structure

Figure 8 shows the structure of a decoder using the hybrid H-matrix. The normalized uniformly most probable belief propagation (UMP-BP) algorithm [21] is used instead of the sum-product algorithm [7] to reduce the complexity of the hardware. The UMP-BP algorithm uses the function of finding the minimum value and additions instead of addition and multiplication in the sum-product algorithm. It does not require the channel estimation process, which is necessary in the sum-product algorithm. The received signals are processed between the VNU block and the CNU block iteratively. The number of iterations is predetermined or adaptively determined depending on the decoding condition. The decoded bits are generated in the decision unit after the iterative process.

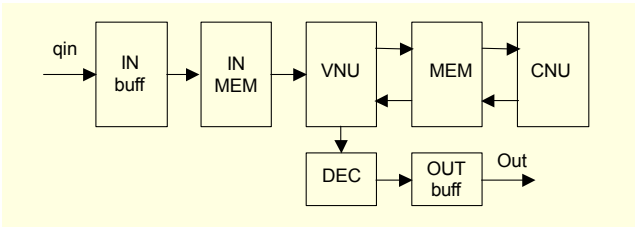

Fig. 8. The structure of a decoder using a hybrid H-matrix.

III. Design and Implementation

We need to modify the H-matrix in order to reduce the encoding complexity of the partly parallel structure as mentioned above. As we have already shown in section II, an H-matrix generated using the semi-random technique consists of two parts, H^d and H^p. An H^d-matrix with a random form can be replaced by another one. The decoder structure according to the semi-random technique has a large hardware complexity that is not easy to implement. On the other hand, the encoder for the partly parallel decoding scheme is not adequate for implementation. The structure of a decoder in the semi-random technique is not adequate for the partly parallel structure because of the random form of the H^d-matrix. We replace the H^d-matrix in the semi-

random technique with an expanded matrix that is used in the partly parallel decoding scheme. By applying the semi-random technique to partly parallel structures, it is possible to implement both encoders and decoders of LDPC codes with a practical hardware complexity.

We make an H-matrix to construct the proposed hybrid H-matrix. We first make a (32 × 32) base matrix using the bit-filling algorithm and expand it to a (8,192 × 8,192) matrix with (256 × 256) identity matrices. Each identity matrix that replaces the positions of 1's in the base matrix is shifted right by the amount of randomly generated integers. The size (32 × 32) is the minimum size to satisfy the 6-cycle-free characteristic that enhances the BER performance. Figure 9 shows an example of a generated base matrix for implementation with an (8 × 8) base matrix. The numbers in the matrix represent the amount of right-shift in each identity matrix.

The H-matrix is a combination of H^d-matrix and (8,192 × 8,192) H^p-matrix shown in Fig 1. The size of the H-matrix is (16,384 × 8,192), and its code rate is 1/2. We synthesize an LDPC encoder of the hybrid partly parallel structure using a 0.35 um CMOS standard cell library; it occupies 33,900 gate counts and 8,608 bit memory as shown in Table 1. The operation frequency is 99.5 MHz and the throughput is 99.5 Mbps. The results show that the encoder using the hybrid H-matrix has a low hardware complexity.

The decoder structure with a hybrid H-matrix is similar to that of the partly parallel decoder since the H^d-matrix is the same as the left half of the H-matrix of the partly parallel coding scheme. The structure is slightly changed due to the H^p-matrix, which corresponds to the right half of the H-matrix of the partly parallel decoding scheme. The VNU block and the interleaver in Fig. 10 are modified from those of the partly parallel decoder to process the H^p-matrix part. The CNU block and the de-interleaver are also changed slightly. We assume that the received data, "data_in", are quantized as 4 bits. The CNU receives 5 × 4 bits of data and the VNU receives and processes 7 × 4 bits of data.

We synthesize an LDPC decoder of the hybrid partially parallel structure using a 0.35 um CMOS standard cell library; it occupies 6,900 gate counts and 337,600 bit memory as shown in Table 1. The operation frequency is 98.1 MHz and the throughput is 49.1 Mbps. The throughput of the decoder can be increased if we increase the number of the VNU and CNU. The number of the VNU and CNU can be up to 32 for the base matrix we use, and the throughput also becomes 32 times the value shown in Table 1.

The hardware complexity, throughput, and memory size of three methods for LDPC codes are compared in Table 2. The results of the decoder with the semi-random technique are obtained assuming a fully parallel decoding scheme. As we mentioned, there is trade-off between the throughput and the hardware complexity. The proposed decoding scheme with the hybrid H-matrix has mostly the same hardware complexity as

$$\begin{bmatrix} 0 & 41 & 35 & 62 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 33 & 0 & 0 & 44 & 0 \\ 22 & 0 & 46 & 0 & 0 & 18 & 0 & 0 \\ 16 & 0 & 0 & 0 & 9 & 0 & 0 & 49 \\ 0 & 49 & 0 & 0 & 0 & 59 & 0 & 41 \\ 0 & 0 & 0 & 43 & 51 & 38 & 0 & 0 \\ 0 & 0 & 27 & 0 & 0 & 0 & 60 & 7 \\ 0 & 12 & 0 & 0 & 62 & 0 & 25 & 0 \end{bmatrix}$$

Fig. 9. Example of generated base matrix for implementation.

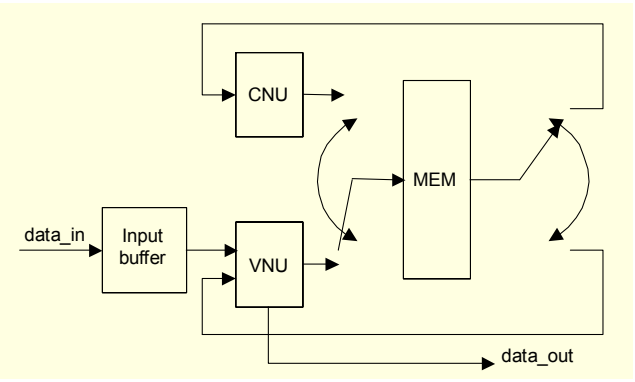

Fig. 10. The structure of the proposed decoding scheme.

Table 1. Results of synthesis using a 0.35 um CMOS standard cell library.

	Encoder	Decoder
Gate-count	33,900	6,900
Memory size (bits)	8,608	337,600
Operating frequency (MHz)	99.5	98.1
Throughput (Mbps)	99.5	49.1

Table 2. Comparison of three methods of implementation for LDPC codes (N = 16,384, code rate = 1/2).

	Semi-random	Partly parallel	Hybrid partially parallel
HW complexity of encoder	~N	>>N	~N
CNU	8,192	32	1
VNU	16,384	64	2
Throughput of decoder (1 iteration)	2	2p	2p
Required memory in decoder	L + p N	L + N	L + N

N: block length p: identity matrix size (=256)

that of the partly parallel methods. On the other hand, the hardware complexity of the proposed encoder is simpler than that of the encoder with the partly parallel coding scheme, and linear time encoding is possible.

IV. Conclusions

An encoding scheme using a semi-random H-matrix is efficient in hardware implementation, while the decoder is not adequate for hardware implementation. The partly parallel decoding scheme is efficient in hardware implementation while the corresponding encoder is not practical for hardware implementation. The encoder using the hybrid H-matrix has a similar hardware complexity of the encoder with the semi-random technique. The decoder using the hybrid H-matrix has similar operation characteristics and hardware complexity to the partly parallel decoder. We generate a (16,384 × 8,192) hybrid H-matrix, and implement the encoder and decoder of the LDPC code using the optimal hybrid H-matrix. The encoder and the decoder have a reasonable size and high throughput.

References

[1] F.E. O'Brien and R.D. Jr. Guenther, "Global Standardization of IMT-2000," *Emerging Technologies Symposium: Broadband, Wireless Internet Access, 2000 IEEE,* Apr. 2000, pp.10-11.

[2] Jong Kang Park and Jong Tae Kim, "Soft IP Compiler for a Reed-Solomon Decoder," *ETRI J.*, vol.25, no.5, Oct. 2003, pp.305-314.

[3] Sooyoung Kim, Woo Seok Yang, and Ho-Jin Lee, "Trellis-Based Decoding of High-Dimensional Block Turbo Codes," *ETRI J.*, vol.25, no.1, Feb. 2003, pp.1-8.

[4] Junichiro Kawamoto, Takahiro Asai, Kenichi Higuchi, and Mamoru Sawahashi, "Independent Turbo Coding and Common Interleaving Method among Transmitter Branches Achieving Peak Throughput of 1 Gbps in OFCDM MIMO Multiplexing," *ETRI J.*, vol.26, no.5, Oct. 2004, pp.375-383.

[5] Chanho Lee, "A Viterbi Decoder with Efficient Memory Management," *ETRI J.*, vol.26, no.1, Feb. 2004, pp.21-26.

[6] R. G Gallager, "Low Density Parity Check Codes," *IRE Trans. Inform. Theory*, vol. IT-8, Jan. 1962, pp. 21-28.

[7] D. J. C. MacKay and R. M. Neal, "Near Shannon Limit Performance of Low Density Parity Check Codes," *Electron. Lett.*, vol. 32, Aug. 1996, pp. 1645-1646.

[8] S.-Y. Chung, G. D. Forney Jr., T. J. Richardson, and R. Urbanke, "On the Design of Low-Density Parity-Check Codes within 0.0045 dB of the Shannon Limit," *IEEE Commun. Lett.*, vol. 5, Feb. 2001, pp. 58-60.

[9] T. Zhang, Z. Wang, and K. K. Parhi, "On Finite Precision Implementation of Low-Density Parity-Check Codes Decoder," *Proc. of 2001 IEEE Int. Symp. on Circuits and Systems* (*ISCAS*), Sydney, Australia, vol. 4, May 2001, pp. 202-205.

[10] DVB-S2 DRAFT ETSI EN 302 307 V1.1.1 (204-06), *Digital Video Broadcasting-Satellite Version 2*, ETSI, 2004.

[11] T. J. Richardson and R. Urbanke, "Efficient Encoding of Low-Density Parity-Check Codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, Feb. 2001, pp. 638-656.

[12] L. Ping, W. K. Leung, and N. Phamdo, "Low Density Parity Check Codes with Semi-Random Parity Check Matrix," *IEE Electronics Lett.*, vol. 35, Jan. 1999, pp. 38-39.

[13] T. Zhang and K. K. Parhi, "A 54 Mbps (3,6)-Regular FPGA LDPC Decoder," *Signal Proc. Systems, 2002. IEEE Workshop* (*SiPS*), San Diego, USA, Oct. 2002, pp. 16-18.

[14] D. J. C. MacKay, "Good Error-Correcting Codes Based on very Sparse Matrices," *IEEE Trans. Inform. Theory*, vol. 45, Mar. 1999, pp. 399-431.

[15] H. Zhong and T. Zhang, "Design of VLSI Implementation-Oriented LDPC Codes," *IEEE Vehicular Technology Conf.*, Orlando, USA, Oct. 2003.

[16] J. Hao, "Analysis of Scaling Soft Information on Low Density Parity Check Codes," *Electronics Letters*, 39(2), Jan 2003, pp.219-221.

[17] R. Echard, and S.-C. Chang, "The π-Rotation Low-Density Parity Check Codes," *IEEE Global Telecom. Conf.*, vol. 2, San Antonio, USA, Nov. 2001, pp. 980-984.

[18] T. Zhang, and K. K. Parhi, "VLSI Implementation-Oriented (3,k)-Regular Low-Density Parity Check Codes," *IEEE Workshop, Signal Processing Systems* (*SiPS*), Antwerp, Belgium, Sept. 2001, pp. 25-36.

[19] J. Campello and D. S. Modha, "Extended Bit-Filling and LDPC Code Design," *IEEE Global Telecom. Conf.*, 2001, San Antonio, USA, Nov. 2001, pp. 985-989.

[20] T. Zhang, "Efficient VLSI Architectures for Error-Correcting Coding," *Doctoral thesis*, Univ. of Minnesota, 2002.

[21] J. Chen and M.P.C. Fossorier, "Near Optimum Universal Belief Propagation Based Decoding of Low-Density Parity Check Codes," *IEEE Trans. Commun.,* vol. 50 issue 3, March 2002, pp. 406-414.

Chanho Lee received the BS and MS degrees in electronic engineering from Seoul National University, Seoul, Korea, in 1987 and 1989, and the PhD degree from the University of California, Los Angeles, in 1994. In 1994, he joined the semiconductor R&D center of Samsung Electronics, Giheung, Korea. Since 1995, he has been a faculty member of the School of Electronic Engineering, Soongsil University, Seoul, Korea, and he is currently an Associate Professor. His research interests are in the design of a channel codec, 2D/3D graphic processor and MPEG codec, SoC on-chip-bus, and in low-power designs. He is a senior member of IEEE.