

# 블록 저밀도 패리티 검사 부호 설계를 위한 테너 그래프 기반의 저복잡도 순환 주기 탐색 알고리즘

명 세 창\*, 전 기준\*, 고 병 훈\*, 이 성 로\*\*, 김 광 순<sup>o</sup>

## Tanner Graph Based Low Complexity Cycle Search Algorithm for Design of Block LDPC Codes

Se Chang Myung\*, Ki Jun Jeon\*, Byung hoon Ko\*, Seong Ro Lee\*\*, Kwang Soon Kim<sup>o</sup>

### 요 약

본 논문은 블록 LDPC(low density parity check) 부호 설계를 위한 순환 천이 값(shift index)을 탐색하는 효율적인 알고리즘을 제안한다. 여기에는 메시지-패싱(message-passing) 기반의 순환 주기(cycle) 탐색 알고리즘과 ACE(approximate cycle extrinsic message degree) 알고리즘이 결합되어 있다. LDPC 부호 성능에 영향을 미치는 요인들에 우선순위를 두어 효율적으로 순환 천이 값을 찾을 수 있도록 했다. 이 알고리즘을 통해 기존의 탐색 알고리즘 보다 훨씬 낮은 복잡도로 행렬 저장 공간을 절약하면서 좋은 성능의 패리티 검사 행렬(parity check matrix)을 만들 수 있다.

**Key Words** : block LDPC code, shift index, cycle search algorithm, maritime satellite communication, low complexity

### ABSTRACT

In this paper, we propose a efficient shift index searching algorithm for design of the block LDPC codes. It is combined with the message-passing based cycle search algorithm and ACE algorithm. We can determine the shift indices by ordering of priority factors which are effect on the LDPC code performance. Using this algorithm, we can construct the LDPC codes with low complexity compare to trellis-based search algorithm and save the memory for storing the parity check matrix.

### I. 서 론

해양 위성 통신은 바다에서 선박과 육상, 선박과 선박 사이에 정보 교환이나 위치 추적, 긴급 의료 지원

등에 사용 되는 중요한 통신 수단이다. 지상 통신 서비스를 받기 어려운 해양에서는 신뢰도 높은 통신 채널을 확보하는 것이 중요하다. Gallager가 LDPC 부호를 제안한 이래로<sup>[1]</sup> LDPC 부호는 뛰어난 비트 오

※ 이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2011-0029321)  
 ※ 본 연구는 미래창조과학부 및 정보통신산업진흥원의 IT융합 고급인력과정 지원사업의 연구결과로 수행되었음 (NIPA-2014-H0401-14-1009)  
 ♦ First Author : The department of Electrical and Electronic Engineering, Yonsei University, myungse@yonsei.ac.kr, 학생회원  
 ° Corresponding Author : The department of Electrical and Electronic Engineering, Yonsei University, ks.kim@yonsei.ac.kr, 중신회원  
 \* 연세대학교 전기전자공학부puco201@yonsei.ac.kr, bhko@yonsei.ac.kr, 학생회원  
 \*\* 목포대학교 정보전자공학과 srlee@mokpo.ac.kr, 정회원  
 논문번호 : KICS2014-04-151, Received April 30, 2014; Revised August, 8, 2014; Accepted August 8, 2014

## II. 본 론

류율(bit error rate)과 병렬처리(parallel processing)에 의한 효율적인 인코딩(encoding)이 가능한 장점 때문에 수많은 연구들이 진행 되어 왔다. 또한 낮은 디코딩 복잡도를 갖기 때문에 현재 해양 위성 통신에서 사용되는 DVB-S2 표준 부호에도 사용되고 있다<sup>[2]</sup>. 더불어 멀티미디어 기반 해상통신 등에도 응용이 가능하고 최근 여러 분야에서 터보 코드를 대체하는 오류 정정 부호로 주목 받고 있다<sup>[3]</sup>.

LDPC 부호의 성능은 패리티 검사 행렬을 어떻게 구성하느냐에 달려있다. 이상적으로 무한한 블록 길이에 순환 주기가 없다고 가정한 LDPC 부호의 성능은 샤논 한계(Shannon limit)에 가깝다<sup>[4]</sup>. 하지만 실제 유한한 블록 길이를 갖는 테너 그래프(Tanner graph)에서는 순환 주기가 존재하기 때문에 심각한 성능 저하가 발생한다. 따라서 좋은 성능의 LDPC 부호 설계를 위해서는 패리티 검사 행렬에서 순환 주기를 탐색하여 성능 저하를 발생시키는 순환 주기들을 미리 제거해주는 것이 필요하다. 특히 짧은 길이의 순환 주기는 LDPC 부호의 폭포 영역(waterfall region)에 큰 영향을 미치고, 순환 주기가 어떻게 구성되어 있는지에 대한 연결성(connectivity)은 오류-마루(error-floor)에 영향을 미친다<sup>[5]</sup>. 또한 최근 안테나와 MCS(modulation and coding scheme)의 증가로 부호어(codeword)의 길이가 길어지면서 길이가 긴 순환 주기의 고려가 중요해졌다. 그런데 기존의 트렐리스(trellis) 순환 주기 탐색 알고리즘<sup>[6]</sup>은 긴 길이의 순환 주기를 찾으면 복잡도가 높고 메시지-패싱 기반의 순환 주기 탐색 알고리즘<sup>[7]</sup>은 복잡도는 낮지만 이진 단계(binary level)의 순환 주기 탐색만 가능한 한계가 있다.

본 논문은 순환 천이 행렬과 패리티 검사 행렬의 관계<sup>[8]</sup>를 활용하여 블록 단계(block level)에서 모든 길이의 순환 주기 탐색이 가능한 낮은 복잡도의 알고리즘을 제안한다. 이 알고리즘은 메시지-패싱 기반의 순환 주기 탐색 알고리즘<sup>[9]</sup>과 ACE 알고리즘을 결합된 형태로 패리티 검사 행렬 전체를 저장하지 않아도 되기 때문에 행렬 저장 공간 또한 절약 할 수 있다. 이 알고리즘을 활용하면 순환 주기들의 길이뿐만 아니라 개수와 ACE값들까지 고려하여 최적의 폭포 영역과 오류-마루 특성을 갖는 LDPC 부호설계를 효율적으로 할 수 있다.

본론에서는 1) 제안하는 탐색 알고리즘을 예제와 함께 간단하게 설명하고 2) 같은 크기로 확장(Lifting)했을 경우에 기존의 순환 주기 탐색 알고리즘과 제안하는 알고리즘의 계산 복잡도를 비교하여 제안하는 알고리즘의 효율성을 보였다.

### 2.1 제안하는 순환 주기 탐색 알고리즘

순환 주기 탐색은 [7]에서와 같이 테너 그래프에서 변형된 메시지-패싱 알고리즘을 사용한다. '0'과 '1'을 메시지로 변수 노드(variable node)와 검사 노드(check node)가 엣지(edge)를 통해 서로 메시지(message)를 주고받으면서 시작 노드에 연결된 한엣지 출발한 메시지가 다시 시작 노드로 돌아오면 순환 주기가 형성 된다.

[8]은 순환 천이 값을 원소로 갖는 특성 행렬을 정의하고 이 특성 행렬과 패리티 검사 행렬간의 관계를 이용하여 블록 단계에서 패리티 검사 행렬 순환 주기를 탐색할 수 있다.

[9]는 위 두 논문을 결합한 형태로 블록 단계의 특성행렬에서 주어진 패리티 검사 행렬의 모든 길이의 순환 주기와 개수를 탐색 할 수 있다.

본 논문은 여기에 [5]에서 제시한 ACE 알고리즘을 결합하여 패리티 검사 행렬의 모든 순환 주기의 길이

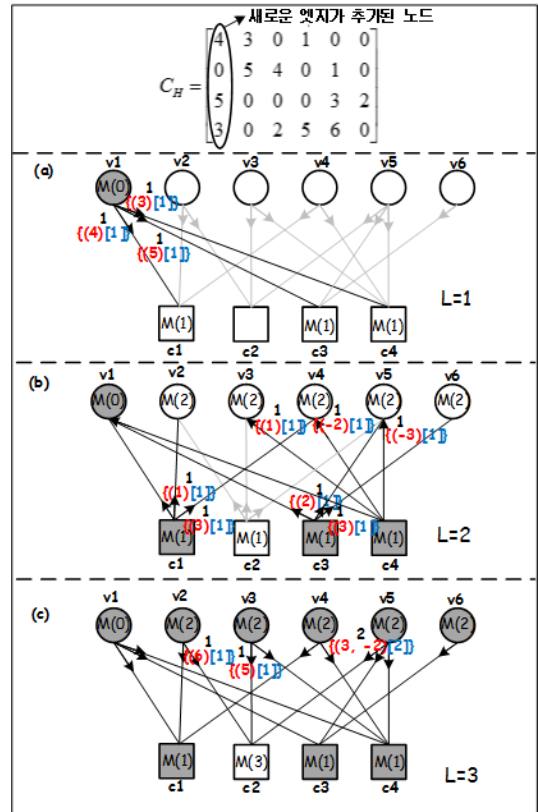


그림 1. 제안하는 탐색 알고리즘의 예제  
Fig. 1. Example of the proposed search algorithm

와 개수, ACE값 탐색할 수 있는 알고리즘을 제안한다. 성능에 더 큰 영향을 주는 요인을 고려하여 최적의 순환 천이 값을 결정한다. 블록 단계에서 모든 순환 주기 탐색이 가능하기 때문에 행렬 저장 공간을 절약할 수 있고 메시지-패싱 알고리즘을 사용하기 때문에 계산 복잡도를 크게 줄이면서 빠르고 효율적으로 LDPC 부호 설계가 가능하다.

그림 1에서 검은색 숫자는 메시지를, 소괄호 안의 빨간색 숫자는 교차 합 값을 그리고 대괄호 안의 파란색 숫자는 ACE 값을 의미한다. 여기서 ACE 값  $\eta_{ACE}$ 는 아래와 같이 정의한다.

$$\eta_{ACE} = \sum_i (d_i - 2) \quad (1)$$

여기서  $d_i$ 는  $i$ 번째 변수 노드에 연결된 엣지의 수 (degree)를 의미한다.

부호 워드의 길이와 확장(lifting)값이 정해지면 순환 천이 값의 범위가 정해진다. 이 범위 내에서 후보 순환 천이 값들을 바꿔가며 반복적으로 탐색한다. 각 순환 천이 값들로부터 다양한 길이, 개수 그리고 ACE 값을 갖는 순환 주기를 찾을 수 있고 크게 아래 3가지 경우로 분류 할 수 있다.

- (i) 길이가 서로 다른 복수의 순환 주기
- (ii) 길이가 같고 개수가 다른 복수의 순환 주기
- (iii) 길이와 개수가 같고 ACE값이 다른 복수의 순환 주기

LDPC부호 성능에 더 큰 영향을 미치는 요인을 고려하여 우선순위를 매기게 되는데 첫 번째 경우에는 순환 주기의 길이가 긴 것, 두 번째로 길이가 같다면 개수가 적은 것, 세 번째로 길이와 개수가 같다면 ACE값이 큰 순환 천이 값을 택한다.

## 2.2 기존 순환 주기 탐색 알고리즘과의 복잡도 비교

이 절에서는 간단한 예제를 통하여 패리티 검사 행렬을 구성하는 방법을 설명하고 제안하는 알고리즘을 사용하여 패리티 검사 행렬을 구성했을 때와 기존 알고리즘을 사용했을 때의 계산 복잡도를 비교해본다.

$$h = \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 2 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \quad (2)$$

$$H = \begin{bmatrix} 100110000000 \\ 010011000000 \\ 001101000000 \\ 000101100001 \\ 000110010010 \\ 000011001010 \\ 000010100100 \\ 000001010010 \\ 000100001001 \end{bmatrix} \quad (3)$$

식 (3)는 크기가  $3 \times 4$  기본 프로토타그램 (protograph)를 인접(adjacent) 행렬로 나타낸 식 (2)를  $B_1 (= 3)$ 배 확장하여 만든  $9 \times 12$  파생(derived) 그래프를 행렬로 나타낸 예제이다. 패리티 검사 행렬을 만들기 위해서는 두 번의 확장(lifting)을 수행해야 하는데 기본 프로토타그램으로부터 인접 행렬의 행과 열사이의 연결 정도 조건을 만족하는 위치 후보들의 모든 조합들을 고려하고 이와 동시에 순환 주기 탐색을 반복적으로 수행하여 1의 위치를 결정한다. 2차 확장은 파생 그래프의 해당 1의 위치에  $B_2$ 길이의 순환 행렬을 이용한다. 두 번의 확장 수행에서 제안하는 알고리즘을 활용하여 순환 주기의 길이가 길고 개수가 적으며 큰 ACE값을 갖는 순환 천이 값을 선택한다.

패리티 검사 행렬을 구성하고자 할 때 아래 세 가지 경우에 대해 계산 복잡도를 비교해보자.

- 1) 이진 PEG(progressive edge growth)와 [7]의 MP (message-passing)알고리즘을 사용할 때
- 2) 블록 PEG와 [8]의 블록 연산식과 결합된 트렐리스 (trellis) 순환 주기 탐색 방법을 사용할 때
- 3) 본 논문에서 제안하는 알고리즘을 사용할 때

먼저 블록 행렬의 크기와 패리티 검사 행렬의 크기를 각각  $m \times n$ ,  $M \times N (= Bm \times Bn)$ 으로 두었을 때, 2)와 3)의 1의 위치 후보 수는  $O(dmn)$ 이고 1)은  $O(B^2 dmn)$ 이다. 여기서  $d$ 는 열의 평균 연결정도이고  $B$ 는 확장 값이다.

$2L$ 길이의 순환주기 탐색을 위해  $L$ 번의 반복 혹은 길이  $L$ 까지 탐색할 때 후보 1의 위치마다 필요한 연산 횟수는 1)의 경우  $O(LdBm)$ 정도이고 3)은  $O(Ldm)$ 이다. 그리고 변수 노드와 검사 노드의 연결 정도를 각각  $d$ 와  $(dn/m)$ 로 가정하면 2)는  $O(d^{L-1}(n/m)^{L/2-1})$ 의 후보 경로를 검사해야 한다. 또한 1)에서 비트 하나의 논리 연산과 비교하여 [8]의 블록 연산식에 필요한 정수 연산은  $\log_2 B$ 개의 논리 연산과 비슷하고 후보 경로들의 순환 천이 값 연산에 필요한 연산 횟수와 이로부터 패리티 검사 행렬의 순환주기를 계산하는데 필요한 연산 횟수는 2)

$O(d^2nL/m\log_2B), O(\log_2B)$  3)  $O(Ldm\log_2B), O(B\log_2B)$ 이다. 따라서 최종적인 비트 논리 연산 횟수로 따진 계산 복잡도는 아래와 같다.

- 1)  $O(LB^3d^2m^2n)$
- 2)  $O[dmn\{Ld^{L+1}(n/m)^{L/2}\log_2B + B\log_2B\}]$
- 3)  $O((Ld^2m^2n + Bdmn)\log_2B)$

### III. 모의 실험 결과

이 장에서는 주어진 프로토그래프로부터 제안한 알고리즘을 사용해 실제 패리티 검사 행렬을 구성했을 때 부호의 성능과 기존의 알고리즘과의 계산 복잡도 차이를 모의실험으로 보인다.

그림 2의 예제 프로토그래프로부터 코드워드 길이 16200 및 360 비트 당 블록 병렬 처리를 위해서 부호율 1/3의 경우는  $B_1 = 15, B_2 = 360$ 으로 1차, 2차 확장을 수행하고 1/5의 경우는  $B_1 = 9, B_2 = 360$ 으로 1차, 2차 확장을 수행한다.

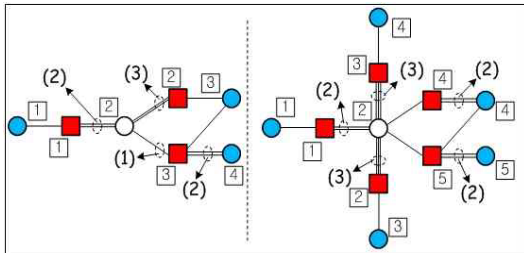


그림 2. 부호율 1/3, 1/5 프로토그래프 예제  
Fig. 2. Example of the protograph with rate 1/3 and 1/5

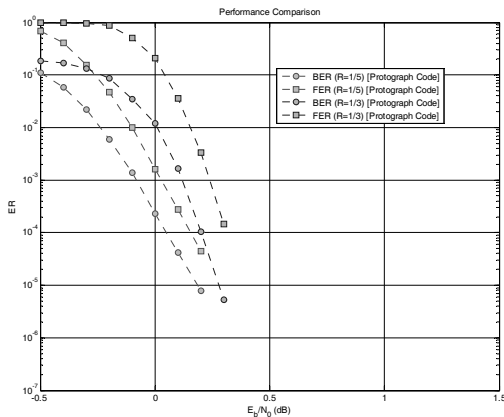


그림 3. 주어진 프로토그래프의 부호 비트오류확률/프레임 오류 확률 성능  
Fig. 3. BER/FER performance of given protograph code

그림 3은 그림 2의 프로토그래프를 제안하는 알고리즘을 사용하여 패리티 검사 행렬을 구성했을 때의 BER/FER 그래프로 좋은 폭포영역과 오류-마루 특성을 갖는다. 이 결과는 BPSK 변조를 사용하고 수신단에서 SPA 기반 최대 반복 횟수 100번 이하에서 복호 수행시 얻어지는 비트오류확률 및 프레임 오류확률에 대한 모의실험 결과로 프레임 오류 개수 200개에서의 성능 그래프이다.

표 1은 그림 2의 프로토그래프로부터 얻은 과생 그래프를  $B = 360$ 으로 2차 확장하여 패리티 검사 행렬을 구성할 때 필요한 계산 복잡도이다.

그림 4는 그림 2의 부호율 1/3 프로토그래프로부터 패리티 검사 행렬을 구성할 때 앞에서 언급한 세 가지 알고리즘을 각각 사용하여 확장 값  $B$ 에 따른 계산 복잡도를 구해본 것이다. 그래프로부터 이진 단계에서 설계하는 첫 번째 방법은  $B$ 가 커짐에 따라서 복잡도가 점점 증가하여 가장 복잡도가 높고 두 번째 트렐리스 알고리즘은 일정 확장 값 이상이면 이진 단계 설계보다 유리하지만 길이  $L$ 에 따라 복잡도 차이가 크게 났다. 제안하는 알고리즘은 확장 값이 커져도 상대적으로 낮은 계산 복잡도를 갖는 것을 확인 할 수 있다. 이상의 모의 실험 결과로부터 제안하는 알고리즘

표 1. 각 알고리즘별 비트 연산 횟수 비교  
Table 1. Comparison of the number of bit operations for each algorithm

Code rate	Binary+MP	Trellis+BL	Proposed
1/3	5.1e+14	5.3e+11	1.3e+8
1/5	4.6e+14	2.8e+11	1.2e+8

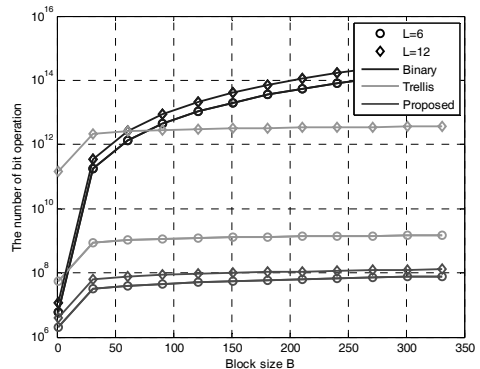


그림 4. 블록 크기 따른 비트 연산 횟수의 반로그그래프  
Fig. 4. Semilogarithmic plot of the number of bit operations as a function of block size

이 주어진 프로토타입으로부터 패리티 검사 행렬을 구성할 때 낮은 계산 복잡도로 순환 주기 탐색이 가능하고 부호 성능에 영향을 미치는 요인들을 고려하여 최적의 순환 천이 값을 결정하였기 때문에 좋은 특성을 가지는 부호를 낮은 복잡도로 설계가 가능함을 알 수 있다.

#### IV. 결 론

본 논문에서는 해양 위성 통신에 응용 가능한 블록 LDPC 부호 설계를 위한 효율적인 순환 천이 값 탐색 알고리즘을 제안하였다. 간단한 예제를 통하여 순환 천이 값 결정 방법과 기존 알고리즘 대비 제안하는 알고리즘이 갖는 장점들에 대해 설명 하였다. 또한 주어진 프로토타입으로부터 기존의 알고리즘을 사용할 때와 제안하는 알고리즘을 사용하여 패리티 검사 행렬을 만들 때의 계산 복잡도를 비교하였다. 모의실험 결과 블록 단계에서 LDPC 부호를 설계함에 있어서 기존 대비 계산 복잡도 면에서 이득을 얻을 수 있는 효율적인 알고리즘임을 보였고, 이를 이용해 성능이 우수한 LDPC 부호를 낮은 복잡도로 설계할 수 있음을 보였다.

#### References

[1] R. G. Gallager, "Low-density parity check codes," *IRE Trans. Inform. Theory*, vol. 8, no. 1, pp. 21-28, Jan. 1962.

[2] J. G. Ryu, D. G. Oh, and H. J. Yu, "Design of maritime satellite communication systems sharing frequency with DVB-S2," *J. Korea Soc. Comm. Space Tech.(KOSST)*, vol. 8, no. 4, pp. 75-80, Dec. 2013.

[3] J. W. Jung, H. C. Kwon, Y. J. Kim, S. H. Park, and S. R. Lee, "A study on high speed LDPC decoder algorithm based on DVB-S2 standard," *J. KICS*, vol. 38C, no. 03, pp. 311-317, Mar. 2013.

[4] T. Richardson, M. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 638-656, Feb. 2001.

[5] T. Tian, C. R. Jones, J. D. Villasenor, and R. D. Wesel, "Selective avoidance of cycles in

irregular LDPC code construction," *IEEE Trans. Commun.*, vol. 52, pp. 1242-1247, Aug. 2004.

[6] Y. Mao and A. H. Banihashemi, "A heuristic search for good low-density parity-check codes at short block lengths." in *Proc. IEEE Int. Conf. Commun.*, vol. 1, pp. 11-14, Helsinki, Finland, Jun. 2001.

[7] S. H. Lee, K. S. Kim, Y. H. Kim, and J. Y. Ahn, "A cycle search algorithm based on a message-passing for the design of good LDPC codes," *IEICE Trans. Fundam.*, vol. E88-A, no. 6, pp. 1955-1604, Jun. 2005.

[8] K. S. Kim, S. H. Lee, Y. H. Kim, and J. Y. Ahn, "Design of binary LDPC code using cyclic shift matrices," *Electron. Lett.*, vol. 40, no. 5, pp. 325-326, Mar. 2004.

[9] S. C. Myung, K. J. Jeon, B. H. Ko, K. J. Kim, and K. S. Kim, "A cycle search algorithm for design of block LDPC codes," in *Proc. KICS Winter Conf.*, pp. 850-851, Yongpyong, Korea, Jan. 2014.

#### 명 세 창 (Se Chang Myung)



2013년 2월 : 연세대학교 전기  
전자공학부 공학사  
2013년 3월~현재 : 연세대학교  
전기전자공학부 석사 과정  
<관심분야> 통신이론, LDPC,  
채널 코딩

#### 전 기 준 (Ki Jun Jeon)



2008년 2월 : 경희대학교 전기  
전자공학과 공학사  
2010년 2월 : 연세대학교 전기  
전자공학과 석사  
2010년 3월~현재 : 연세대학교  
전자공학과 박사과정  
<관심분야> 정보이론, 소스-채  
널 코딩, 영상 코딩

고 병 훈 (Byung hoon Ko)



2006년 8월 : 연세대학교 전기  
전자 공학부 졸업 (공학사)  
2007년 2월~현재 : 연세대학교  
전기전자공학과 석박사통합  
과정  
<관심분야> 애드혹 멀티캐스트  
네트워크, 계층 간 최적화

이 성 로 (Seong Ro Lee)

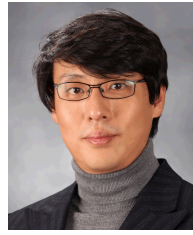


1987년 2월 : 고려대학교 전자  
공학과 공학사  
1990년 2월 : 한국과학기술원 전  
기 및 전자공학과 공학석사  
1996년 8월 : 한국과학기술원 전  
기 및 전자공학과 공학박사  
1997년 9월~현재 목포대학교

공과대학 정보전자공학과 교수

<관심분야> 디지털통신시스템, 이동 및 위성통신시  
스템, USN/텔레미틱스응용분야, 임베디드시스템,  
생체인식시스템

김 광 순 (Kwang Soon Kim)



1994년 2월 : 한국과학기술원 전  
기전산학과 공학사 (최우등)  
1996년 2월 : 한국과학기술원 전  
기전산학과 공학석사  
1999년 2월 : 한국과학기술원 전  
기전산학과 공학박사  
1999년 3월~2000년 3월 : UC

San Diego 박사 후 연구원

2000년 4월~2004년 2월 : ETRI 책임 연구원

2004년 3월~2009년 2월 : 연세대학교 전기전자공학부  
조교수

2009년 3월~현재 : 연세대학교 전기전자공학부 부교수  
<관심분야> 통신이론, 코딩 이론, LDPC부호 설계,  
하이브리드 빔 형성기, 신호 검출 이론, 이중 셀  
방식 네트워크, D2D 네트워크