http://dx.doi.org/10.7840/kics.2015.40.3.491

Griesmer 한계식을 만족하는 [2^k-1+k, k, 2^{k-1}+1] 부호 설계 및 부분접속수 분석

김 정 현•, 남 미 영*, 박 기 현*, 송 홍 엽°

Construction of [2^k-1+k, k, 2^{k-1}+1] Codes Attaining Griesmer Bound and Its Locality

Jung-Hyun Kim•, Mi-Young Nam*, Ki-Hyeon Park*, Hong-Yeop Song°

요 약

본 논문에서는 Griesmer 한계식을 만족하는 [2^k-1, k, 2^{k-1}] 심플렉스(simplex) 부호와 [2^k-1+k, k, 2^{k-1}+1] 부호를 소개한다. 또한 두 부호의 부분접속수(locality)에 대해 유도하고 그 값들을 비교한다. [2^k-1+k, k, 2^{k-1}+1] 부호는 주어진 부호차원과 최소거리에 대해 최적의 부호길이를 가질 뿐만 아니라 좋은 부분접속수 특성을 가진다. 그러므로 이 부호는 다양한 분산 저장 시스템에 널리 사용될 수 있을 것으로 기대된다.

Key Words : Distributed Storage Systems, Locality, Locally Repairable Codes, Griesmer Bound, Optimal Codes

ABSTRACT

In this paper, we introduce two classes of optimal codes, [2^k-1, k, 2^{k-1}] simplex codes and [2^k-1+k, k, 2^{k-1}+1] codes, attaining Griesmer bound with equality. We further present and compare the locality of them. The [2^k-1+k, k, 2^{k-1}+1] codes have good locality property as well as optimal code length with given code dimension and minimum distance. Therefore, we expect that [2^k-1+k, k, 2^{k-1}+1] codes can be applied to various distributed storage systems.

Ⅰ. 서 론

빅데이터(Big Data) 시대의 개막으로 최근 학계뿐만 아니라 산업체에서도 분산 저장 시스템이 주목받고 있다. 분산 저장 시스템은 시스템 내에서 빈번히 발생하는 데이터 소실을 극복하기 위해 주어진 데이터를 작은 데이터 블록으로 나누어 다수의 저장 장치에 분산 저장한다[1-2]. 따라서 동일한 저장 공간을 사용하여 최대 몇 개의 데이터 소실을 복구할 수 있는지와 데이터 복구 시 최소 몇 개의 노드에 접속해야 하는지 등이 주요한 성능 지표로 사용된다[3-5]. 특히 데이터 복구 시 필요한 최소 접속 노드 수를 부분접속수(locality)라고 부른다[6].

최근 Papailiopoulos 등에 의해 부분접속 복구 부호(Locally Repairable Code, LRC)가 제안되었다[7]. 부분접속 복구 부호는 소실된 데이터 복구 시 접속 노드

※ This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(No. 2013R1A1A2062061).
◆ First Author : School of Electrical and Electronic Engineering, Yonsei University, jh.kim06@yonsei.ac.kr, 학생회원
° Corresponding Author : School of Electrical and Electronic Engineering, Yonsei University, hysong@yonsei.ac.kr, 종신회원
* School of Electrical and Electronic Engineering, Yonsei University, my.nam@yonsei.ac.kr, kh.park@yonsei.ac.kr, 학생회원
논문번호 : KICS2014-12-493, Received December 17, 2014; Revised February 16, 2015; Accepted February 16, 2015

수, 즉, 부분접속수를 최소화하는 부호이다. [6-7] 등에서 이러한 부호의 최소거리에 대한 이론적 한계식이 제시되었다. 이 한계식의 등호를 만족하는 부호를 최적 부분접속 복구 부호라 한다. 그러나 기존의 부분접속 복구 부호에 대한 대부분의 연구들이 충분한 크기의 필드(field) 상에서 부호를 설계하고 있다. Cadambe 등은 이진 필드 상에서 이 바운드가 충분히 엄밀한 한계식이 아님을 보였다[8]. 즉, 이진 필드 상에서 특정 부호 파라미터를 갖는 최적 부분접속 복구 부호는 존재하지 않을 수 있다. 그럼에도 불구하고 시스템 상에서 연산량 최소화와 기존 하드웨어와 호환성 등의 문제로 마이크로소프트와 페이스북 등의 기업들은 이진 부분접속 복구 부호를 선호하고 있다[9,10].

본 논문에서는 부분접속 복구 부호 중의 하나인 심플렉스(simplex) 부호[11,13]의 부분접속수를 보인다. 심플렉스 부호는 Griesmer 한계식[12]을 만족한다[13]. Griesmer 한계식을 만족하는 부호는 주어진 부호차원과 최소거리에 대해, 더 작은 길이의 부호가 존재하지 않는다는 점에서 최적 부호이다. 심플렉스 부호는 Griesmer 한계식을 만족하는 최적 부호인 동시에 좋은 부분접속수 특성을 갖는다.

또한 본 논문에서는 Griesmer 한계식을 만족하는 또 다른 부호[14,15]를 소개한다. 이 부호를 IR-심플렉스(Identity Repeated simplex, IR-simplex) 부호라고 부른다. 이는 IR-심플렉스 부호의 생성 행렬이 심플렉스 부호의 생성 행렬에 항등 행렬(identity matrix)을 추가한 형태이기 때문이다. 흥미롭게도 IR-심플렉스 부호는 심플렉스 부호보다 최소거리가 1만큼 클 뿐만 아니라 평균 부분접속수가 더 좋은 특성을 갖는다. 또한 부호어의 구조가 데이터 부분을 반복하고 패리티 부분을 추가하는 형태이므로, 3회 반복(3 times repetition) 부호를 사용하는 기존의 하둡(Hadoop)[16,17]과 같은 시스템에서 일부 수정을 통해 용이하게 구현될 수 있을 것으로 기대된다.

본 논문의 구조는 다음과 같다. Ⅱ장에서는 Griesmer 한계식을 만족하는 두 가지 최적 부호들에 대해 소개한다. Ⅲ장에서는 Griesmer 한계식을 만족하는 두 가지 최적 부호들의 부분접속수를 증명을 통해 보이고, 예를 통해 서로 비교 및 분석한다. Ⅳ장에서 결론으로 논문을 마친다.

Ⅱ. Griesmer 한계식를 만족하는 최적 부호들

본 장에서는 Griesmer 한계식을 만족하는 최적 부호로 잘 알려진 심플렉스 부호를 정의하고 [14-15]에서 제안된 또 다른 최적 부호군을 소개한다. 본 논문의 남은 부분에서 $[n,k,d]_2$ 부호는 길이가 n, 차원이 k, 그리고 최소거리가 d인 이진 선형 부호를 말한다.

2.1 심플렉스 부호

정의 1. [13] 임의의 양의 정수 k에 대해, $n=2^k-1$ 그리고 G를 각 열들이 F_2^k 상에서 영벡터가 아닌 서로 다른 벡터로 정의되는 $k\times n$ 행렬이라 하자. 그리고 부호 C는 G를 생성 행렬(generating matrix)로 갖는 $[n,k,d]_2$ 부호라 하자. 이러한 부호 C를 최소거리 $d=2^{k-1}$을 갖는 심플렉스 부호라 부른다.

예제 1. $[7,3,4]_2$ 심플렉스 부호의 생성 행렬 G를 시스터매틱(systematic) 형태로 표현하면 다음과 같다.

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

2.2 IR-심플렉스 부호

정의 2. [14] G를 심플렉스 부호의 생성 행렬에 항등 행렬을 추가한 행렬이라고 하자. 즉, $G=(I\,|\,G_S)$이다. 여기서 I는 항등 행렬이고, G_S는 심플렉스 부호의 생성 행렬이다. 부호 C는 G를 생성 행렬로 갖는 $[n,k,d]_2$ 부호라 하자. 이러한 부호 C를 길이 $n=2^k-1+k$ 그리고 최소거리 $d=2^{k-1}+1$을 갖는 IR-심플렉스 부호라 부른다.

IR-심플렉스 부호의 최소거리가 $d=2^{k-1}+1$이 됨은 부호어의 해밍 무게(Hamming weight)를 통해 확인할 수 있다. IR-심플렉스 부호의 부호어를 $c=(m\,|\,s)$로 두 부분으로 나누어 표현하자. 여기서 s는 심플렉스 부호어에 해당되고 m은 부호어 c의 나머지 부분에 해당한다. s의 모든 해밍 무게는 2^{k-1}이고 m의 최소 해밍 무게는 1이므로 IR-심플렉스 부호의 최소거리는 $d=2^{k-1}+1$이 된다.

이러한 IR-심플렉스 부호는 [15]에서 정의한 Griesmer 한계식을 만족하는 최적 부호군의 특수한 형태이다.

예제 2. $[10,3,5]_2$ IR-심플렉스 부호의 생성 행렬 G를 시스터매틱(systematic) 형태로 표현하면 다음과 같다.

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

Ⅲ. Griesmer 한계식를 만족하는 최적 부호들의 부분접속수

정의 3. [6] C는 $[n,k,d]_2$ 부호라 하자. 임의의 정수 $i\in\{1,2,...,n\}$에 대해, C의 부호화된 심볼 Y_i가 다음 조건을 만족한다고 하자.

$$Y_i=\sum_{j\in R(i),\,R(i)\subseteq\{1,2,...,n\}\setminus\{i\}}\alpha_j\bullet Y_j, \quad (3)$$

여기에서 $\alpha_j\in F_2$이다. 그러면 이러한 $R(i)$를 Y_i의 복구 집합(repair set)이라고 한다.

특정 심볼 Y_i의 복구 집합은 여러 개 존재할 수 있으며 그 중 가장 작은 크기를 갖는 복구 집합의 원소의 수를 심볼 Y_i의 부분접속수라고 한다. 또한 모든 심볼의 부분접속수 중 가장 큰 값을 부호 C의 부분접속수라고 한다.

[11]에서 모든 심플렉스 부호의 부분접속수는 2임을 보였다. 본 논문에서는 IR-심플렉스 부호의 부분접속수가 2임을 보인다. 증명의 간략화를 위하여 다음과 같이 부호화된 심볼과 생성 행렬의 각 열 사이의 관계를 이용한다.

C는 G를 생성행렬로 갖는 $[n,k,d]_2$ 부호라 하자. G를 열벡터들로 표현하면 $G=(g_1,g_2,...,g_n)$이다. 그리고 $X=(x_1,x_2,...,x_k)$를 부호화되기 전의 심볼 벡터라고 하자. 만약 G의 열벡터 g_i에 대해

$$g_i=\sum_{j\in R(i),\,R(i)\subseteq\{1,2,...,n\}\setminus\{i\}}\alpha_j\bullet g_j \quad (4)$$

이면

$$\begin{aligned}&X\bullet g_i=X\bullet\sum_{j\in R(i),\,R(i)\subseteq\{1,2,...,n\}\setminus\{i\}}\alpha_j\bullet g_j\\&=X\bullet\sum_{j\in R(i),\,R(i)\subseteq\{1,2,...,n\}\setminus\{i\}}\alpha_j\bullet X\bullet g_j\\&\Rightarrow Y_i=\sum_{j\in R(i),\,R(i)\subseteq\{1,2,...,n\}\setminus\{i\}}\alpha_j\bullet Y_j\end{aligned} \quad (5)$$

여기에서 $\alpha_j\in F_2$이다. 따라서 위 관계를 토대로 부호화된 심볼들 대신 생성 행렬의 열들의 관계를 이용하여 복구 집합을 정의하고 부분접속수를 구할 수 있다.

정리 1. C는 $[n,k,d]_2$ IR-심플렉스 부호라 하자. 그러면 C의 부분접속수는 2이다.

증명. C의 생성 행렬 G를 두 개의 항등 행렬 부분과 나머지 부분으로 나누어 정렬한다. 즉, $G=(I|I|P)$이다. 이제 임의의 열벡터 g_i를 선택하자. 우리는 다음의 두 경우를 나누어 생각할 수 있다.

경우 1) $i\in\{1,2,...,2k\}$

이 경우, 모든 g_i들은 g_j, $j\equiv(i+k)\bmod(2k)$에 의해 표현될 수 있다. 따라서 Y_i의 부분접속수는 1이다.

경우 2) $i\in\{2k+1,2k+2,...,n\}$

이 경우, 모든 g_i들은 G에서 유일하므로 하나의 다른 열벡터로 표현될 수 없다. 즉, g_i를 표현하기 위해서는 두 개 이상의 열벡터들이 필요하다. 임의의 열벡터 g_{j_1}, $j_1\in\{1,2,...,2k\}$를 선택하자. 그러면 $j_2\neq i$인 $g_{j_2}=g_i+g_{j_1}$가 결정된다. 이제 이러한 g_{j_1}와 g_{j_2}를 이용하여 g_i를 표현할 수 있다. 즉,

$$g_i=g_{j_1}+g_{j_2}=g_{j_1}+\left(g_i+g_{j_1}\right).$$

따라서 Y_i의 부분접속수는 2이다.

종합하면, 두 경우에서 최대 부분접속수인 2가 부호 C의 부분접속수가 된다.

다음 표는 앞서 언급한 심플렉스 부호와 IR-심플렉스 부호, 그리고 현재 하둡 시스템에서 기본적으로 사용되는 3회 반복 부호의 부분접속수 분포를 나타낸 것이다.

위의 표 1.을 토대로 부호차원이 3인 경우에 부호별 특성에 대해 살펴보자. 이때 3회 반복 부호를 위해 사용된 생성 행렬은 다음과 같다.

표 1. 3회 반복 부호, 심플렉스 부호, IR-심플렉스 부호의 부분접속수 분포
Table 1. Locality distribution of 3 times repetition codes, simplex codes, and IR-simplex codes

Number of symbols with locality r	$r=1$	$r=2$
3 times repetition codes	n	
simplex codes		n
IR-simplex codes	$2k$	$n-2k$

$$G=\begin{bmatrix}1\,0\,0\,1\,0\,0\,1\,0\,0\\0\,1\,0\,0\,1\,0\,0\,1\,0\\0\,0\,1\,0\,0\,1\,0\,0\,1\end{bmatrix} \quad (6)$$

$[9,3,3]_2$ 3회 반복 부호, $[7,3,4]_2$ 심플렉스 부호, $[10,3,5]_2$ IR-심플렉스 부호의 최소거리는 각각 3, 4, 5이므로, 복구 가능한 최대 소실 심볼의 수는 각각 2, 3, 4로 IR-심플렉스 부호가 가장 크다. 반면, 세 부호의 부분접속수는 각각 1, 2, 2이다. 따라서 부분접속수 측면에서는 3회 반복 부호가 가장 우수하다. 주목할 점은 심플렉스 부호는 모든 심볼에 대해 부분접속수가 2로 일정하지만, IR-심플렉스 부호는 부분접속수가 1인 심볼과 부분접속수가 2인 심볼이 모두 존재한다는 점이다. 특히 $[10,3,5]_2$ IR-심플렉스 부호의 경우 전체 10개 중 6개의 심볼이 부분접속수 1을 갖고 나머지 4개의 심볼이 부분접속수 2를 갖는다.

이로부터 우리는 특정 부호의 부분접속수 특성을 고려할 때 심볼들의 부분접속수 중 최댓값뿐만 아니라 평균값도 비교하는 것이 더욱 효과적임을 알 수 있다. 예를 들어, $[7,3,4]_2$ 심플렉스 부호의 평균 부분접속수는 2이지만 $[10,3,5]_2$ IR-심플렉스 부호의 평균 부분접속수는 1.4이다. 즉, $[10,3,5]_2$ IR-심플렉스 부호는 $[7,3,4]_2$ 심플렉스 부호에 비하여 임의의 심볼 복구 시 필요한 심볼의 수를 평균적으로 30% 감소시킬 수 있다.

Ⅳ. 결 론

본 논문에서는 Griesmer 한계식을 만족하는 두 가지 최적 부호군들에 대해 소개하고, 이들의 부분접속수를 증명을 통해 보였다. 또한 예제를 통하여, 기존 연구들에서 주로 다루는 부분접속수뿐만 아니라 평균 부분접속수를 고려하는 것이 효과적임을 확인하였다.

특히 본 논문에서 소개된 IR-심플렉스 부호는, 최근 낮은 복잡도와 낮은 부분접속수를 갖는 부분접속 복구 부호로 주목받고 있는 심플렉스 부호보다 더 좋은 부분접속수 특성을 보이며 복구 가능한 최대 소실 심볼의 수도 1만큼 더 크다. 따라서 심플렉스 부호 대비 부호차원만큼의 저장 공간의 증가가 크게 문제되지 않는 시스템이라면 효과적으로 사용될 수 있을 것으로 기대된다. 또한 부호어의 구조가 데이터 부분을 반복하고 패리티 부분을 추가하는 형태이므로, 3회 반복 부호를 사용하는 기존의 하둡과 같은 시스템에서 일부 수정을 통해 용이하게 구현될 수 있을 것으로 기대된다.

본 논문의 결과를 토대로 향후 추가 연구로서 (1) 다양한 Griesmer 한계식을 만족하는 일반적인 형태의 부호군들, $d > 2^{k-1}$인 부호군[17]과 $d \le 2^{k-1}$인 부호군[18]에 대한 부분접속수 분석, (2) Hamming 한계식, Singleton 한계식 등 기존의 이론적 한계식[13]을 만족하는 부호들에 대한 부분접속수 분석, (3) 우수한 부분접속수를 갖는 새로운 부호의 설계 등을 고려할 수 있다.

References

[1] J.-C. Park, "Improving data availability by data partitioning and partial overlapping on multiple cloud storages," *J. KICS*, vol. 36, no. 12, Nov. 2011.

[2] T.-H. Kim, J. Kim, and Y. I. Eom, "A scheme on high-performance caching and high-capacity file transmission for cloud storage optimization," *J. KICS*, vol. 37C, no. 8, Aug. 2012.

[3] J.-H. Kim, J. S. Park, K.-H. Park, M. Y. Nam, and H.-Y. Song, "Trends of regenerating codes for next-generation cloud storage systems," *Inf. Commun. Mag.*, vol. 31, no. 2, pp. 125-131, Feb. 2014.

[4] J.-H. Kim and H.-Y. Song, "Coding techniques for distributed storage systems," in *Proc. 2013 CITS 3rd CITW*, Samsung Electronics, Seoul, Korea, Oct. 2013.

[5] J. S. Park, J.-H. Kim, K.-H. Park, and H.-Y. Song, "Average repair read cost of linear repairable code ensembles," *J. KICS*, vol. 39B, no. 11, Nov. 2014.

[6] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, "On the locality of codeword symbols," *IEEE Trans. Inform. Theory*, vol. 58, no. 11, pp. 6925-6934, Nov. 2012.

[7] D. S. Papailiopoulos and A. G. Dimakis, "Locally repairable codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 5843-5855, Oct. 2014.

[8] V. Cadambe and A. Mazumdar, "An upper bound on the size of locally recoverable

codes," in *Proc. IEEE Int. Symp. Netw. Coding*, pp. 1-5, Calgary, Canada, Jun. 2013.

[9] C. Huang, H. Simitci, Y. Xu, A. Ogus, B. Calder, P. Gopalan, J. Li, and S. Yekhanin, "Erasure coding in Windows Azure Storage," in *Proc. 2012 USENIX Annu. Technical Conf.*, pp. 1-12, Boston, USA, Jun. 2012.

[10] M. Sathiamoorthy, M. Asteris, D. Papailiopoulos, A. G. Dimakis, R. Vadali, S. Chen, and D. Borthakur, "XORing Elephants: novel erasure codes for Big Data," in *Proc. 39th Int. Conf. Very Large Data Bases*, vol. 6, no. 5, pp. 325-336, Trento, Italy, Aug. 2013.

[11] M. Kuijper and D. Napp, *Erasure codes with simplex locality*(2014), Last access(Feb. 16, 2015), http://arxiv.org/abs/1403.2779.

[12] J. H. Griesmer, "A bound for error-correcting codes," *IBM J. Res. Develop.*, vol. 4, pp. 532-542, Nov. 1960.

[13] W. C. Huffman and V. Pless, *Fundamentals of error correcting codes*, Cambridge, 2003.

[14] J.-H. Kim and H.-Y. Song, "Simple construction of [2^k-1+k, k, 2^{k-1}+1] code attaining the Griesmer bound," in *Proc. 9th Joint Conf. Commun. & Inf.*, pp. 420-422, Icheon, Korea, Apr. 1999.

[15] T. Helleseth, "New constructions of codes meeting the Griesmer bound," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 434-439, Mar. 1983.

[16] M. N. Krishnan, N. Prakash, V. Lalitha, B. Sasidharan, P. V. Kumar, S. Narayanamurthy, R. Kumar, and S. Nandi, "Evaluation of codes with inherent double replication for Hadoop," in *Proc. 6th USENIX Workshop on Hot Topics in Storage and File Systems*, pp. 1-5, Philadelphia, USA, Jun. 2014.

[17] M. Shahabinejad, M. Khabbazian, and M. Ardakani, "An efficient binary locally repairable code for Hadoop distributed file system," *IEEE Commun. Lett.*, vol. 18, no. 8, pp. 1287-1290, Aug. 2014.

[18] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*, North-Holland Mathematical Library, 1977.

김 정 현 (Jung-Hyun Kim)

2006년 8월 : 연세대학교 전기전자공학과 졸업
2008년 8월 : 연세대학교 전기전자공학과 석사
2010년 7월~2013년 2월 : 한국전자통신연구원 연구원
2013년 3월~현재 : 연세대학교 전기전자공학과 박사과정
<관심분야> 통신공학, 정보이론, 부호이론, 분산저장시스템

남 미 영 (Mi-Young Nam)

2005년 2월 : 연세대학교 전기전자공학과 졸업
2005년 2월~2007년 8월 : 삼성전자 연구원
2009년 8월 : 연세대학교 전기전자공학과 석사
2009년 9월~현재 : 연세대학교 전기전자공학과 박사과정
<관심분야> 통신공학, 정보이론, 부호이론, 분산저장시스템

박 기 현 (Ki-Hyeon Park)

2007년 2월 : 연세대학교 전기전자공학과 졸업
2009년 2월 : 연세대학교 전기전자공학과 석사
2009년 3월~현재 : 연세대학교 전기전자공학과 박사과정
<관심분야> 통신공학, 정보이론, 암호이론, 이산수학

송 홍 엽 (Hong-Yeop Song)

1984년 2월 : 연세대학교 전자공학과 졸업
1986년 5월 : University of Southern California Dept. of EE. Systems 석사
1991년 12월 : University of Southern California Dept. of EE. Systems 박사
1992년 1월~1993년 12월 : Post-Doc Research Associate, University of Southern California Dept. of EE. Systems
1994년 1월~1995년 8월 : Senior Engineer, Qualcomm Inc., San Diego, California.
2002년 3월~2003년 2월 : Visiting Professor, University of Waterloo, Canada
1995년 9월~현재 : 연세대학교 전기전자공학과 교수
<관심분야> 통신공학, 정보이론, 부호이론, 암호이론, 이산수학