https://doi.org/10.7840/kics.2020.45.4.639

맥도날드 부호의 협력 부분접속수

Zhi Jing◆, 최 효 정°, 송 홍 엽*

Cooperative Locality of MacDonald Codes

Zhi Jing◆, Hyojeong Choi°, Hong-Yeop Song*

요 약

맥도날드 부호(MacDonald code)는 잘 알려진 부분접속 복구 부호(locally repairable code)이다. 지금까지 이 부호의 부분접속수(locality)는 2 또는 3임이 잘 알려져 있다. 이는 단일 소실(single failure) 심볼을 복구하기 위한 부분접속수 이다. 최근 여러 소실 심볼을 복구하기 위한 협력 부분접속수(cooperative locality)에 대한 논의가 활발하다. 본 논문에서는 맥도날드 부호에서 두 소실(double failures) 심볼을 복구하기 위한 협력 부분접속수가 3 또는 4임을 찾고 이를 증명한다.

Key Words : Distributed storage system, Locally repairable code, Locality, Cooperative locality, Availability, Simplex codes, MacDonald codes

ABSTRACT

MacDonald codes is a well-known example of locally repairable codes. The locality of this code is known to be either 2 or 3. This is the locality for single failure. Recently, cooperative locality of the codes has been studied for multiple failures. In this paper, we calculate and prove that the cooperative locality for double failures of the MacDonald codes is 3 or 4.

Ⅰ. 서 론

최근 빅데이터(big data)의 중요성이 대두되면서, 분산 저장 시스템에 막대한 양의 데이터를 안정적이고 효율적으로 저장하는 기법이 요구되고 있다. 분산 저장 시스템에서는 노드의 손실로 인한 데이터의 소실을 극복하기 위해 오류정정 부호가 사용된다. 가장 간단한 방법인 반복 부호(Repetition codes)[1]는 가장 낮은 계산 복잡도를 갖지만 저장 공간 오버헤드 측면에서 비효율적이다. 최대 거리 분리 가능(Maximum distance separable)[1]부호는 최소한의 저장 공간 오버헤드를 갖지만 손실된 노드를 복구하기 위한 훨씬 더 많은 노드에 접속해야 하는 단점이 있다.

단일 노드 손실은 전체 손실의 최대 98%를 구성하기 때문에[2], 부분접속으로도 복구 가능한 부분접속복구 부호(locally repairable codes, LRCs)[3]가 제안되었다. 부분접속복구 부호의 중요한 지표인 부분접속수(Locality)[3]는 단일 노드 손실을 복구하기 위해 필요한 최소 노드의 수를 의미하고 부호 C의 각 심볼들이 최대 r의 부분접속수를 갖는다면 그 부호 C는 부분접속수 r을 갖는다고 한다. 이진 부분접속복구 부호를 설계하는 다양한 방법들에는 t-스프레드[4], 그래프[5],

※ 이 성과는 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2017R1A2B4011191).
◆ First Author : Yonsei University School of Electrical and Electronic Engineering, z.jing@yonsei.ac.kr, 학생(석박통합과정), 학생회원
° Corresponding Author : Yonsei University School of Electrical and Electronic Engineering, hjchoi3022@yonsei.ac.kr, 학생(석사과정), 학생회원
* School of Electrical and Electronic Engineering, hysong@yonsei.ac.kr, 정교수, 종신회원
논문번호 : KICS201911-318-A-RN, Received November 25, 2019; Revised January 18, 2020; Accepted January 22, 2020

부호 변형(code modification)[6,7]을 이용한 방법이 있다.

분산 저장 시스템의 규모가 증가하면서 다중 노드 소실이 동시에 발생하는 경우도 고려해야 하므로 또 다른 지표로서 가용도(availability)[6]와 협력 부분접속수(cooperative locality)가 있다. 임의의 한 심볼이 다른 심볼들로 구성된 t개의 분리된 복구 집합들로부터 각각 복구가 가능하다면 (r,t)-가용도를 갖는다고 하고[6] 만약 부호 C의 각 심볼이 최대 r의 부분접속수를 갖으면서 최소 t의 가용도를 갖는다면 그 부호 C는 (r,t)-가용도를 갖는다고 한다. 이를 기반으로 부분접속수와 가용도에 대한 연구가 활발히 진행되고 있다[3,8-12]. 한 심볼 이상의 동시 장애가 발생한 경우 하나 이상의 노드의 복구를 위한 노드 수를 의미하는 지표인 (r,l)-협력 부분접속수[8]는 부분접속수의 일반화된 개념으로 제안되었으며, 부호 C가 (r,l)-협력 부분접속수를 갖는다는 것은 l개 심볼들의 임의의 집합이 최대 r개의 다른 심볼들로 복구될 수 있음을 의미한다. 본 논문에서는 표현을 간단하게 통일하기 위해 (r,l)-협력 부분접속수를 r_l로, 기존의 부분접속수 r을 r_1로 표현한다. (r,l)-협력 부분접속수 r_l과 기존의 부분접속수 r_1은 l의 단일 값만 고려한다. 이후 단일 값 l대신에 다수의 l값을 고려하는 개념인 결합 부분접속수(joint locality)[9]가 제안되었고, 결합 부분접속수에 대한 몇 가지 결과들이 연구되었다[6,9].

심플렉스 부호는 좋은 부분접속수와 가용도로서 주목을 받아 왔다. 그러나 심플렉스 부호는 아주 낮은 부호율을 갖는 단점이 있기 때문에 심플렉스 부호의 블록-펑쳐링(block-puncturing)과 서브블록-펑쳐링(subblock‐puncturing)에 의해 새로운 LRC가 제안되었다[6]. 펑쳐드 심플렉스 부호인 맥도날드 부호는 심플렉스 부호보다 더 좋은 부호율을 갖는다. $[2^k-2^m,k,2^{k-1}-2^{m-1}]$ 맥도날드 부호는 $m<k-1$일 때 $r_1=2$이고 $m=k-1$일 때 $r_1=3$으로 좋은 부분접속수를 갖는다[11]. 따라서 본 논문에서는 두 소실 심볼에 대한 맥도날드 부호의 협력 부분접속수 r_2를 분석한다.

본 논문의 구조는 다음과 같다. Ⅱ장에서는 부분접속복구 부호와 맥도날드 부호를 간단하게 소개한다. Ⅲ장에서는 맥도날드 부호의 협력 부분접속수 r_2를 계산한다. 그리고 Ⅳ장에서의 결론으로 본 논문을 마친다.

Ⅱ. 부분접속복구 부호와 맥도날드 부호

$[a,b]=\{i\in Z^+|a\le i\le b\}$, $[n]=[1,n]$라고 하자. 0_n^T와 1_n^T는 길이가 n이며, 각각 모든 원소가 0이고 모든 원소가 1인 열벡터라고 하자. 이진 $[n,k,d]$ 선형부호 C는 부호 길이가 n, 차원이 k, 최소거리 d를 갖는다. C의 생성행렬은 $G=[g_1,g_2,\cdots,g_n]$이며, 여기서 $g_i\in F_2^k$는 $i\in[n]$에 대한 열벡터 이다. $\boldsymbol{c}=(c_1,c_2,\cdots,c_n)$는 길이가 n인 이진 행벡터이다.

부호 C의 부분접속수는 생성행렬 G로부터 얻을 수 있다[11]. 부호화된 심볼 c_i가 부분접속수 r을 갖는다는 것은 $c_i=c_{l_1}+c_{l_2}+\cdots+c_{l_r}$를 의미하고, $\{c_{l_1},c_{l_2},\cdots,c_{l_r}\}$은 c_i의 복구집합이라고 한다. $\boldsymbol{u}$를 정보벡터라고 할 때 다음과 같이 나타낼 수 있다.

$$c_i=\boldsymbol{u}\cdot g_i=\boldsymbol{u}(g_{l_1}+g_{l_2}+\cdots+g_{l_r}) \tag{1}$$

그러므로 생성행렬 G로부터 부분접속수 r을 얻을 수 있다.

정의 1[6,8] $[n,k,d]$ 부호 C는 $|S|=l$인 각각의 모든 $S\subset[n]$에 대해 다음을 만족하는 집합 $\Gamma_S\subseteq[n]\setminus S$를 갖는다면 협력 부분접속수 r_l을 갖는다.

1. $|\Gamma_S|\le r_l$,
2. 임의의 부호어 $\underline{c}=(c_1,c_2,\cdots,c_n)\in C$ 에 대해서, l개 부호 심볼들 $c_S:=\{c_i:i\in S\}$은 부호 심볼들 $c_{\Gamma_S}:=\{c_i:i\in\Gamma_S\}$의 함수이다.

정의 2[6,9] C를 $[n,k,d]$ 부호라고 하자. 만약 카디날리티 l의 모든 심볼 집합 $\{i\}$가 최대 r_l의 부분접속수를 갖는다면 정수들의 집합 $\{(r_l)_i|\,l\in J,J\subseteq\{1,2,\cdots,d-1\},|J|\ge 2\}$은 C의 결합 부분접속수라 한다.

k가 양의 정수일 때 C_k는 $[2^k-1,k,2^{k-1}]$ 심플렉스 부호이고 $\boldsymbol{c}=(c_1,c_2,\cdots,c_n)$는 C_k의 부호어라고 하자. 생성행렬 S_k는 크기가 $k\times(2^k-1)$이고, 다음의 재귀에 의해 얻을 수 있다.

먼저, 초기행렬은 $S_1=(1)$, 그리고

$$S_k=\begin{pmatrix} S_{k-1} & 0_{k-1}^T & S_{k-1} \\ 0_{2^{k-1}-1} & 1 & 1_{2^{k-1}-1}\end{pmatrix},\ \text{for}\ k=2,3,\cdots. \tag{2}$$

다음 논의에 대한 편의를 위해, $S_k\equiv(A\ \ B)$라 하자.

$$A=\begin{pmatrix} S_{k-1} \\ 0_{2^{k-1}-1} \end{pmatrix},\ B=\begin{pmatrix} 0_{k-1}^T & S_{k-1} \\ 1 & 1_{2^{k-1}-1} \end{pmatrix} \quad (3)$$

보조정리 1[12] $[n,k]$ 심플렉스 부호 C_k는 부분접속수 $r_1=2$과 가용도 $t=2^{k-1}-1$를 갖는다.

정의 3[11] $k \geq 3$이고 $1 \leq m \leq k-1$라 하자. S_k로부터 처음 2^m-1개의 열을 삭제한 결과행렬을 $G_k(m)$로 표기한다. $G_k(m)$에 의해 생성된 부호 $M_k(m)$는 $[2^k-2^m,k,2^{k-1}-2^{m-1}]$ 맥도날드 부호라 부른다.

보조정리 2[11] 맥도날드 부호 $M_k(m)$는 $m<k-1$ 일 때 $r_1=2$, $m=k-1$일 때 $r_1=3$의 부분접속수를 갖는다.

정의 3으로부터 각 맥도날드 부호 $M_k(m)$는 S_k에 의해 생성된 해당 심플렉스 부호 C_k를 갖는다. 논의의 편의를 위해 $M_k(m)$의 표기는 대응하는 심플렉스 부호 C_k를 따를 것이다. $M_k(m)$의 생성행렬을 $G_k(m)=(g_{2^m},g_{2^m+1},\cdots,g_{2^k-1})$라 하고 부호어를 $\boldsymbol{c}=(c_{2^m},c_{2^m+1},\cdots,c_{2^k-1})$라 하자. 여기서 g_i는 S_k의 i번째 열이고 c_i는 C_k의 i번째 열이다.

예제 1 부호율이 $3/7$인 [7,3,4]심플렉스 부호로부터 정의 3에 따라서 $k=3$이고 $m=1$일 때 부호율이 $3/6$로 향상된 [6,3,3] 맥도날드 부호를 생성하기 위해 S_3으로부터 첫째 열을 삭제하여 생성행렬 $G_3(1)$을 얻을 수 있다.

$$G_3(1)=\begin{pmatrix} 0\,1\,0\,1\,0\,1 \\ 1\,1\,0\,0\,1\,1 \\ 0\,0\,1\,1\,1\,1 \end{pmatrix} \quad (4)$$

$G_3(1)=(g_2,g_3,\cdots,g_7)$에서 $g_2=g_4+g_6$, $g_3=g_5+g_6$, $g_4=g_2+g_6$, $g_5=g_2+g_7$, $g_6=g_2+g_4$, $g_7=g_2+g_5$이므로 [6,3,3] 맥도날드 부호는 부분접속수 $r_1=2$를 갖는다.

Ⅲ. 맥도날드 부호의 협력 부분접속수

이제 본 논문의 가장 중요한 정리를 설명하고 이를 증명하겠다.

정리 1 맥도날드 부호 $M_k(m)$는 $m<k-1$일 때 $r_2=3$이고 $m=k-1$이고 $k \geq 4$일 때 $r_2=4$의 협력 부분접속수를 갖는다.

주의 : $k=3$와 $m=k-1=2$일 때 맥도날드 부호 $M_3(2)$는 최소거리가 2를 갖는다. 따라서 손실된 두 개의 심볼들은 복구할 수 없다. 그러므로 $m=k-1$의 경우 k가 4이면 충분하다.

심플렉스 부호의 복구 집합을 관찰하면 두 가지 규칙이 적용된다. 심플렉스 부호의 c_i 심볼에 대해, 인덱스 i가 식 (3)에서 A의 열 인덱스에 해당하는 $i\in[2^{k-1}-1]$라면 A의 열 인덱스를 갖는 심볼들로만 구성되거나 B의 열 인덱스를 갖는 심볼들로만 구성된 복구집합을 갖는다. c_i의 인덱스 i가 식 (3)에서 B의 열 인덱스에 해당하는 $i\in[2^{k-1},2^k-1]$라면 A의 열 인덱스를 갖는 심볼 하나와 B의 열 인덱스를 갖는 심볼 하나로 구성된 복구집합들을 갖는다.

증명) 증명의 요점은 해당 심플렉스 부호의 각 심볼에 대한 다중 복구집합을 활용하는 것이다. S_k에서 일부의 열을 삭제한 후 심플렉스 부호의 각 심볼에 대한 일부 복구집합이 유효하지 않게 된다. 이를 유효하지 않은 복구집합이라고 한다. c_i와 c_j는 $M_k(m)$의 임의의 소실된 심볼들이라고 가정하자.

먼저, $m<k-1$ 일 때 식 (3)에서 1) i,j가 모두 A의 열 인덱스에 해당하는 경우, 2) i,j가 모두 B의 열 인덱스에 해당하는 경우, 3) i는 A의 열 인덱스에 해당하고 j는 B의 열 인덱스에 해당하는 세 가지 경우로 나눌 수 있다 :

경우1) $2^m \leq i,j \leq 2^{k-1}-1$

경우2) $2^{k-1} \leq i,j \leq 2^k-1$

경우3) $2^m \leq i < 2^{k-1} \leq j \leq 2^k-1$

경우 1) 심플렉스 부호의 복구 집합들의 구성의 규칙에 따라 $c_{2^{k-1}},c_{2^{k-1}+1},\cdots,c_{2^k-1}$는 모두 c_i와 c_j의 유효한 복구 집합에 있다. 따라서 c_i의 복구집합 $\{c_\alpha,c_\beta\}$가 α,β는 $\alpha,\beta\in[2^{k-1},2^k-1]$에 대해서 존재한다. 그러면 c_j의 한 복구집합 $\{c_\alpha,c_\gamma\}$가 존재한다. 여기서 γ는 $\gamma\in[2^{k-1},2^k-1]\setminus\{\beta\}$이다. 그러므로 c_i와 c_j는 $c_\alpha,c_\beta,c_\gamma$에 의해 복구될 수 있다.

경우 2) 경우 1과 비슷한 방법으로 $c_{2^m}, c_{2^m+1}, \cdots, c_{2^{k-1}-1}$는 모두 c_i와 c_j의 유효한 복구 집합에 있다. c_i의 복구집합 $\{c_\alpha, c_\beta\}$가 존재한다. 여기서 $\alpha \in [2^m, 2^{k-1}-1]$이고 $\beta \in [2^{k-1}, 2^k-1] \setminus \{i,j\}$이다. 그러면 c_j의 한 복구집합 $\{c_\alpha, c_\gamma\}$가 $\gamma \in [2^{k-1}, 2^k-1] \setminus \{i,j,\beta\}$에 대해 존재한다. 그러므로 c_i와 c_j는 $c_\alpha, c_\beta, c_\gamma$에 의해 복구될 수 있다.

경우 3) $2^{k-1} \le j \le 2^k-1$에 대해서 $x \in [2^m, 2^{k-1}-1] \setminus \{i\}$인 각 심볼 c_x들은 c_j의 서로 다른 유효 복구집합에 각각 속해있다. c_j의 $\alpha \in [2^m, 2^{k-1}-1] \setminus \{i\}$와 $\beta \in [2^{k-1}, 2^k-1] \setminus \{j\}$인 한 복구집합 $\{c_\alpha, c_\beta\}$이 존재한다. 그러면 $2^m \le i \le 2^{k-1}$에 대해서 $x \in [2^{k-1}, 2^k-1] \setminus \{j\}$인 각 심볼 c_x들은 c_i의 유효복구집합 안에 각각 속해있고, c_i에 대한 $\gamma \in [2^{k-1}, 2^k-1] \setminus \{j,\beta\}$인 한 복구집합 $\{c_\beta, c_\gamma\}$이 존재한다. 그러므로 c_i와 c_j는 $c_\alpha, c_\beta, c_\gamma$에 의해 복구될 수 있다.

다음으로 $m=k-1$이면서 $k \ge 4$경우를 증명한다. c_i와 c_j가 C_k의 손실된 두 심볼로 볼 때 선형결합 $g_i = g_\alpha + g_\beta$가 존재한다. 여기서 α, β는 $\alpha \in [2^{k-1}-1]$이고 $\beta \in [2^{k-1}, 2^k-1] \setminus \{j\}$이다. S_k로부터 처음 $2^{k-1}-1$ 열들을 삭제하기 때문에 g_α는 $G_k(m)$의 열이 아니다. 그러나 $g_\alpha = g_{\alpha'} + g_{\alpha''}$를 만족시키는 $g_{\alpha'}, g_{\alpha''} \in B \setminus \{g_i, g_j, g_\beta\}$인 $g_{\alpha'}$와 $g_{\alpha''}$가 존재한다. 그래서 $g_i = g_\alpha + g_\beta$이다. 그러면, $g_\gamma = g_j + g_{\alpha'} + g_{\alpha''}$이라고 하자. $g_j + g_{\alpha'} + g_{\alpha''}$의 마지막 원소는 1이기 때문에 $g_\gamma \in G_k(m)$이다. 또한 $G_k(m)$에 적어도 8열이 남아있게 되므로 $g_i \ne g_j, g_\gamma \ne g_\beta$이고 $g_\beta \ne g_j, g_\gamma \ne g_i$이고 $g_{\alpha'}(\text{or } g_{\alpha''}) \ne g_j, g_\gamma \ne g_{\alpha''}(\text{or } g_{\alpha'})$이 가능하다. 그리고$g_\alpha$는 영벡터가 아니기 때문에 $g_\gamma \ne g_j$이고, g_γ는 $G_k(m)$에 존재하며 이는 $g_j = g_\gamma + g_{\alpha'} + g_{\alpha''}$를 만족시킨다. 그러므로 g_i와 g_j는 $g_{\alpha'}, g_{\alpha''}, g_\beta$ 그리고 g_γ의 선형 결합이다. ■

Ⅳ. 결 론

본 논문에서는, 심플렉스 부호보다 높은 부호율을 갖는 맥도날드 부호의 동시 노드 소실을 고려한 협력 부분접속수 r_2를 분석하였다. 이 결과를 보조정리 2의 부분접속수와 결합하여 맥도날드 부호의 결합 부분접속수는 $m < k-1$일 때 $(r_1, r_2) = (2,3)$이고, $m = k-1$일 때 $(r_1, r_2) = (3,4)$임을 증명하였다.

References

[1] 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.

[2] K. V. Rashmi, N. B. Shah, D. Gu, H. Kuang, D. Borthakur, and K. Ramchandran, "A solution to the network challenges of data recovery in erasurecoded distributed storage systems: A study on the Facebook warehouse cluster," in *5th USENIX Workshop on Hot Topics in Storage and File Systems (HotStorage)*, 2013.

[3] 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.

[4] M.-Y. Nam and H.-Y. Song, "Binary locally repairable codes with minimum distance at least six based on partial t-spreads," *IEEE Commun. Lett.*, vol. 21, no. 8, pp. 1683-1686, Aug. 2017.

[5] J.-H. Kim, M.-Y. Nam, and H.-Y. Song, "Binary locally repairable codes from complete multipartite graphs," *J. KICS*, vol. 40, no. 9, pp. 1734-1740, Sep. 2015.

[6] J.-H. Kim, M. K. Song, and H.-Y. Song, "Block-punctured binary simplex codes for local and parallel repair in distributed storage systems," *IEICE Trans. Fundamentals of Electron., Commun. and Comput. Sci.*, vol. E101, no. 12, pp. 2374-2381, Dec. 2018.

[7] Z. Jing, G. Kim, and H.-Y. Song, "A concatenated binary locally repairable codes with locality 2 using puncturing," *IWSDA 2019*, Dongguan, China, Oct. 2019.

[8] A. S. Rawat, A. Mazumdar, and S. Vishwanath, "Cooperative local repair in distributed

storage," *arXiv Preprint arXiv:1409.3900*, 2014.
[9] J.-H. Kim, M.-Y. Nam, and H.-Y. Song, "Optimal binary locally repairable codes with joint information locality," in *Proc. IEEE ITW*, pp. 54-58, Oct. 2015.
[10] P. Huang, E. Yaakobi, H. Uchikawa, and P. H. Siegel, "Binary linear locally repairable codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6268-6283, Nov. 2016.
[11] Q. Fu, R. Li, L. Guo, and L. Lv, "Locality of optimal binary codes," *Finite Fields and Their Appl.*, vol. 48, pp. 371-394, Nov. 2017.
[12] M. Kuijper and D. Napp, "Erasure codes with simplex locality," in *Proc. MTNS*, pp. 1606-1609, Jul. 2014.

Zhi Jing

2014년 7월 : China University of Geosciences (Beijing) Dept. of Electronic Information Engineering 학사
2015년 11월 : Hong Kong Baptist University Dept. of Computer Science 석사
2016년 9월~현재 : 연세대학교 전기전자공학과 석박사통합과정
<관심분야> 통신공학, 정보이론, 부호이론
[ORCID:0000-0002-1444-3289]

최 효 정 (Hyojeong Choi)

2018년 2월 : 연세대학교 컴퓨터정보통신공학부 졸업
2018년 3월~현재 : 연세대학교 전기전자공학과 석사과정
<관심분야> 통신공학,부호이론, 분산저장시스템
[ORCID:0000-0003-2305-5111]

송 홍 엽 (Hong-Yeop Song)

1984년 2월 : 연세대학교 전자공학과 졸업
1986년 5월 : University of Southern California Dept. of EE. System 석사
1991년 12월 : University of Southern California Dept. of EE. System 박사
1992년 1월~1993년 12월 : University of Southern California 박사 후 연구원
1994년 1월~1995년 8월 : Qualcomm, San Diego, Senior Engineer
1995년 9월~현재 : 연세대학교 전기전자공학과 전임교수
<관심분야> 통신공학, 정보이론, 부호이론
[ORCID:0000-0001-8764-9424]