공학석사 학위논문

분산 저장에서 다중 노드 손실을 고려한 부분접속수와 가용도에 대한 연구

Locality and Availability with Multiple Erasure Tolerance in Distributed Storage

2019년 2월

서울대학교 대학원

전기 정보 공학부

소 병 현

분산 저장에서 다중 노드 손실을 고려한 부분접속수와 가용도에 대한 연구

지도 교수 이 정 우

이 논문을 공학석사 학위논문으로 제출함

2018년 11월

서울대학교 대학원

전기 정보 공학부

소 병 현

소병현의 공학석사 학위논문을 인준함

2018년 12월

위 원 장	노 종 선	(인)
부위원장	이 정 우	(인)
위 원	남 상 욱	(인)

초 록

최근 여러 시스템에서 다루는 데이터의 양이 방대해지면서 분산 저장 시스템의 중요성이 커지고 있다. 분산 저장 시스템에서는 네트워크 상의 문제 혹은 장비의 문제로 인해 노드 손실이라는 결함이 생긴다. 이 경우 손실되지 않은 노드를 통해 손실된 노드를 원상태로 복구하는 것이 중요하다. 이 때 분산 저장에 사용된 부호가 복구의 성능을 결정짓게 된다. 시스템의 용도에 따라 분산 저장에 사용되는 부호의 성능을 결정하는 요소가 다르다. 그 중 '부분접속수(locality)'는 어떤 손실된 노드를 복구하기 위해 필요한 노드의 수를 의미하고 가용도는 어떤 손실된 노드를 복구할 수 있는 서로소(disjoint)인 복구집합의 수를 의미한다.

실용적인 측면에서 가용도 개념을 도입할 경우 다수의 사용자가 동시에 여러 데이터에 병렬적으로 접근함으로써 동시에 데이터를 읽을 수 있다는 장점이 있다. 따라서 가용도를 고려한 부분접속복구 부호는 핫 데이터가 주로 저장된 분산 저장 시스템에 매우 유용하다.

본 논문에서는 분산 저장 시스템에서 다중 노드 손실과 가용도를 함께 고려한 부분접속복구 부호를 새롭게 제안하고 그 부호에 대한 최소 거리의 상계를 구한다. 그리고 새롭게 제안한 부호의 최소 거리의 상계의 achievability를 보이기 위해 최소 거리 상계에 대한 등식을 만족하는 부호를 설계한다.

특히 본 논문에서는 정보 심볼들에 대한 복구집합들의 노드 손실까지 고려했기 때문에 기존의 가용도만을 고려한 부분접속복구 부호에 비해 손실에 대한 tolerance가 더 크다. 따라서 본 논문에서 제안하는 (n,k,r,t,δ) −부분접속복구 부호는 손실이 자주 일어나며 동시에 접속할 필요가 있는 핫 데이터 사용에 더욱 적합하다.

주요어 : 분산저장시스템, 부분접속복구 부호, 가용도, 최소 거리

학 번: 2014−22562

목 차

그림 목차

제 1 장 서 론

제 1 절 연구의 배경

최근 여러 시스템에서 다루는 데이터의 양이 방대해지면서 분산 저장 시스템의 중요성이 커지고 있다. 분산 저장 시스템에서는 네트워크 상의 문제 혹은 장비의 문제로 인해 노드 손실이라는 결함이 생긴다. 이 경우 손실되지 않은 노드를 통해 손실된 노드를 원상태로 복구하는 것이 중요하다. 이 때 분산 저장에 사용된 부호가 복구의 성능을 결정짓게 된다.

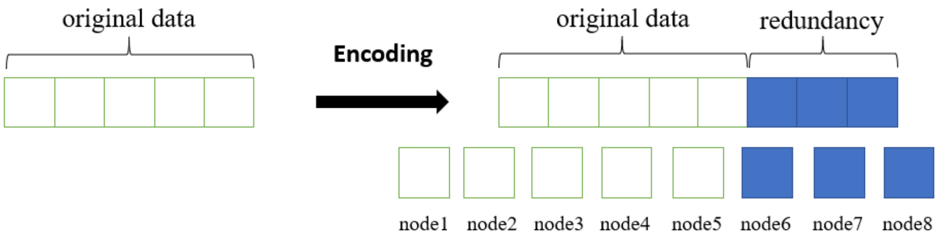


그림 1. 분산저장을 위한 부호화

시스템의 용도에 따라 분산 저장에 사용되는 부호의 성능을 결정하는 요소가 다르다. 복구대역폭(repair bandwidth), 부호율(code rate) 부분접속수(locality), 가용도(availability) 등이 대표적인 부호 성능을 결정하는 요소다. 여기서 부분접속수는 어떤 손실된 노드를 복구하기 위해 필요한 노드의 수를 의미하고 가용도는 어떤 손실된 노드를 복구할 수 있는 서로소(disjoint)인 복구집합의 수를 의미한다.

부분접속수를 성능의 지표로 가지는 부분접속복구 부호에 대한 다양한 연구가 진행되었다. 특히 [1]에서는 부분접속복구 부호에 대한 개념을 처음으로 제안했고 일반적인 부분접속복구 보호의 최소거리에 대한 상계를 제시하였다. 그 이후 다양한 형태의 부분접속복구 부호와 그 부호에 대한 최소거리의 상계가 연구되었다[2][3]. 대표적으로 [4]에서는 가용도라는 새로운 변수를 도입함으로써 부분접속복구 부호의 영역을 확장했다.

제 2 절 연구의 내용

본 논문의 제2장에서는 분산 저장 시스템에서의 복구 부호에 대한 기본적인 정의 및 개념을 소개한다. 제3장에서는 기존에 연구된 부분접속복구 부호와 가용도 개념에 대해서 소개한다. 제4장에서는 분산 저장 시스템에서 다중 노드 손실과 가용도를 함께 고려한 부분접속복구 부호를 새롭게 제안하고 그 부호에 대한 최소 거리의 상계를 구한다. 제5장에서는 새롭게 제안한 부호의 최소 거리의 상계의 achievability를 보이기 위해 최소 거리 상계에 대한 등식을 만족하는 부호를 설계한다.

제 2 장 배경이론

이번 장에서는 전통적인 부호이론에서 사용되는 몇 가지 기본 정의, 개념 및 기술을 소개한다.

제 1 절 생성 행렬(Generator Matrix)과 패리티 검사 행렬(Parity Check Matrix)

하나의 부호(Code)는 하나의 벡터를 또 다른 하나의 벡터로 맵핑을 시켜주는 역할을 한다. 본 논문에서는 부호 중에서 오직 선형 부호(Linear Code)에 대해서만 논한다. 선형 부호의 경우 $\mathbf{u}$벡터와 $\mathbf{x}$벡터가 아래와 같은 벡터행렬 곱으로 표현될 수 있다.

$$\mathbf{uG} = \mathbf{x}$$

여기서 G는 생성 행렬(Generator Matrix)이라고 불리며 $\mathrm{k} \times \mathrm{n}$ 행렬이고 행렬의 성분(coefficient)들은 유한체(Finite Field)에 속한다. 그리고 일반적으로 u는 정보 심볼(information symbol), 그리고 x는 코드 워드(codeword)라고 불린다. 하나의 부호는 보통 C로 표기하며 매개변수를 강조하여 (n,k) 부호라고 쓰기도 한다. 여기서 n은 부호의 길이를 나타내며 k는 부호의 차원(dimension)을 나타낸다. 특히, $\frac{\mathrm{k}}{\mathrm{n}}$은 (n,k) 부호의 'rate' 라 부른다.

생성 행렬이 아래와 같은 형태를 가질 경우 코드 워드는 원래의 정보 심볼을 그대로 가지고 있게 된다.

$$G = [\,I \;\; A\,]$$

이 경우 부호는 'systematic'하다고 한다.

이와 같이 생성 행렬을 통해 정보 심볼로부터 코드 워드가 어떻게 생겨나는지를 알 수 있다. 반면 '패리티 검사 행렬(Parity Check Matrix)'을 통해 어떤 코드 워드가 주어진 부호의 코드 워드인지 확인할 수가 있다.

일반적으로 우리는 (n, k) 부호 C를 패리티 검사 행렬이라 불리는 하나의 $(n-k) \times n$ 행렬 H와 연관지을 수 있고 아래의 성질을 가진다.

x가 부호 C의 코드 워드일 경우, $Hx^t = 0$

제 2 절 부호의 최소 거리(Minimum distance)와 싱글톤 상계(Singleton Bound)

앞서 (n, k) 부호 는 k개의 정보 심볼을 통해 $n-k$ 개의 심볼을 추가한다는 것을 알았다. 이 $n-k$ 개의 심볼은 redundancy가 된다. 예를 들어 하나의 정보 심볼 u를 erasure 채널을 통해 전달한다고 했을 때, 수신 측에서는 u를 받거나 아무것도 받지 못하게 된다. 하지만 만약 $(n, 1)$ 반복 부호를 사용한다면 수신측은 $n-1$ 개의 노드 손실이 발생해도 u를 읽을 수 있다. 일부에서는 노드 손실 대신에 에러r를 가진 채널을 소개하지만 본 논문에서는 오직 erasure 채널 및 erasure 부호만을 고려하도록 한다.

다음으로는 매개변수 (n, k)를 가진 하나의 선형 부호가 견뎌낼 수 있는 최대 노드 손실의 수를 알아보도록 한다. 이를 위해서 해밍 거리(Hamming Distance)와 해밍 웨이트(Hamming Weight)의 개념을 알아본다. 두 벡터 x와 y가 주어졌을 때 x와 y 사이의 해밍 거리는 x와 y 사이에 서로 다른 계수의 개수와 같다. 특히 x와 y사이의 해밍 거리는 $d(x, y)$ 로 표기한다.

벡터 x가 주어졌을 때, x의 해밍 웨이트는 x의 0이 아닌 계수의 개수로 정의되며 $wt(x)$로 표기한다.

해밍 거리와 해밍 웨이트는 아래와 같은 관계를 가지게 된다.

$$d(x, y) = wt(x - y)$$

하나의 부호 C의 ‘최소 (해밍) 거리 $d_H(C)$’는 임의의 서로 다른 코드 워드 사이의 해밍 거리 중 가장 작은 해밍 거리를 의미한다.

$$d_H(C) = \min d(x, y) = \min wt(x - y)$$

때로 어떤 부호의 최소 거리가 강조되어야 할 필요가 있을 경우에는 $d_H(C) = d$로 표기하고 (n, k, d) 부호라고 부른다.

특히 부호 C가 선형 부호일 경우,

$$d_H(C) = \min wt(x)$$

이다. 왜냐하면 선형 부호에서 임의의 두 코드 워드의 차이는 다시 하나의 코드 워드가 되기 때문이다.

만약 어떤 부호의 최소 거리가 d일 경우 이 부호는 $d - 1$개의 노드 손실을 견딜 수 있다. $d - 1$개의 손실을 견딘다는 말은 $d - 1$개의 노드 손실이 발생해도 나머지 노드들의 심볼만으로도 원래의 정보를 복구할 수 있다는 것을 의미한다. 그 이유는 위에서 언급한 바와 같이 모든 서로 다른 두 개의 코드 워드는 적어도 d개의 심볼이 다르고 d개 이상의 심볼이 손실되지 않는 이상 그들을 구분할 수 있다.

최소 거리는 패리티 검사 행렬과도 관계가 있다. H가 길이 n인 부호 C의 패리티 검사 행렬이고 C의 최소 거리가 d인 것은 H의 모든 $d - 1$개의 열이 선형 독립(linearly independent)이고 어떤 d개의 열들은 선형 종속(linearly dependent)임과 동치이다.

증명. 부호 C에 $wt(x) = d$인 코드 워드 x가 존재한다는 것은 해밍 웨이트가 d인 x에 대해 $Hx^t = 0$임과 동치이다. 또한 이는 H의 d개의 열들이 선형 독립임과 동치이다.

싱글톤 상계(Singletone Bound)는 n과 k가 주어졌을 때 최소 거리의 상한계에 대해서 알려준다.

부호 C가 (n, k, d) 선형 부호일 경우,

$$n - k \geq d - 1$$

이고, 이는 다시 표현하면

$$d \le n - k + 1$$

이다.

증명) H의 rank는 $n-k$이고 정의에 의해 이것은 H의 선형 독립적인 H의 열들의 최대 개수를 의미한다.

싱글톤 상계를 통해서 싱글톤 상계의 등호 조건을 만족하는 (n, k) 부호는 $(n-k)$ 개까지의 erasure가 발생해도 원래의 information을 복구할 수 있음을 알 수 있다.

싱글톤 상계의 등호조건을 만족하는 부호는 maximum distance separable(MDS) 부호라고 부른다. 왜냐하면 MDS 부호는 n과 k가 주어졌을 때 가장 좋은 erasure protection을 보여주기 때문이다.

제 3 장 부분접속복구 부호(Locally Repairable Codes)

제 1 절 부분접속복구 부호(Locally Repairable Codes)

분산 저장 부호에서 Exact Repair 문제는 중요한 이슈이다. Exact Repair 문제는 부호화된 정보를 저장하고 있는 하나의 노드가 손실 됐을 때 같은 신뢰도 수준을 유지하기 위해 새로운 노드에 지워진 정보와 정확히 같은 정보를 재생성 하는 것이다. 이 문제에서 중요한 이슈는 정확하면서도 낮은 복구비용 그리고 높은 data rate 을 유지하는 부호를 디자인하는 것이다.

이번 장에서는 '부분접속수(locality)'라는 것에 대해 관심을 가진다. 부분접속수는 하나의 노드를 복구하는 동안 필요한 디스크 접속 수를 의미한다. 또한 부분접속수와 부호의 최소거리, 그리고 노드당 저장 용량에 대한 정보이론적인 상충관계를 소개한다.

먼저 부호의 최소거리를 설명하기 위해 어떻게 저장된 부호 정보들에 엔트로피를 사용하는지를 소개한다. 엔트로피 개념을 도입함으로써 부호(선형 부호 혹은 비선형 부호)의 부분접속수와 최소거리, 그리고 저장용량 사이의 정보이론적인 상충관계를 만들 수 있다. 크기 M 인 정보를 아래와 같이 k개의 동일한 크기의 조각으로 나눌 수 있다.

$$x = [\, X_1, \dots, X_k \,]$$

여기서 X_i들은 어떤 유한체 F 에 대한 source 성분이며 엔트로피 $H(X_i)$는 $H(X_i) = \frac{M}{k}$ for all $i \in [k]$인 i.i.d random variable 이다. 그리고 생성 함수를 $G : F_{1\,x\,k} \rightarrow F_{1\,x\,n}$라고 한다. 그러면

$$G(x) = y = [\, Y_1, \dots, Y_n \,]$$

이다. 여기서 각 부호화된 성분들의 엔트로피는 다음과 같다.

$$H(Y_i) = \alpha \geq \frac{M}{k} \quad \text{for all } i \in [n]$$

생성 함수 G는 부호 C를 정의하며, 부호율은 저장된 정보의 총합에 대한 쓸모 있는(useful) 정보의 총합 비율이 된다. 즉, 엔트로피로 표현하면 아래와 같다.

$$R = \frac{H(X_1, \ldots, X_k)}{\sum_{i=1}^{n} H(Y_i)} \leq \frac{k}{n}, \quad \alpha = \frac{k}{n} \text{ 일 때 등호조건}$$

다음으로 엔트로피를 사용하여 부호의 최소거리를 정의해본다. 어떤 부호 C의 최소거리 d는 다음과 같이 정의될 수 있다.

$$d = \min|\varepsilon|$$
$$\text{such that } H(\{Y_1, \ldots, Y_n\} \backslash \varepsilon) < M, \text{ and } \varepsilon \in 2^{\{Y_1, \ldots, Y_n\}}$$

다시 말해서 하나의 부호는 $d-1$개의 부호화된 성분이 지워져도 원래의 파일을 복구하기 위한 충분한 엔트로피를 가진다는 것을 나타낸다. 위에서 정의한 부호의 최소거리는 아래와 같은 형태로도 재정의가 가능한다.

$$d = n - \max_{H(S)<M} |S|, \text{ where } S \in 2^{\{Y_1, \ldots, Y_n\}}$$

이번에는 부분접속수에 대해서 정의해본다. 하나의 부호화된 성분 $Y_i, i \in [n]$가 $Y_i = f_i(Y_{R(i)})$ 와 같이 r개의 다른 부호화된 변수들의 함수일 경우 Y_i는 부분접속수 r을 가진다고 한다. 여기서 집합 $R(i)$는 Y_i를 복구할 수 있는 가장 작은 r개의 부호화된 성분들의 집합을 가리키고 f_i는 r개의 부호화된 성분에 대한 어떤 함수이다.

[1]에서 Gopalan은 각 부호화된 성분들이 엔트로피 $\alpha = \frac{M}{k}$ 를 가지고 부분접속수 r, 그리고 길이 n의 스칼라 선형 부호에 대해서 아래와 같은 최소거리의 상계를 얻었다.

$$d \leq n - k - \left\lceil \frac{k}{r} \right\rceil + 2$$

 위 상계에 따르면 낮은 부분접속수를 가질수록 $\frac{k}{r}$ 컴포넌트에 의해 최소거리에 대해 손해를 보게 된다. 이와 같이 스칼라 부호에서는 최소거리에 대한 불이익이 불가피하다. 다른 한편 (n, k) MDS 부호의 경우 최소 거리 $d = n - k + 1$이고 최소거리에 대해서는 최대 값을 가지는 대신 부분접속수에 대해서 $r = k$ 가 되어 가장 안 좋은 경우가 된다. 하지만 본 장에서의 목적은 낮은 부분접속수를 얻어내는 것이다.

 다음에서 부분접속수 r과 최소거리 d 그리고 저장용량 α 사이의 정보이론적인 상충관계를 알아보고 이를 통해 어떻게 세번째 매개변수인 저장용량이 높은 최소거리와 낮은 부분접속수를 얻어내는 데 사용되어 질 수 있을지 알아본다.

 부호 $C(n, r, d, \alpha)$에 대한 최소거리의 상계는 아래와 같다.

$$d \leq n - \left\lceil \frac{M}{\alpha} \right\rceil - \left\lceil \frac{M}{r\alpha} \right\rceil + 2$$

위 부등식에 대한 증명은 [5]에서 볼 수 있다. 특히 [2]에서 위 부등식의 achievability 를 보인다.

제 2 절 분산저장에서 부분접속수와 가용도

여기에서는 부호 심볼의 가용도(availability)에 대해서 소개한다. 만약 어떤 부호 심볼이 t개의 서로소인 다른 심볼들의 그룹(각 그룹의 최대 크기는 r)으로부터 복구가 가능하다면 이 심볼은 (r, t)- 가용도를 가진다고 말한다. 예를 들어 3-replication 부호의 경우 각 심볼이 $t = 2$개의 다른 복제된 그룹으로부터 복구가 가능하므로 (1,2) - 가용도를 가지게 된다. 가용도 개념을 도입함으로써 데이터를 병렬적으로 동시에 읽을 수 있게 된다. 따라서 핫 데이터에 사용이 매우 적합하다.

 가용도 개념을 도입한 (n, k, r, t)−부분접속복구 부호는 systematic 한 부호이며 각 정보 심볼들은 부분접속수 r을 가진다. 또한 모든 systematic 심볼에 대해서 그 심볼을 복구할 수 있는 t개의 서로소인 심볼 그룹들이 존재한다. 즉, (n, k, r, t)−부분접속복구 부호에서 정보 심볼들은 (r, t)−가용도를 가진다. 형식적으로 (n, k, r, t)−부분접속복구 부호에 대해서 정의하면 아래와 같다. 여기에서는 오직 길이 n의

systematic 한 부호만을 고려하며 일반성을 잃지 않고 코드 워드 $c = (c_1, c_2, \dots, c_n)$ 의 첫 k개의 심볼을 정보 심볼이라고 가정한다. (n, k, r, t)−부분접속복구 부호는 아래의 3 가지 성질을 만족한다.

1) 각 systematic 한 정보 심볼들 c_i, $i \in [k]$ 에 대하여 t 개의 부분집합 $\Gamma_1(i), \dots, \Gamma_t(i) \subset [n] \backslash \{i\}$ 이 존재하고 c_i 는 $c_{\Gamma_j(i)}$ 들의 함수로 표현될 수 있다.

2) 모든 $i \in [k], j \in [t]$에 대하여 $|\Gamma_j(i)| \le r$ 이다.

3) 모든 $i \in [k]$와 $j \neq l \in [t]$에 대하여 $\Gamma_j(i) \cap \Gamma_l(i) = \emptyset$ 이다.

위 정의에 의해 (n, k, r, t)−부분접속복구 부호의 각 정보 심볼들 c_i는 그 자신과 t개의 복구 그룹 $\Gamma_1(i), \dots, \Gamma_t(i)$에 의해 가리켜지는 심볼들에 접속함으로써 병렬적으로 복구가 가능하다. 정의에 의해 정보 심볼들만 부분접속수 r을 가지는 경우 'information−symbol locality'라 하며, 만약 n개의 모든 부호 심볼들이 부분접속수 r을 가질 경우 'all−symbol locality'라 한다.

다음으로 선형 (n, k, r, t)−부분접속복구 부호에 대한 새로운 최소거리의 상계를 알아본다. [4]에서 소개하는 주요 정리에서는 부호에 대한 간단한 상황(condition)을 설정한다. 각 정보 심볼들과 연관된 모든 복구집합들은 오직 1 개의 패리티 심볼만을 가진다. [4]의 후반부에는 위에서 설정한 상황을 없앤 더 일반적인 상황에서의 최소거리에 대한 상계를 보인다. [4]에서 소개하는 정리는 다음과 같다.

[정리] C가 선형 (n, k, r, t)−부분접속복구 부호이고 k개의 정보심들에 대한 모든 복구 그룹들이 오직 1 개의 패리티 심볼만을 가진다면 부호 C의 최소 거리의 상계는 다음과 같다.

$$d_{min}(C) \le n - k - \left\lceil \frac{kt}{r} \right\rceil + t + 1$$

자세한 증명은 [4]에서 소개한다.

여기서 주목해야할 점은 위 이론에서 소개하는 최소거리의 상계에 대한 식에서 $t = 1$인 경우는 [1]에서 소개하는 부분접속수 r을 가지는 선형 부분접속복구 부호에 대한 상계와 같다.

[4]에서는 더 일반적인 (n,k,r,t)−부분접속복구 부호의 최소거리에 대한 상계도 소개한다. 다음의 상계는 부호의 선형성이나 모든 복구 그룹들이 오직 하나의 패리티 심볼만을 가져야 한다는 가정을 하지 않는다.

[정리] (n,k,r,t)−부분접속복구 부호에 대해서 최소거리 d 는 다음의 상계를 가진다.

$$\mathrm{d}_{min}(C) \le n - k - \left\lceil \frac{t(k-1)+1}{t(r-1)+1} \right\rceil + 2$$

자세한 증명은 [4]에서 소개한다. 선형 부호에 대해서는 위 상계를 만족하는 부호가 설계되었지만 일반적인 경우에 대한 위 부등식의 tightness 는 아직 open problem 으로 남아있다.

제 4 장 다중 노드 손실을 고려한 부분접속수와 가용도

지금까지 부분접속수를 성능의 지표로 가지는 부분접속복구 부호에 대한 다양한 연구가 진행되었다. 특히, [1]에서는 부분접속복구 부호에 대한 개념을 처음으로 제안했고, 일반적인 부분접속복구 부호의 최소거리에 대한 상한계를 제시하였다. 그 이후 다양한 형태의 부분접속복구 부호와 부호의 최소거리에 대한 상계가 연구되었다[2][3]. 대표적으로 [4]에서는 가용도라는 새로운 변수를 도입함으로써 부분접속복구 부호의 영역을 확장했다. 이번 장에서는 [4]의 결과를 확장하여 다중 노드 손실과 가용도를 함께 고려한 부분접속복구 부호를 새롭게 제안하고 그 부호에 대한 최소 거리의 상한계를 소개한다.

제 1 절 다중 노드 손실과 가용도를 고려한 부분접속복구 부호

기존 [4]의 (n, k, r, t)−부분접속복구 부호에서 다중 노드 손실을 고려하여 (n, k, r, t, δ)−부분접속복구 부호를 새롭게 정의한다. 또한, 새로 정의한 부호의 상계를 구하기 위하여 멤버십 행렬 및 최소거리를 정의한다. 정의에 앞서 일반성을 잃지 않고 n개의 심볼 중에서 처음 k개를 정보 심볼로 가정한다.

먼저 새롭게 정의하는 (n, k, r, t, δ)−부분접속복구 부호는 다음의 세 가지 성질을 가진다.

1) 모든 $i \in [k], j \in [t]$에 대하여 t개의 복구집합 $\Gamma_1(i), \ldots, \Gamma_t(i) \subset [n]\backslash\{i\}$가 존재하며, 정보 심볼 c_i는 $\Gamma_j(i)$에 속하는 임의의 r개의 원소에 의해 가리켜지는 심볼들에 의한 함수로 표현 가능하다.
2) 모든 $i \in [k]$ 그리고 $j \neq l \in [t]$에 대하여 $\Gamma_j(i) \cap \Gamma_l(i) = \emptyset$이다.
3) 모든 $i \in [k], j \in [t]$에 대하여 $|\Gamma_j(i)| \leq r + \delta - 2$이다.

위 정의에 따르면 (n,k,r,t,δ)−부분접속복구 부호의 모든 정보 심볼들은 정보 심볼 그 자신과 t개의 서로소인 복구집합 $\Gamma_1(\cdot),\ldots,\Gamma_t(\cdot)$로부터 가리켜지는 심볼들로 병렬적으로 복구가 가능하다. 또한 부분접속수 관점에서 보면 t개의 서로소인 복구집합을 통해 정보 심볼을 복구할 때 각 복구집합에서 최대 r개의 원소에 의해 가리켜지는 심볼만으로 정보 심볼 복구가 가능하다.

다음으로 위에서 정의한 (n,k,r,t,δ)−부분접속복구 부호의 최소거리에 대한 상계를 구하기 위해 멤버십 행렬 R 을 정의한다.

(정의) 모든 $i\in[k], j\in[t]$에 대하여 $\Gamma_j(i)$의 총 개수를 m이라고 하자. 이 때 각 성분이 0 또는 1 인 $k\times m$ 멤버십 행렬을 정의하고 R이라고 부른다. 멤버십 행렬의 요소들은 복구집합 m개에 참여하는 정보 심볼들을 나타낸다. 이는 R의 (i,j) 요소가 1 이면, i번째 정보 심볼이 j번째 복구집합에 참여한다는 의미이다. 따라서 R의 각 행은 정보 심볼의 index 를 나타내고 각 열은 하나의 복구집합을 나타낸다.

마지막으로 제 3 장에서 정의했던 부호 C의 최소거리에 대한 일반적인 정의는 아래와 같다.

$$\mathrm{d}_{min}(C)=n-|S^*|$$

여기서 S^*는 S^*의 원소들에 의해 가리켜지는 심볼로 k개의 모든 정보 심볼을 완전히 복구할 수 없는 집합 중에서 가장 원소의 개수가 많은 집합을 가리킨다.

제 2 절 $(\mathbf{n},\mathbf{k},\mathbf{r},\mathbf{t},\boldsymbol{\delta})$−부분접속복구 부호의 최소거리에 대한 상계

이번 장에서는 선형 (n,k,r,t,δ)−부분접속복구 부호에 대한 최소거리의 상계를 보인다. 앞으로 보일 주요 정리에서 우리는 각 복구 집합들이 오직 $\delta-1$ 개의 패리티 심볼을 가진다는 간단한 상황을 가정한다. 주요 정리를 보이기에 앞서 몇 가지 보조정리를 살펴보도록 한다.

(보조정리) 선형 $(n,k,r,t,\delta)-$부분접속복구 부호에서 어떤 정보 심볼 $c_i, i \in [k]$에 대한 모든 복구집합들은 최소 $\delta-1$개의 패리티 심볼을 포함한다.

(증명) $(n,k,r,t,\delta)-$부분접속복구 부호의 정의에 의하면 $(n,k,r,t,\delta)-$부분접속복구 부호의 각 복구집합의 size 는 $r+\delta-2$보다 작거나 같다. 또한 정보 심볼 c_i, $i \in [k]$는 해당 복구 집합의 임의의 r개의 원소에 의해 가리켜지는 심볼들로 복구할 수 있어야 한다. 따라서 각 복구 집합에서 임의의 $\delta-2$개의 심볼이 지워지더라도 c_i를 복구할 수 있어야 한다. 하지만 만약 패리티 심볼이 $\delta-1$보다 작다면 어떤 복구 집합의 모든 패리티 심볼이 지워질 경우 남은 심볼들은 모두 정보 심볼들이기 때문에 c_i에 대한 정보를 전혀 포함하지 않게 된다. 따라서 c_i를 복구할 수가 없다. 따라서 선형 $(n,k,r,t,\delta)-$부분접속복구 부호의 정보 심볼 $c_i, i \in [k]$에 대한 모든 복구 집합들은 최소 $\delta-1$개의 패리티 심볼을 포함해야 한다. □

위 보조정리에 의해 정보 심볼 $c_i, i \in [k]$에 대한 모든 복구 집합들은 최소 $\delta-1$개라는 것을 알 수 있고 이를 근거로 앞으로 보이게 될 주요정리에서 각 복구집합은 오직 $\delta-1$개의 패리티 심볼만을 가진다는 상황을 설정했다. 위와 같은 가정을 할 경우가정을 할 경우 아래와 같은 추가적인 보조정리를 이끌어 낼 수 있다.

(보조정리) 선형 $(n,k,r,t,\delta)-$부분접속복구 부호의 멤버십 행렬에 의해 정의되는 모든 복구 집합들이 오직 $\delta-1$개의 패리티 심볼만을 가질 경우 모든 복구집합들의 패리티 심볼들은 서로소이다.

(증명) 먼저 $(n,k,r,t,\delta)-$부분접속복구 부호의 정의에 의해 어떤 정보 심볼 $c_i, i \in [k]$에 대한 모든 복구 집합들의 패리티 심볼들은 서로소이다. (정의에 의해) 즉, 멤버십 행렬에서 i번째 행의 성분이 1 인 복구 집합들의 모든 패리티 심볼은 서로소이다. 다음으로 멤버십 행렬의 i번째 행의 성분이 1 인 복구 집합의 패리티 심볼들과 성분이 0 인 복구 집합의 패리티 심볼들이 서로소임을 보이면 된다. $(n,k,r,t,\delta)-$부분접속복구 부호의 성질과 모든 복구 집합들이 오직 $\delta-1$개의 패리티 심볼만을 가진다는 가정을 통해 멤버십 행렬의 i번째 행의 성분이 1 인

복구집합의 모든 패리티 심볼들은 정보 심볼 c_i의 정보를 포함해야 한다. 여기서 만약 멤버십 행렬의 i번째 행의 성분이 1 인 복구집합과 멤버십 행렬의 i번째 행의 성분이 0 인 복구집합이 어떤 패리티 심볼을 공유하게 된다면 그 패리티 심볼은 반드시 c_i의 정보를 가져야 하고 이 경우 멤버십 행렬의 i번째 행의 성분이 0 인 복구집합에서 패리티 심볼의 역할을 하지 못하게 된다. 따라서 $(n, k, r, t, \delta)-$부분접속복구 부호의 멤버십 행렬에 의해 정의되는 모든 복구 집합들의 패리티 심볼들은 서로소이다. □

또한 언급한 상황에서의 선형 $(n, k, r, t, \delta)-$부분접속복구 부호의 멤버십 행렬에 대해 아래와 같은 보조정리를 얻을 수 있다.

(보조정리) $(n, k, r, t, \delta)-$부분접속복구 부호에서 R 이 {0, 1} 의 성분을 가지는 $k \times m$의 멤버십 행렬일 때 R의 열의 개수 m은 다음 부등식을 만족한다.

$$\mathrm{m} \geq \left\lceil \frac{kt}{r} \right\rceil$$

(증명)

정의에 의해 (n, k, r, t, δ) −부분접속복구 부호의 k 개의 정보 심볼들은 각각 t개의 서로소인 복구 집합을 가진다. 따라서,

$$\text{멤버십 행렬 R의 성분 중 1 의 개수} \geq \mathrm{k} \times \mathrm{t}$$

이다. 또한 정의에 의해

$$\text{모든 } \mathrm{i} \in [\mathrm{k}], \mathrm{j} \in [\mathrm{t}]\text{에 대하여 } |\Gamma_{\mathrm{i}}(j) \cup \{i\}| \leq r + \delta - 1$$

이고 가정에 의해 각 복구 집합은 $\delta - 1$ 개의 패리티 심볼을 가지므로 $(n, k, r, t, \delta)-$부분접속복구 부호의 멤버십 행렬의 모든 열의 1 의 개수는 r 보다 작거나 같다. 따라서,

$$\text{멤버십 행렬 R 의 성분 중 1 의 개수} \leq \mathrm{m} \times \mathrm{r}$$

이다. 위에서 얻은 식을 종합함으로써

$$m \geq \left\lceil \frac{kt}{r} \right\rceil$$

을 얻을 수 있다. □

(주요 정리) (n, k, r, t, δ)−부분접속복구 부호에서 각 복구 집합이 오직 $\delta - 1$개의 패리티 심볼을 가질 때, 부호의 최소 거리에 대한 상계는 다음과 같다.

$$d_{min}(C) \leq n - k + 1 - \left(\left\lceil \frac{kt}{r} \right\rceil - t\right)(\delta - 1)$$

(증명) 최소 거리의 상계를 구하기에 앞서 집합 S 를 구성한다. S 는 S 의 성분에 의해 가리켜지는 심볼들로는 k 개의 보든 정보 심볼을 복구할 수 없도록 구성한다. S 를 구성할 때 다음 두 가지 경우를 생각한다.

Case 1) 어떤 i번째 정보 심볼이 정확히 t개의 서로소인 복구 집합만을 가지는 경우, 즉 멤버십 행렬 R의 i번째 행이 오직 t개의 1 을 가지는 경우를 생각한다. 그리고 S를 다음과 같이 구성한다.

$$S = ([k] \backslash i) \cup P_{R_i},$$

P_{R_i}는 R 의 i번째 성분이 0 인 열들의 모든 패리티 심볼들의 집합

이 경우,

$$\left|P_{R_i}\right| = (m - t) \times (\delta - 1)$$

이다. 여기서 S에 의해 가리켜지는 심볼들로는 i번째 정보 심볼을 복구할 수 없고 이를 통해 아래 부등식을 얻을 수 있다.

$$|S^*| \geq |S| = k - 1 + (m - t)(\delta - 1)$$

$d_{min}(C) = n - |S^*| \leq n - |S|$이기 때문에 위 식을 적용함으로써

$$d_{min}(C) \leq n - k + 1 - (m - t)(\delta - 1)$$

를 얻을 수 있고 보조정리로부터 얻은 $m \geq \left\lceil\frac{kt}{r}\right\rceil$과 위 식을 결합함으로써

$$d_{min}(C) \leq n - k + 1 - (\left\lceil\frac{kt}{r}\right\rceil - t)(\delta - 1)$$

를 얻을 수 있다.

Case 2) (n, k, r, t, δ) −부분접속복구 부호의 멤버십 행렬의 행들 중에서 가장 1 의 개수가 적은 행이 가지는 1 의 개수 t'이 t보다 클 때

$$kt' \leq \text{R 의 성분 중 1 의 개수} \leq mr$$

이 되고,

$$m \geq \left\lceil\frac{kt'}{r}\right\rceil$$

을 얻을 수 있다. 여기서 어떤 $i \in [k]$에 대해서 R의 i번째 행이 정확히 t'개의 1 을 가진다고 가정한다. 그리고 case 1 과 비슷하게 아래와 같이S를 구성한다.

$$S = ([k] \backslash i) \cup P_{R_i},$$

여기서 S에 의해 가리켜지는 심볼들로는 i번째 정보 심볼을 복구할 수 없게 되고 아래와 같은 부등식을 얻을 수 있다.

$$|S^*| \geq |S| = k - 1 + (m - t')(\delta - 1)$$

$d_{min}(C) = n - |S^*| \leq n - |S|$ 이고 $m \geq \left\lceil\frac{kt'}{r}\right\rceil$ 이므로 아래의 식을 얻을 수 있다.

$$\mathrm{d}_{min}(C) \le n - k + 1 - \left(\left\lceil \frac{kt'}{r} \right\rceil - t'\right)(\delta - 1)$$

여기서 $\mathrm{r} \le \mathrm{k}$이기 때문에 위 부등식의 우변은 주요 정리에서 보이고자 하는 부등식의 우변보다 작거나 같게 된다. 따라서 우리는 두 경우를 결합하여 최종적으로

$$\mathrm{d}_{min}(C) \le n - k + 1 - \left(\left\lceil \frac{kt}{r} \right\rceil - t\right)(\delta - 1)$$

를 얻을 수 있다. □

여기서 $\delta - 1 = 1$인 경우 각 복구 집합이 오직 1 개의 패리티 심볼만을 가지는 상황을 가정한 [4]의 선형 $(\mathrm{n}, \mathrm{k}, \mathrm{r}, \mathrm{t})-$부분접속복구 부호의 최소거리 상계에 대한 식과 같아진다. 위 부등식을 통해 다중 노드 손실을 고려할 경우 복구 집합의 노드 손실에 대한 protection 과 최소 거리 사이에 상충관계가 있음을 알 수 있다.

제 5 장 $(\mathbf{n},\mathbf{k},\mathbf{r},\mathbf{t},\boldsymbol{\delta})$−부분접속복구 부호의 최소 거리 상계에 대한 achievability

이번 장에서는 (n,k,r,t,δ) −부분접속복구 부호를 설계하고 이 부호의 최소 거리가 앞서 제시한 최소거리에 대한 상계의 등호조건을 만족함을 보인다. 이를 통해 앞서 제시한 (n,k,r,t,δ) −부분접속복구 부호의 최소 거리 상계에 대한 achievability를 보인다.

제 1 절 $(\mathbf{n},\mathbf{k},\mathbf{r},\mathbf{t},\boldsymbol{\delta})$−부분접속복구 부호의 설계

이번 절에서는 $r|k$이고 아래의 가정을 만족하는 경우에 대해서 (n,k,r,t,δ)−부분접속복구 부호를 설계한다.

(가 정) 어떤 $k\times t\frac{k}{r}$인 행렬 R이 아래의 조건을 만족한다.

1) R의 모든 열들은 r개의 0이 아닌 성분을 가진다.
2) R의 열들의 성분은 t개의 [k]의 파티션을 이룬다.
3) R의 임의의 모든 두 행들은 최대 1개의 성분만이 위치가 겹친다.

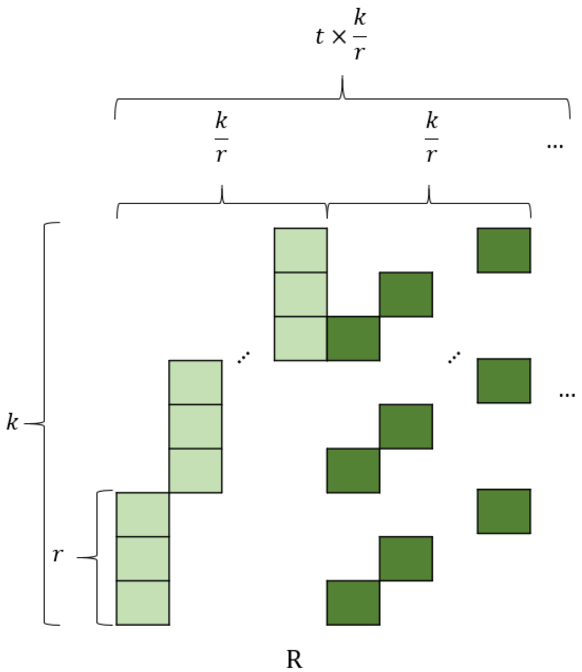


그림 2. 행렬 R의 설계

그리고 R 에서 $\frac{k}{r}$ 개씩의 열들을 뽑아 t개의 컬렉션 $R_1, \ldots, R_t$를 얻을 수 있다. 여기서 어떤 $(N+t(\delta-1),k)$ MDS 부호의 생성 행렬 $\hat{G}$가 주어졌을 때 $\left(n=N+\frac{kt}{r}(\delta-1),k,r,t,\delta\right)$−부분접속복구 부호의 생성 행렬 G는 아래와 같이 만들어진다.

(Construction 1)

- G의 첫 N개의 열들은 $\hat{G}$의 첫 N 개의 열과 같다.
- 각 $i \in [t], j \in [\delta-1]$에 대해서 $\hat{G}$의 $(N+i\times j)$ 열은 각각 r개의 weight 를 가지는 $\frac{k}{r}$ 개의 열로 갈라져 G의 나머지 $\frac{kt}{r}(\delta-1)$개의 열을 구성한다. 여기서 어떤 i에 대해 $\hat{G}$의 1 개의 열이 $\frac{kt}{r}$ 개의 열로 갈라질 때 모든 j에 대하여 갈라진 열들의 성분 위치는 R_i의 $\frac{k}{r}$ 개의 열의 성분위치와 같다.

여기서 G의 처음 k개의 심볼은 systematic 한 심볼이며, G의 $k+1$에서 N 까지의 열들은 전역 패리티 심볼과 연관이 있다. 또한 $\hat{G}$ 의 마지막 $t(\delta-1)$ 개의 컬럼을 쪼개서 얻은 G의 $\frac{kt}{r}(\delta-1)$개 열들은 지역 패리티 심볼과 관련이 있음을 주목한다.

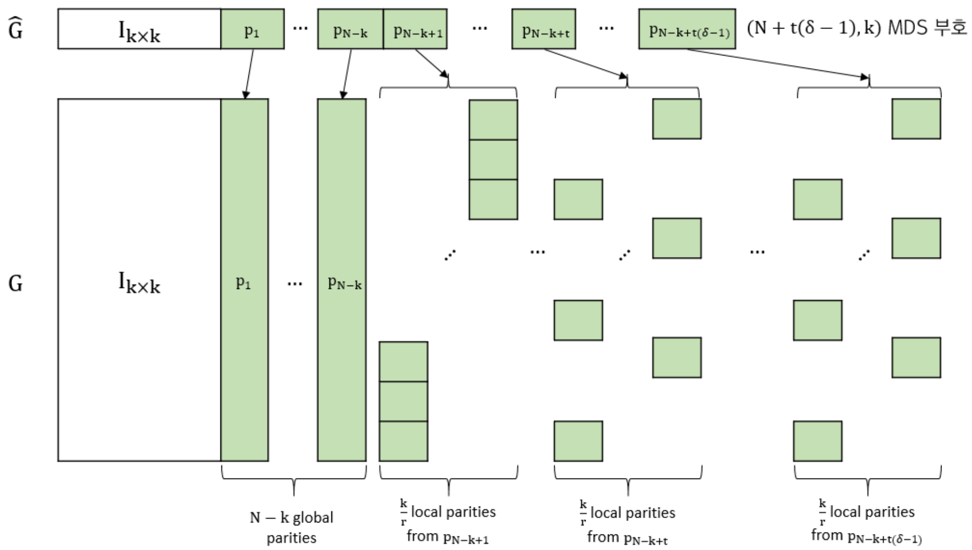


그림 3. 생성행렬 G의 설계

제 2 절 최소거리 상계에 대한 achievability

이번 절에서는 앞 절에서 설계한 $\left(n = N + \frac{kt}{r}(\delta - 1), k, r, t, \delta\right)-$부분접속복구 부호의 최소 거리가 제 4 장에서 보인 최소 거리의 상계와 같음을 보인다.

(이론) $r|k$ 이고 가정 1 을 만족할 경우 construction 1 을 통해 만들어진 $\left(n = N + \frac{kt}{r}(\delta - 1), k, r, t, \delta\right)-$부분접속복구 부호의 최소 거리는 아래 식을 만족한다.

$$d_{min}(C) = n - k + 1 - \left(\left\lceil \frac{kt}{r} \right\rceil - t\right)(\delta - 1)$$

(증명)

Construction 1 의 MDS 부호의 $t(\delta - 1)$ 개의 패리티 심볼들로부터 $\frac{kt}{r}(\delta - 1)$ 개의 지역 패리티를 만들기 위해 R의 열들을 사용한다. R의 열들은 t개의 [k]의 파티션을 이루고 이는 각 정보 심볼들에게 t개의 지역 패리티 심볼이 관여함을 의미한다. 또한 R의 임의의 두 행의 교집합에 대한 제한으로부터 하나의 정보 심볼에 대한 t 개의 복구 집합들은 해당 정보 심볼을 제외하고 서로소이다.

다음으로 Construction 1 로부터 얻어진 부호의 최소 거리가 위에서 보인 등식을 만족함을 보이기 위해 임의의 $n - k - \left(\left\lceil \frac{kt}{r} \right\rceil - t\right)(\delta - 1) = N + k\frac{t}{r}(\delta - 1) - k - \left(\frac{kt}{r} - t\right)(\delta - 1) = N - k + t(\delta - 1)$개의 심볼에 손실이 일어나더라도 원래의 정보를 복구할 수 있음을 보이고자 한다.

증명에 앞서 부호 C의 길이 n 인 코드 워드에 대해서 systematic 한 정보 심볼들의 인덱스들의 집합을 I, 전역 패리티 심볼들의 인덱스들의 집합을 P^{global}, 지역 패리티 심볼들의 인덱스들의 집합을 P^{local}이라고 하자. 그리고 $i \in [t], j \in [\delta - 1]$에 대하여 $P_{i,j}^{local}$는 $\widehat{G}$의 $(N + i \times j)$ 에 의해 얻어지는 지역 패리티 심볼들의 인덱스들의 집합이다. 특히 여기서 $\left|P_{i,j}^{local}\right| = \frac{k}{r}$ 이다. 다음으로 우리는 다음 두 가지 경우를 생각한다.

Case1) 집합 $A = I \cup P^{global}$ 에 의해 인덱스 되는 심볼들 중에서 최대 N−k 개의 손실이 일어난 경우.

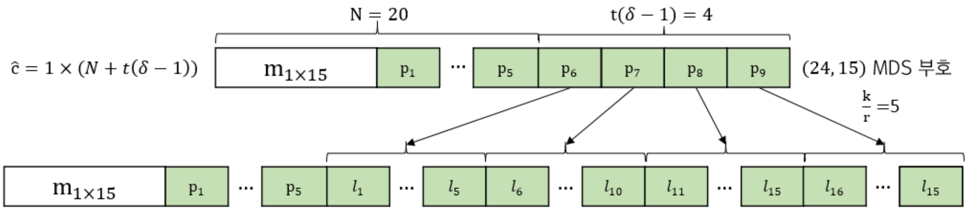
이 경우 A의 인덱스에 의해서 얻어지는 부호는 (N,k) MDS 부호이기 때문에 A에서 어떤 임의의 $\mathrm{N}-\mathrm{k}$ 개의 손실이 일어나더라도 원래의 정보 심볼들 $\mathbf{m}$을 복구할 수 있다.

Case2) A에서 $\mathrm{N}-\mathrm{k}+\mathrm{x}\,(0 \leq \mathrm{x} \leq \mathrm{t})$개의 손실이 일어난 경우
이경우 P^{local}에서 $\mathrm{t}(\delta-1)-\mathrm{x}$개의 손실이 존재한다. 최악의 경우 $\mathrm{t}(\delta-1)-\mathrm{x}$개의 손실이 $\{\mathrm{P}_{1,1}^{\mathrm{local}},\ldots,\mathrm{P}_{t,\delta-1}^{\mathrm{local}}\}$의 $\mathrm{t}(\delta-1)$개의 집합들에 퍼져 있게 된다. 여기서 $\{\mathrm{P}_{k_1}^{\mathrm{local}},\ldots,\mathrm{P}_{k_x}^{\mathrm{local}}\}$가 손실이 일어난 심볼이 없는 지역 패리티 심볼들에 대한 집합들이라고 하자. 이 때 위 집합들을 통해서 우리는 $\hat{\mathrm{G}}$에 의해 생성된 $(\mathrm{N}+\mathrm{t}(\delta-1),\mathrm{k})$ MDS 부호의 x개의 전역 패리티 심볼을 복구해낼 수 있다. 이 경우 A에서의 손실이 일어나지 않은 심볼들과 $\{\mathrm{P}_{k_1}^{\mathrm{local}},\ldots,\mathrm{P}_{k_x}^{\mathrm{local}}\}$에 의해서 복구할 수 있는 x개의 심볼을 통해 $\hat{\mathrm{G}}$에 의해 생성된 MDS 부호의 코드 워드 중 k개의 심볼을 얻을 수 있다. 이는 원래의 정보 심볼들 $\mathbf{m}$을 복구할 수 있음을 의미한다. □

위 증명을 통해 construction 1 을 통해 만들어진 $\left(\mathrm{n}=\mathrm{N}+\frac{\mathrm{kt}}{\mathrm{r}}(\delta-1),\mathrm{k},\mathrm{r},\mathrm{t},\delta\right)$ −부분접속복구 부호의 최소 거리는 제 4 장에서 보인 최소거리에 대한 상계의 등식을 만족함을 알 수 있고 이를 통해 제 4 장에서 보인 최소거리에 대한 상계가 tight 함을 알 수 있다.

쉬운 이해를 위해 Construction 1 의 한 예를 살펴본다. Construction 1 에 의해 설계된 (40, 15, 3, 2, 3)−부분접속복구 부호를 살펴본다. Construction 1 에 언급된 것처럼 먼저 생성 행렬 $\hat{\mathrm{G}}$를 가지는 systematic 한 $(\mathrm{N}+\mathrm{t},\mathrm{k})$ =(22,15)−MDS 부호를 가져온다. 그리고 원래의 정보를 $\mathbf{m}=(\mathrm{m}_1,\ldots,m_{15})$라 하고 (22, 15)−MDS 부호에 생성된 코드워드를 $\hat{\mathrm{c}}=(\mathrm{m}_1,\ldots,m_{15},p_1,\ldots,p_9)$ 라고 하자. 다음으로 $p_6,\ldots,p_9$에 해당하는 $\hat{\mathrm{G}}$의 $\mathrm{t}(\delta-1)=4$개의 열들을 $\frac{\mathrm{kt}}{r}$개씩 분리함으로써 정보 $\mathbf{m}$에 대한 (40, 15, 3, 2, 3)−부분접속복구 부호의 코드워드를 얻을 수 있다. $(l_1,\ldots,l_{20})$를 위에서 설명한 방식으로 얻은 지역 패리티 심볼들이라고 하자. 그리고 $\mathrm{p}_6=\sum_{i=1}^{15}a_i m_i$, $\mathrm{p}_7=\sum_{i=1}^{15}b_i m_i$, $\mathrm{p}_8=\sum_{i=1}^{15}a_i' m_i$, $\mathrm{p}_9=\sum_{i=1}^{15}b_i' m_i$ 이고 $a_i \neq a_i'$ 이고 $b_i \neq b_i'$ 라 가정하자. 여기서 p_6,p_8 그리고 p_7,p_9는 각각 Construction 1 에 앞서 가정한 동일한 R과 연관이 있음을 유의한다. 그러면 l_i를 그림 (~~~)와 같이 생성할 수 있다. $p_6,\ldots,p_9$에

의해 생성된 각 지역 패리티 심볼들의 그룹들은 $\mathrm{r}=3$ 의 크기로 $\frac{\mathrm{k}}{\mathrm{r}}=$ 5개의 $\{\mathrm{m}_1, \dots, m_{15}\}$의 파티션을 이루는 것을 확인할 수 있다.



$l_1 = a_1m_1 + a_2m_2 + a_3m_3$	$l_6 = b_1m_1 + b_5m_5 + b_6m_6$	$l_{11} = a'_1m_1 + a'_2m_2 + a'_3m_3$	$l_{16} = b'_1m_1 + b'_5m_5 + b'_6m_6$
$l_2 = a_6m_6 + a_7m_7 + a_8m_8$	$l_7 = b_4m_4 + b_7m_7 + b_{11}m_{11}$	$l_{12} = a'_6m_6 + a'_7m_7 + a'_8m_8$	$l_{17} = b'_4m_4 + b'_7m_7 + b'_{11}m_{11}$
$l_3 = a_{11}m_{11} + a_{12}m_{12} + a_{13}m_{13}$	$l_8 = b_8m_8 + b_9m_9 + b_{12}m_{12}$	$l_{13} = a'_{11}m_{11} + a'_{12}m_{12} + a'_{13}m_{13}$	$l_{18} = b'_8m_8 + b'_9m_9 + b'_{12}m_{12}$
$l_4 = a_4m_4 + a_9m_9 + a_{14}m_{14}$	$l_9 = b_3m_3 + b_{10}m_{10} + b_{14}m_{14}$	$l_{14} = a'_4m_4 + a'_9m_9 + a'_{14}m_{14}$	$l_{19} = b'_3m_3 + b'_{10}m_{10} + b'_{14}m_{14}$
$l_5 = a_5m_5 + a_{10}m_{10} + a_{15}m_{15}$	$l_{10} = b_2m_2 + b_{13}m_{13} + b_{15}m_{15}$	$l_{15} = a'_5m_5 + a'_{10}m_{10} + a'_{15}m_{15}$	$l_{20} = b'_2m_2 + b'_{13}m_{13} + b'_{15}m_{15}$

그림 4. (40, 15, 3, 2, 3) – 부분접속복구 부호의 코드워드

위 설정을 통해 (40, 15, 3, 2, 3)−부분접속복구 부호의 systematic 한 정보 심볼들이 각각 $\mathrm{t}=2$ 개의 서로소인 복구 집합으로부터 그 자신을 복구할 수 있고 특히 각 복구 집합에서 $\delta-1=2$ 개의 손실이 발생하더라도 관련된 정보 심볼을 충분히 복구할 수 있음을 알 수 있다. 예를 들어 m_1 의 경우 $\{\mathrm{m}_2, m_3, l_1, l_{11}\}$ 그리고 $\{\mathrm{m}_5, m_6, l_6, l_{16}\}$으로부터 각각 적어도 3 개의 심볼만으로 복구될 수 있다.

다음으로 설계한 (40, 15, 3, 2, 3)−부분접속복구 부호의 최소거리가 앞서 보인 $(\mathrm{n}, \mathrm{k}, \mathrm{r}, \mathrm{t}, \delta)$ −부분접속복구 부호의 최소거리 상계를 만족함을 확인할 수 있다.

$$\mathrm{d}_{min}(C) = n - k + 1 - (\left\lceil \frac{kt}{r} \right\rceil - t)(\delta - 1)$$

이는 (40, 15, 3, 2, 3)−부분접속복구 부호의 코드워드 중 임의의 $\mathrm{d}_{min}(C) - 1 = \mathrm{n} - \mathrm{k} - \left(\left\lceil \frac{kt}{r} \right\rceil - t\right)(\delta - 1) = 40 - 15 - (10 - 2) \times 2 = 9$ 개의 심볼에 손실이 일어나더라도 원래의 정보 $\mathbf{m}$를 복구할 수 있음을 보이면 충분하고 이는 앞선 최소거리 상계 만족을 보이는 증명과 같은 방식을 통해 쉽게 확인 할 수 있다.

제 6 장 결 론

실용적인 측면에서 가용도 개념을 도입할 경우 다수의 사용자가 동시에 여러 데이터에 병렬적으로 접근함으로써 동시에 데이터를 읽을 수 있다는 장점이 있다. 따라서 가용도를 고려한 부분접속복구 부호는 핫 데이터가 주로 저장된 분산 저장 시스템에 매우 유용하다. 특히 본 논문에서는 가용도만 아니라 정보 심볼들에 대한 복구집합들의 노드 손실까지 고려했기 때문에 기존의 가용도만을 고려한 부분접속복구 부호에 비해 손실에 대한 tolerance가 더 크다. 따라서 본 논문에서 제안하는 $(n,k,r,t,\delta)-$부분접속복구 부호는 손실이 자주 일어나며 동시에 접속할 필요가 있는 핫 데이터 사용에 더욱 적합하다.

본 논문에서는 각 복구집합들이 오직 $\delta-1$개의 패리티 심볼만을 가지는 선형 $(n,k,r,t,\delta)-$부분접속복구 부호에 대한 최소 거리 상계와 상계의 등호 조건을 만족하는 부호를 설계했다. 각 복구집합들의 패리티 심볼을 최소화하는 것은 전체 부호의 길이를 줄일 수 있기 때문에 부호율 측면에서 유리하다. 각 복구합들이 $\delta-1$ 개 이상의 패리티 심볼을 가지거나 혹은 비선형 (n,k,r,t,δ) 부분접속복구 부호와 같은 일반적인 $(n,k,r,t,\delta)-$부분접속복구 부호의 최소거리 상계와 그에 대한 achievability는 open problem으로 남긴다. 또한 본 논문에서 제안하는 부호는 동시에 모든 임의의 두 정보 심볼을 읽는 것에 대한 보장을 하지 않는다. 이 역시 흥미로운 연구주제가 될 수 있다.

참고 문헌

[1] 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.

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

[3] N. Prakash, G. M. Kamath, V. Lalitha, and P. V. Kumar, "Optimal linear codes with a local–error–correction property," *in Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2012, pp. 2776–2780.

[4] A. S. Rawat, D. S. Papailiopoulos, A. G. Dimakis, and S. Vishwanath, "Locality and Availability in Distributed Storage," *in Proc. IEEE Int. Symp. Inf. Theory (ISIT),* Honolulu, HI, USA, June. 2014, pp. 681–685.

[5] D.S. Papailiopoulos and A. G. Dimakis, "Locally repairable codes," full version available at http://tinyurl.com/82cucvd

Abstract

Locality and Availability with Multiple Erasure Tolerance in Distributed Storage

So Byeonghyun

Department of Electrical and Computer Engineering

The Graduate School

Seoul National University

Recently, as the amount of data to be handled by various systems has increased, the importance of distributed storage systems has increased. In a distributed storage system, there is a flaw in the node loss due to network problems or equipment problems. In this case, it is important to reconstruct the lost node through the non−lost node. At this time, the code used for distributed storage determines the performance of recovery. Depending on the use of the system, the factors that determine the performance of the codes used for distributed storage are different. Among them, 'locality' means the number of nodes needed to recover a lost node, and availability means the number of disjoint recovery sets that can recover a lost node.

In practical terms, when the ‘availability’ is introduced, it is advantageous that a plurality of users simultaneously access data at the same time and simultaneously read data. Therefore, locally repairable code considering availability is very useful for distributed storage systems where hot data is mainly stored.

In this paper, we propose a locally repairable code considering multi − node loss and availability in a distributed storage system. Moreover, we find the upper bound of minimum distance for the code. In order to show the achievability of the upper bound of the minimum distance of the newly proposed code, a code satisfying the equation for the bound is designed.

In particular, since we consider multiple node loss of recovery sets, we have more tolerance for loss than locally repairable code considering only the availability. Therefore, the (n, k, r, t, δ) − locally repairable code proposed in this paper is more suitable for using hot data which has frequent loss and frequent connection.

Keywords : Distributed Storage, Locally Repairable Code, Availability, Minimum Distance
Student Number : 2014−22562