JKIICE

Short Paper

한국정보통신학회논문지 Vol. 26, No. 3: 479~482, Mar. 2022

분산 학습으로의 적용을 위한 극소 부호의 확장 기법

Extension of Minimal Codes for Application to Distributed Learning

Dongsik Jo[1] · Jin-Ho Chung[1*]

[1*]Assistant Professor, Department of Electrical and Computer Engineering, University of Ulsan, Ulsan, 44610 Republic of Korea

ABSTRACT

Recently, various artificial intelligence technologies are being applied to smart factory, finance, healthcare, and so on. When handling data requiring protection of privacy, distributed learning techniques are used. For distribution of information with privacy protection, encoding private information is required. Minimal codes has been used in such a secret-sharing scheme. In this paper, we explain the relationship between the characteristics of the minimal codes for application in distributed systems. We briefly deals with previously known construction methods, and presents extension methods for minimal codes. The new codes provide flexibility in distribution of private information. Furthermore, we discuss application scenarios for the extended codes.

Keywords : Distributed system, block code, privacy, security

Ⅰ. 서 론

빅데이터(big data)와 사물 인터넷(IoT, Internet of Things)의 시대에는 다양하고 방대한 정보들이 각종 기기를 통해 전송되고 학습된다. 최근 연합학습(federated learning) 등과 같은 분산화된 학습 알고리즘들이 정보보호와 효율성을 동시에 만족시키는 대안으로 주목받고 있다 [1,2]. 이러한 학습 알고리즘에서는 각각의 사용자가 전체 정보를 가질 수 없지만, 최종적인 학습 효과는 전체 정보를 통해 학습한 것과 같은 효과를 내는 것을 목표로 한다. 따라서, 사용자들끼리 종속되지 않는 정보를 분배하고, 학습한 다음에 결합하는 것이 중요하다. 극소 부호(minimal code)는 블록 부호(block code)의 일종으로서 서로 다른 사용자들끼리 정보를 종속시키지 않으면서 최종적으로 합성된 정보를 얻어낼 수 있는 기밀 공유 기법(secret-sharing scheme)에 사용될 수 있다 [3]. 이를 위한 대수적인 설계 방법들이 꾸준히 제시되어 왔다 [4-7]. 또한, 연합학습 뿐만 아니라 블록체인과 같이 정보보호가 필요한 분야들에서 그 이용 방법들이 연구되고 있다 [8].

극소 부호는 통상적인 블록 부호와 마찬가지로 유한체 (finite field)의 구조와 성질을 이용해서 설계되었다. 이진 극소 부호 뿐만 아니라 소수 알파벳(prime alphabet)을 가지는 극소 부호들이 연구되어 왔다. 하지만 유한체의 구조적인 제한으로 인해 길이와 형태에 있어서 한정적인 경우에 대해서 설계가 제시되어 왔다. 따라서, 다양한 애플리케이션과 환경에 맞는 파라미터들을 가지는 극소 부호를 설계하는 것은 매우 중요한 문제이다.

본 논문에서는 극소 부호의 특징과 분산 시스템과의 연관성을 설명한다. 또한, 기존의 알려진 설계 방법들을 간단하게 다루고, 새로운 부호를 위한 결합 방법들을 제시한다. 또한, 이러한 결합 방법들이 적용될 수 있는 시나리오를 제안한다.

본 논문의 구성은 다음과 같다. II장에서는 극소 부호 관련 배경 지식들을 설명한다. III장에서는 극소 부호의 설계 방법을 제시하고, 이에 대한 적용 시나리오들을 제안한다. IV장에서는 설계된 극소 부호가 적용될 수 있는 시나리오들을 소개한다. 마지막으로 V장에서 결론을 맺는다.

Ⅱ. 배 경

유한체는 체(field)의 일종으로서 실수, 무리수 집합

Received 26 January 2022, **Revised** 7 February 2022, **Accepted** 17 February 2022

*** Corresponding Author** Jin-Ho Chung(E-mail:jinho@ulsan.ac.kr, Tel:+82-52-259-1644),
Assistant Professor, Department of Electrical and Computer Engineering, University of Ulsan, Ulsan, 44610 Republic of Korea

Open Access http://doi.org/10.6109/jkiice.2022.26.3.479 print ISSN: 2234-4772 online ISSN: 2288-4165

등과는 다르게 유한한 개수의 원소를 가진다. 체에서는 기본적으로 덧셈, 뺄셈, 곱셈, 나눗셈의 사칙 연산이 자유롭기 때문에 많은 블록 부호들이 유한체 위에서 설계되어 왔다. 본 장에서는 유한체와 극소 부호의 정의와 개념을 소개한다.

2.1. 유한체의 수학적 정의

유한체는 소수 p와 자연수 m에 대해서 p^m개의 원소와 두 개의 연산 덧셈과 곱셈을 가진다. 덧셈에 대한 항등원 0과 곱셈에 대한 순환 그룹으로 이루어진다 [9]. 곱셈에 대한 순환 그룹은 원시 원소(primitive element) α의 거듭제곱들인 $1=\alpha^0,\alpha,\alpha^2,...,\alpha^{p^m-2}$로 구성된다. 유한체는 덧셈에 대해서는 가환군(commutative group)이며, 0을 제외한 나머지 원소들은 곱셈에 대해서 순환군(cyclic group)을 이룬다. 이러한 유한체는 $\mathrm{GF}(p^m)$으로 표기된다. 유한체 $\mathrm{GF}(p^m)$은 $\mathrm{GF}(p)$ 상에서 정의되는 m차원의 벡터 공간으로도 해석될 수 있다. 유한체를 이용한 오류정정부호(error-correcting codes), 부울 함수(boolean function)의 설계 등에 관한 내용은 [10]을 참조할 수 있다.

2.2. 극소 부호의 정의

일반적으로 길이가 n인 선형 블록 부호(linear block code)는 수학적으로 n차원의 벡터 공간의 k차원 부분공간(subspace)으로 정의된다. 알파벳(alphabet)의 크기가 2인 경우에는 이진(binary) 부호라고 불리며, 그 이외의 경우에는 비이진(nonbinary) 부호라고 불린다. 부호어(codeword)는 k개의 정보 벡터(information vector)와 $k\times n$ 행렬의 곱으로 생성된다. 어떤 하나의 부호어의 서포트(support)는 0이 아닌 값을 가지는 좌표들의 집합으로 정의된다. 서포트의 집합 크기를 해밍 무게(Hamming weight)라 부른다. 극소 부호에서는 서로 다른 그림 1과 같이 임의의 부호어들의 서포트들이 서로 포함관계에 있지 않는 성질을 만족한다. 이러한 수학적 정의로 인해 극소 부호는 분산 시스템에서 기밀을 분배할 때 사용될 수 있다. 또한 분산 작업 이후에 정보를 합성할 때, 선형성을 이용해서 다시 전체 정보를 복원하는 것이 가능하다.

2.3. 대표적인 극소 부호

극소 부호의 개념과 기밀 공유 기법(secret-sharing scheme)으로의 응용에 대한 부분들은 Massey에 의해 제안되었다 [3]. Ashikhmin과 Barg는 극소 부호들과 기존 오류정정부호들의 관계를 분석하고, 극소 부호의 무게 분포(weight distribution) 등에 대한 중요한 성질들을 제시하였다 [4]. 또한, 선형 블록 부호가 극소 부호가 될 충분 조건을 다음 정리와 같이 제시하였다.

1	0	1	0	1	0	1

1	0	0	1	0	1	1

Fig. 1 Two codewords in minimal codes

***정리 1**: 유한체 $\mathrm{GF}(p)$ 상에서 정의된 선형 부호 C가 다음을 만족하면 C는 극소 부호이다:*

$$\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q}. \tag{1}$$

여기서, $w_{\min}$는 C의 부호어의 서포트 크기 중 가장 작은 값이고, $w_{\max}$는 가장 큰 값이다 [4].

정리 1은 극소 부호를 설계하는데 있어서 중요한 지침이 될 수 있지만, 동시에 부호어들의 정보량을 특정 범위로 제한할 수 있다. 이러한 충분 조건에 제한되지 않는 이진 극소 부호는 Ding 등에 의해 제안되었다 [5]. 최근에는 Mesnager 등이 정리 1의 범위 밖에 있는 비이진 부호들을 포함한 통합적인 극소 부호의 설계 방법을 제시하였다.

Ⅲ. 극소 부호의 확장 방법

본 장에서는 기존의 극소 이진 부호를 이용해서 확장된 극소 이진 부호를 설계하는 방법을 제시한다.

3.1. 이진 극소 부호의 2배 확장

길이가 N이고 M개의 부호어를 갖는 극소 부호 C의 부호어들 $\underline{x}_1,...,\underline{x}_M$은 각각 길이 N의 벡터로 다음과 같이 나타낼 수 있다:

$$\underline{x}_i = \{x_i(0),x_i(1),...,x_i(N-1)\},\ i=1,...,M. \tag{2}$$

확장된 길이 $2N$의 부호어 $\underline{y}_i$를 다음과 같이 정의하자:

$$\underline{y}_i(t)=\begin{cases}x_i(\lfloor t/2\rfloor), & 2|t\\ x_i(N-1-\lfloor t/2\rfloor), & \text{otherwise.}\end{cases} \quad (3)$$

여기서 $i=1,...,M$이다. 다음과 같이 새로운 부호 Y를 정의하자:

$$\mathrm{Y}=\{\underline{y}_1,...,\underline{y}_M\}. \quad (4)$$

확장된 부호 Y는 길이가 $2N$이고 M개의 부호어를 갖는 부호이다. 또한, 원래 부호어와 인덱스(index)를 거꾸로 읽은 부호어를 조합하여 쉽게 생성할 수 있다. 기존의 부호어들 $\underline{x}_1,...,\underline{x}_M$ 사이에 선형성(linearity)이 성립하고, $\underline{y}_1,...,\underline{y}_M$는 홀수와 짝수 인덱스(index) t에 대해서 각각 선형성이 성립한다. 따라서, 새로운 부호어들의 집합도 선형성을 만족시킨다. 또한, 원래 부호 C의 성질로부터 Y의 부호어들도 서로 서포트가 종속되지 않는다는 것을 추론할 수 있다.

3.2. 이진 극소 부호의 k배 확장

길이가 N_1이고 M_1개의 부호어를 갖는 극소 부호 C_1의 부호어들을 $\underline{x}_{1,1},...,\underline{x}_{1,M_1}$, 길이가 N_2이고 M_2개의 부호어를 갖는 극소 부호 C_2의 부호어들을 $\underline{x}_{2,1},...,\underline{x}_{2,M_2}$이라고 하자. 여기서 N_1과 N_2는 서로 소(relatively prime)이라고 가정한다. 새로운 부호어 $\underline{z}_i$를 다음과 같이 정의하자:

$$\underline{z}_{i,j}(t)=\underline{z}_{i,j}(t_1,t_2)=I\big(\underline{x}_i(t_1),\underline{y}_j(t_2)\big). \quad (5)$$

여기서 $1\le i\le M_1$, $1\le j\le M_2$이고, 시간에 대한 인덱스는 $0\le t\le N_1N_2-1$이다. 또한, $t_1=t \bmod N_1$이고 $t_2=t \bmod N_2$이다. 함수 $I(a,b)$는 a와 b가 모두 1이면 1의 값을 가지고, 나머지 경우에는 0의 값을 가진다. 따라서, $\underline{z}_{i,j}(t)$가 1의 값을 가질 수 있는 t의 개수는 $\underline{x}_{1,i}$의 해밍 무게와 $\underline{x}_{2,j}$의 해밍 무게의 곱과 같다. 또한, 모든 i와 j의 조합에 대해서 $\underline{z}_{i,j}$를 생성할 수 있다. 다음과 같이 새로운 부호 Z를 정의하자:

$$\mathrm{Z}=\{\underline{z}_{i,j}|1\le i\le M_1 \text{ and } 1\le i\le M_2\}. \quad (6)$$

부호 Z의 부호어들은 t_1과 t_2의 값에 따라 기존 부호의 성질을 그대로 물려받기 때문에 서로 다른 부호어들끼리 서포트가 종속되지 않는 것을 알 수 있다. 또한, t_1과 t_2 각각에 대해서 선형성이 성립하고 N_1과 N_2가 서로 소이기 때문에 t에 대해 선형성이 성립한다. 새로운 부호 Z의 부호어의 수는 M_1M_2개가 되고, 각 부호어의 해밍 무게는 두 구성 부호의 해밍 무게의 곱과 같다. 알려진 이진 극소 부호들은 대부분 길이가 의 형태를 가지기 때문에 서로 소인 두 개의 길이를 찾는 것은 또다른 문제라고 할 수 있다.

Ⅳ. 극소 부호의 적용

새롭게 설계된 부호들은 기본적으로 기존 부호의 무게 분포에 의해 성질이 결정된다. 하지만 III.1에서 구성 부호들의 조합을 바꿈으로 인해 새로운 무게 분포들을 생성할 수 있다. 표 1에서는 그러한 조합 중 하나에 대한 무게 분포를 실험적으로 구한 것을 보여준다.

Table. 1 An example of difference between weight distributions of the original code and an extended code

Code	[5]	3.1
Possible weights	0,14,30,32,38	0,28,60,62,64,68,76
Distribution	1,1,49,63,14	1,1,30,28,44,10,10,4
Restriction in (1)	No	No

표 1에서 보는 것과 같이 더 다양한 조합의 무게 분포를 가지는 부호를 합성하는 것이 가능하다. 이를 통해 더욱 다양한 정보량의 분산 조합을 생성할 수 있을 것이다.

3.1에서 설계된 새로운 부호는 두 개의 분산 학습 시스템의 정보들을 하나로 합치는 경우에 사용될 수 있다. 각 시스템에서 분산된 정보들의 형태가 변형되지 않고,

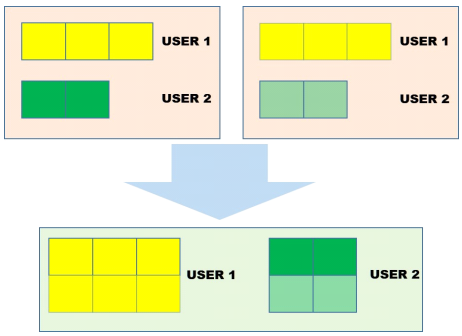

Fig. 2 Merging information sets

기존 부호어에 그대로 포함될 수 있다. 또한 새로운 부호어들끼리 서로 종속되지 않기 때문에, 여전히 기밀은 분산된 형태를 가진다. 그림 2는 이러한 형태의 부호의 적용 시나리오를 나타낸다. 두 개의 서로 다른 시스템 혹은 기관에서 실행하던 데이터들을 병합하는 경우에 대해 사용될 수 있다.

그림 3에서는 3.2에서 제시된 설계 방법의 적용 가능한 시나리오를 나타내었다. 컴퓨팅 자원의 증가로 인해 다룰 수 있는 정보의 양이 많아지고, 참여자가 많아질 때 이러한 시나리오를 적용해 볼 수 있을 것이다. 3.2에서 제시된 서로 소인 길이를 가지는 부호를 사용하지 않는 경우에 두 시스템에 대한 결합 방법을 찾는 것은 새로운 문제가 될 것이다.

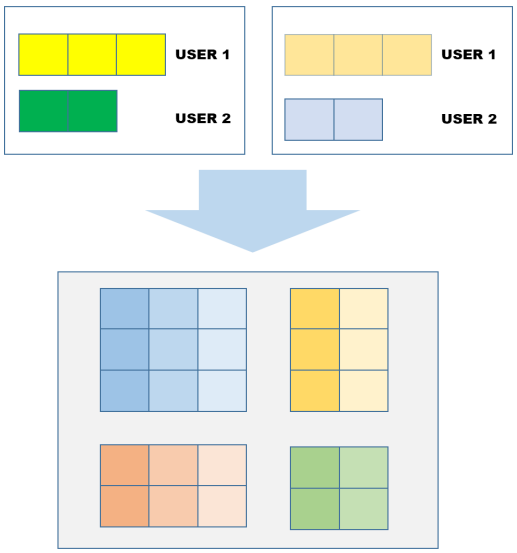

Fig. 3 Extension of codes

Ⅴ. 결 론

본 논문에서는 극소 부호의 확장 방법을 제시하고, 확장된 부호들의 성질에 대해서 분석하였다. 확장된 부호들은 길이 뿐만 아니라 해밍 무게의 측면에서도 증가된 것을 확인할 수 있으며, 부호어들이 서로 종속되지 않는 특성을 가진다. 또한, 다양한 조합을 통해 새로운 해밍 무게 분포를 만들어 낼 수 있음을 실험적으로 확인하였다. 향후 연구는 기존 부호에 대한 대수적 분석을 통해 더욱 다양한 시스템 파라미터에 맞출 수 있는 새로운 부호의 설계와 실제 분산 학습 시스템의 구현을 통한 검증 작업이 될 것이다.

ACKNOWLEDGEMENT

This paper was supported by Samsung Research Funding & Incubation Center of Samsung Electronics under Project Number SRFC-TB1803-03.

REFERENCES

[1] Federated Learning: Collaborative Machine Learning without Centralized Training Data. https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

[2] Federated Learning powered by NVIDIA Clara. https://developer.nvidia.com/blog/federated-learning-clara/

[3] J. Massey, “Minimal codewords and secret sharing,” in *Proc. 6th Joint Swedish –Russian Workshop on Information Theory*, pp.276 – 279, Aug. 22 – 27, 1993.

[4] A. Ashikhmin and A. Barg, “Minimal Vectors in Linear Codes,” *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 2010-2017, Sep. 1998.

[5] C. Ding, Z. Heng and Z. Zhou, “Minimal binary linear codes,” *IEEE Transactions on Information Theory*, vol. 64, no. 10, pp. 6536-6545, Oct. 2018.

[6] G. Xu and L. Qu, “Three classes of minimal linear codes over the finite fields of odd characteristic,” *IEEE Transactions on Information Theory*, vol. 65, no. 11, pp. 7067-7078, Nov. 2019.

[7] S. Mesnager, Y. Qi, H. Ru, and C. Tan, “Minimal linear codes from characteristic functions,” *IEEE Transactions on Information Theory*, vol. 66, no. 9, pp. 5404-5413, Sep. 2020.

[8] G. N. Alfarano, M. Borello, and A. Neri, “A geometric characterization of minimal codes and their asymptotic performance“, *American Institute of Mathematical Sciences*, vol. 16, no. 1. pp. 115-133, Jan. 2022.

[9] R. Lidl and H. Niederreiter, *Finite Fields*, 1st ed.; Publisher: Cambridge University Press, UK, 1997.

[10] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*, 2nd ed.; Publisher: Wiley, US, 2021.