Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 21(4): 300-305, Dec. 2023 Regular paper

Design of Block Codes for Distributed Learning in VR/AR Transmission

Seo-Hee Hwang[1], Si-Yeon Pak[1], Jin-Ho Chung[2], Daehwan Kim[2]*, and Yongwan Kim[3], *Member, KIICE*

[1]Department of AI Convergence, University of Ulsan, Ulsan 44610, Republic of Korea
[2]Department of Electrical, Electronic, and Computer Engineering, University of Ulsan, Ulsan 44610, Republic of Korea
[3]VR/AR Content Research Section, Communications & Media Research Laboratory, Electronics and Telecommunications Research Institute (ETRI), Daejeon 34129, Republic of Korea

Abstract

Audience reactions in response to remote virtual performances must be compressed before being transmitted to the server. The server, which aggregates these data for group insights, requires a distribution code for the transfer. Recently, distributed learning algorithms such as federated learning have gained attention as alternatives that satisfy both the information security and efficiency requirements. In distributed learning, no individual user has access to complete information, and the objective is to achieve a learning effect similar to that achieved with the entire information. It is therefore important to distribute interdependent information among users and subsequently aggregate this information following training. In this paper, we present a new extension technique for minimal code that allows a new minimal code with a different length and Hamming weight to be generated through the product of any vector and a given minimal code. Thus, the proposed technique can generate minimal codes with previously unknown parameters. We also present a scenario wherein these combined methods can be applied.

Index Terms: Blockchain, Distributed Learning, Federated Learning, VR/AR transmission, Virtual performances

I. INTRODUCTION

When the reactions of an audience watching a remote virtual performance are to be transmitted to a server, the data must be sufficiently compressed in such a way that it can be easily restored on the server. In such scenarios, the server must aggregate data from remote viewers and learn group-level reactions or movements that encompass the whole body, actions, and facial expressions. Furthermore, the transmission of this information requires distribution codes, necessitating distributed coding. Distributed learning algorithms, such as federated learning, have recently gained attention as alternatives that satisfy both information security and efficiency requirements [1,2]. In distributed learning, no individual user has access to complete information, with the objective being to achieve a learning effect similar to that when learning with the entire information. It is therefore important to distribute interdependent information among users and subsequently aggregate this information following training.

Minimal code is a type of linear block code [3] used in various applications such as secret-sharing schemes. In a secret sharing scheme, confidential information is distributed and stored among users so that only a specific authorized

Received 15 August 2023, **Revised** 18 October 2023, **Accepted** 21 October 2023
***Corresponding Author** Daehwan Kim (E-mail: daehwankim@ulsan.ac.kr)
Department of Electrical, Electronic, and Computer Engineering, University of Ulsan, Ulsan 44610, Republic of Korea

Open Access https://doi.org/10.56977/jicce.2023.21.4.300 print ISSN: 2234-8255 online ISSN: 2234-8883

subset of users can reconstruct all of it [4].

The distribution of these secrets can be mathematically defined using minimal code. The most important characteristic of such code is that the code word of one user must not be dependent on that of another; i.e., the support of one code word should not be a subset of that of another. Algebraic design methods that satisfy this requirement have previously been proposed [5-8]. Minimal code is expected to become applicable not only in federated learning, but other fields where information dispersion is required, such as blockchain technology. Furthermore, the design of new minimal code techniques is considered an interesting topic in the field of coding theory.

In [5], Aschikhmin and Barg proposed sufficient conditions for a linear block code to be minimal, and presented a method for minimum distance decoding. Mesnager et al. introduced methods for designing minimal codes using characteristic functions defined in finite fields [8]. Various minimal codes have also been designed under the conditions defined by Aschikhmin and Barg [9-11]. Chang and Hyun discovered a design method for minimal codes that is not restricted by sufficient conditions [12]. Ding et al. not only derived the conditions for minimality in binary codes, but also designed a class of infinite binary minimal codes [6]. Heng et al. discovered various binary and ternary minimal codes [13]. Bartoli and Bonini proposed a generalized design method and an inductive extension method for non-binary minimal codes [14]. Most existing minimal codes were designed based on the structures and properties of finite fields, making them limited in length. Instead, it is desirable to design minimal code with new parameters that can accommodate various information lengths and communication environments.

In this paper, we present a new extension technique for block codes for VR/AR transmissions. We briefly examined existing design methods to derive combination methods for new codes. Using our technique, a minimal code with a new length and Hamming weight can be generated through the product of any vector and existing minimal code, thereby yielding minimal codes with previously unknown parameters. We also analyzed the weight properties of the new codes and compared them with those of previously designed codes.

The remainder of this paper is organized as follows. In Section II, we provide an overview of background knowledge pertaining to minimal codes. In Section III, we present a design method based on a combination of distinct minimal codes, and examine properties associated with the weight distribution and minimum distances of the new minimal codes. In Section IV, we introduce scenarios in which the designed minimal codes can be applied, and subsequently present concluding remarks.

II. BACKGROUND

A finite field is a type of field that is distinct from a set of real numbers because it consists of a finite elements [15]. Many block codes have been designed over finite fields, as these fields are suitable for basic arithmetic operations. In the following subsections, we introduce the definitions and concepts of finite fields, linear codes, and minimal codes.

A. Mathematical Definitions of Finite Fields, Linear Block Codes, and Minimal Codes

A finite field comprises p^m elements, where p is a prime number and m is a positive integer. The field is equipped with two operations – addition and multiplication – and composed of an additive identity element 0 and a cyclic group under multiplication [9]. This cyclic group consists of powers of the primitive element α, denoted as $1=\alpha^0$, α, α^2, ..., α^{p^m-2}. A finite field represents a commutative group under addition, where all elements except 0 form cyclic groups under multiplication. The finite field $GF(p^m)$. can also be interpreted as an m-dimensional vector space over $GF(p)$. Information regarding error-correcting codes and the design of Boolean functions using finite fields can be found in [10].

In the finite field F_{p^m}, a linear block code C of length N is defined as the K-dimensional subspace of an N-dimensional vector space. The (N,K)-linear block code C is represented by a set of vectors:

$$\mathrm{C} = \{\underline{x}_0, \underline{x}_1, \dots, \underline{x}_{M-1}\}. \tag{1}$$

In this representation, each vector $\mathbf{x}_i$, where $0 \le i \le M-1$, is called a codeword. M represents the number of distinct codewords, which corresponds to the number of users. K, which represents the length of the informative section, is equivalent to the number of independent vector components. Codewords are generated by the multiplication of K information vectors by a $K \times N$ matrix. Each element of a vector can be represented as follows:

$$\underline{x}_i = (x_i[0], x_i[1], \dots, x_i[N-1]). \tag{2}$$

According to the properties of linear codes, the sum of two codewords $\underline{x}_i + \underline{x}_j$ becomes another codeword $\underline{x}_k$ that belongs to C. Moreover, for any element $\alpha \in F_{p^m}$, the scalar multiplication $a\underline{x}_i$ also yields another codeword $\underline{x}_{k'}$ belonging to C. The support of codeword $\underline{x}_i$ is defined by the following set:

$$\mathrm{supp}(\underline{x}_i) = \{0 \le n \le N-1 : x_i[n] \ne 0\}. \tag{3}$$

This support represents a set of coordinates that have nonzero values. The Hamming weight of the codeword $\underline{x}_i$ is defined as the size of the support set of $\underline{x}_i$. If the support of

any codeword $\underline{x}_i$ in the (N,K)-linear block code C is not a subset of the support of another codeword $\underline{x}_j$, then C is referred to as the (N,K)-minimal code. As shown in Fig. 1, the supports of any two distinct words in a minimal code are mutually exclusive. In such cases, there always exists a position where $\underline{x}_i$ is nonzero and $\underline{x}_j$ is zero, and vice versa.

Codewords
0 0 0 0 0
0 1 0 1 0
1 1 1 0 1

Fig. 1. Three codewords within a minimal code

B. Backgrounds on Minimal Codes

The concept of a minimal code and its application to secret sharing schemes were first proposed by Massey [3]. Ashikhmin and Barg subsequently analyzed the relationship between minimal codes and existing error-correcting codes, obtined the significant properties of minimal codes, such as weight distribution, and explored various aspects related to minimal codes [4]. Furthermore, they derived the sufficient conditions for a linear block code to be minimal, as stated in the following theorem:

Theorem 1 [4]. If a linear block code C over the finite field F_{p^m} satisfies the following condition, then C is a minimal code:

$$\frac{w_{\min}}{w_{\max}} > \frac{p^m - 1}{p^m} \tag{4}$$

where $w_{\min}$ and $w_{\max}$ are the minimum and maximum support sizes among all codewords in C, respectively.

Although Theorem 1 can serve as an important guideline for designing minimal code, it imposes limitations on the range of Hamming weights among code words, restricting the information capacity to a specific range.

To address this limitation, non-binary minimal codes, as well as binary minimal codes that are not restricted by the conditions of Theorem 1, were proposed by Ding et al. [6]. Furthermore, Mesnager et al. introduced integrated approaches for designing minimal codes, encompassing both binary and non-binary codes that fall outside the scope of Theorem 1 [8]. In this context, codes with an alphabet size of two are referred to as binary, whereas those with a larger alphabet are referred to as non-binary. The design of binary and non-binary distribution codes is an important topic, as although the design schemes are similar, their applications are considerably different.

III. DESIGN AND APPLICATION OF DISTRIBUTION CODES

A. New Minimal Codes

1) Extension Methods for New Minimal Codes

For $0 \le n \le N-1$, we define an arbitrary nonzero vector in F_{p^m}, with a length $k \ge 2$, as $\underline{r}_a = (r_a(0), r_a(1), \ldots, r_a(k-1))$. Theorem 2 presents a new minimal code for length kN.

Theorem 2. Let us define codeword $\underline{y}_i$ of length kn as follows:

$$y_i[ak + b] = r_a[b] \cdot x_i[a] \tag{4}$$

where $0 \le n \le N-1$ and $0 \le b \le l-1$. The new code $E = \{\underline{y}_0, \underline{y}_1, \ldots, \underline{y}_{M-1}\}$ is a (kN,K)-minimal code.

Proof: First, we prove that E is a linear code. For any two integers i and j between 0 and $M-1$, the summation

$$y_i[ak + b] + y_j[ak + b] \tag{5}$$

becomes $y_k[a,b]$ by the linearity of the original codewords. Furthermore,

$$ay_i[a, b] = r_a[b](ax_l[a]) = y_l[a, b] \tag{6}$$

for some l. Therefore, E is linear. Next, we prove the minimality of E. Because $\underline{r}_a$ is a nonzero vector,

$$y_i[a] = r_a[b]x_i[a] \neq 0 \tag{7}$$

and there exists $0 \le b \le l-1$ such that

$$y_j[a] = r_a[b]x_j[a] = 0 \tag{8}$$

Therefore, the support of codeword $\underline{y}_i$ is not a subset of the support of codeword $\underline{y}_j$. We can similarly show that the support for $\underline{y}_j$ is not a subset of that for $\underline{y}_i$. Therefore, E is a minimal code. ■

In Theorem 2, each codeword $\underline{y}_i$ can be expressed as the concatenation of vectors obtained by multiplying each element of the original codeword $\underline{x}_i$ by corresponding constants from $\underline{r}_a$. Fig. 2 illustrates this extension method for minimal codes.

$x_i(0) \times r_a(0)$	$x_i(1) \times r_a(1)$	...	$x_i(N-1) \times r_a(N-1)$

Fig. 2. Extension method for minimal codes

2) Weight Properties of New Minimal Code

The weight distribution of the new code E is determined by the weight distributions of the individual vectors $\underline{s}_a$ and the original code C. In the simplest case, when the Hamming weight of each $\underline{s}_a$ is fixed to 1, the weight distribution of E will match that of C. Moreover, the maximum Hamming

weight of $\underline{s}_a$ is equal to the length l. When all $\underline{s}_a$ have a fixed weight of l, each weight value in the original distribution is multiplied by l. Because the Hamming weight of each $\underline{s}_a$ can be arbitrarily selected between 1 and l, various weight distributions can be obtained depending on the variation in the Hamming weights of $\underline{s}_a$ with respect to α. In addition, it is evident that extending a code beyond the constraints of Theorem 1 enables the generation of a new code beyond those constraints.

In linear codes, the minimum distance – which represents the distance between code words – is an important performance metric associated with error probability. Owing to linearity, the minimum distance is equal to the minimum Hamming weight among the code words [3]. Assuming that the original minimum distance of the minimal code C is denoted as d, the minimum distance of the new code E can be observed to range from d to ld with respect to $\underline{s}_a$. Therefore, the ratio between the length and minimum distance is maintained as the length is extended. Table 1 provides examples of the lengths, weights, and minimum distances of extended codes.

Table 1. Sample new parameters of minimal codes (N: length, K: information length, d: minimum distance)

	N	K	d	Number of distinct weights
Original Codes	511	10	120	3
Extended Codes	5110	10	120~1200	3~30

B. Extended Minimal Binary Codes

1) Double Extension of Binary Minimal Codes

Let us define the extended length $2N$ codeword $\underline{y}_i$ as follows:

$$\underline{y}_i(t) = \begin{cases} x_i(\lfloor t/2 \rfloor), & t \text{ is even;} \\ x_i(-\lfloor t/2 \rfloor), & \text{otherwise.} \end{cases} \tag{9}$$

where $i = 1, 2, ..., M$. We now can define the extended code Y as follows:

$$Y = \left\{ \underline{y}_1, \ldots, \underline{y}_M \right\}. \tag{10}$$

Here, Y has a length of $2N$ and contains M code words, which can be easily generated by combining original code words with their reverse-indexed counterparts. The original codewords $\underline{x}_1$, ..., $\underline{x}_M$ hold true mutual linearity, whereas each of the new codewords $\underline{y}_1$, ..., $\underline{y}_M$ holds true linearity for odd and even indices. Therefore, the set of new code words in Y satisfies linearity. Furthermore, based on the properties of the original code C, the codewords in Y and their supports can be inferred to be mutually independent.

2) Interleaved Extension of Binary Minimal Codes

Our code construction is based on the interleaving of two different minimal codes, with the indices of a new code determined by a combination of the two codes. Consider a minimal code C_1 with a length of N_1 that contains M_1 codewords denoted as $\underline{x}_{1,1}$, ..., $\underline{x}_{1,M_1}$, and a minimal code C_2 with a length of N_2 that contains M_2 codewords denoted as $\underline{x}_{2,1}$, ..., $\underline{x}_{2,M_2}$. The new code word $\underline{z}_i$ can be defined as

$$\underline{z}_{i,j}(t) = \underline{z}_{i,j}(t_1, t_2) = \underline{x}_i(t_1) \odot \underline{y}_i(t_2). \tag{11}$$

where $\odot$ is the binary AND operator, $0 \le i \le M_1$, $0 \le i \le M_2$, and $0 \le t \le N_1 N_2 - 1$. Furthermore, $t_1 = t \ mod \ N_1$ and $t_2 = t \ mod \ N_2$. Consequently, the value of $\underline{z}_{i,j}(t)$ can be 1 for the number of t values that equals the product of the Hamming weights of $\underline{x}_{1,i}$ and $\underline{x}_{2,j}$. Furthermore, it is possible to generate $\underline{z}_{i,j}$ for all combinations of i and j. Define the new code Z as follows:

$$Z = \left\{ \underline{z}_{i,j} \middle| \, 1 \le i \le M_1 \text{ and } 1 \le i \le M_2 \right\}. \tag{12}$$

The codewords of Z inherit properties of the original code depending on the values of t_1 and t_2, indicating that the support of the different codewords remains independent. Moreover, as linearity holds for t_1 and t_2 separately, and N_1 and N_2 are relatively prime, linearity also holds with respect to t. The number of codewords in Z is $M_1 M_2$, and the Hamming weight of each codeword is equal to the product of the Hamming weights of the two constituent codes. Finding two relatively prime lengths is another challenging problem, as most known binary minimal codes have lengths in the form of $p^m - 1$.

C. Application of Minimal Codes

The newly designed code is fundamentally determined by the weight distribution of the original code. However, by altering the combinations of the constituent codes, new weight distributions can be generated, as discussed in III.B.1. Table 2 presents the experimentally obtained weight distributions for each combination.

Table 2. Weight distributions of a sample original code and its extension

Code	Lengths	No. of Possible Weights
Original	255	6
Extended	510	12

As seen from the table, codes with a wider range of weight distributions can be synthesized by combining existing codes. This enables a greater variety of information combinations, increasing the diversity of dispersed information.

The newly designed code from III.B.1 can be utilized to

combine information from two distributed learning systems into a single entity. The dispersed forms of information from each system can be incorporated into existing code words without modification. Moreover, because the new codewords remain mutually independent, confidentiality is maintained in a dispersed formIf the codes with relatively prime lengths presented in III.B.2 are not used, finding a method to combine data from the two systems becomes an additional challenge.

IV. CONCLUSIONS

In this study, we propose a method that extends minimal codes to an arbitrary multiple length by increasing the Hamming weight. Furthermore, we demonstrated an increase in the minimum distance of the code; thus, a new Hamming weight distribution can be generated through various combinations. Our extension method can be applied to codes with new designs that can accommodate various parameters.

ACKNOWLEDGEMENTS

This research was supported by the Culture, Sports, and Tourism R&D Program through a Korea Creative Content Agency grant, funded by the Ministry of Culture, Sports, and Tourism in 2023. (Project name: Development of Virtual Reality Performance Platform Supporting Multiuser Participation and Real-Time Interaction, Project Number: R2021 040046)

REFERENCES

[1] B. McMahan and D. Ramage, Federated Learning: Collaborative Machine Learning without centralized training data, *Google Research*, Apr. 2017. [Online], Available: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html.

[2] Y. Wen, W. Li, H. Roth, and P. Dogra, Federated Learning powered by NVIDIA Clara, *NVIDIA Developer*, Dec. 2019. [Online], Available: https://developer.nvidia.com/blog/federated-learning-clara/.

[3] W. E. Ryan, S. Lin, *Channel Codes*, 2nd ed. Cambridge University Press, UK, 2009.

[4] J. L. Massey, "Minimal codewords and ecret sharing," in *Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, Stockholm, Sweden, pp. 276-279. 1993.

[5] A. Ashikhmin and A. Barg, "Minimal vectors in linear codes," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 2010-2017, Sep. 1998. DOI: 10.1109/18.705584.

[6] 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. DOI: 10.1109/TIT.2018.2819196.

[7] 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. DOI: 10.1109/TIT.2019.2918537.

[8] 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. DOI: 10.1109/TIT.2020.2978387.

[9] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 2089-2102, Jun. 2005. DOI: 10.1109/TIT.2005.847722.

[10] J. Yuan and C. Ding, "Secret sharing schemes from three classes of linear codes," *IEEE Transactions on Information Theory*, vol. 52, no. 1, pp. 206-212, Jan. 2006. DOI: 10.1109/TIT.2005.860412.

[11] K. Ding and C. Ding, "A class of two-weight and three-weight codes and their applications in secret sharing," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 5835-5842, Nov. 2015. DOI: 10.1109/TIT.2015.2473861.

[12] S. Chang and J. Y. Hyun, "Linear codes from simplicial complexes," *Designs, Codes and Cryptography*, vol. 86, no. 10, pp. 2167-2181, Oct. 2018.

[13] Z. Heng, C. Ding, and Z. Zhou, "Minimal linear codes over finite fields," *Finite Fields and Their Applications*, vol. 54, pp. 176-196, Nov. 2018. DOI: 10.1016/j.ffa.2018.08.010.

[14] D. Bartoli and M. Bonini, "Minimal linear codes in odd characteristic," *IEEE Transactions on Information Theory*, vol. 65, no. 7, pp. 4152-4155, Jul. 2019. DOI: 10.1109/TIT.2019.2891992.

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

Seo-Hee Hwang

She is currently pursuing a Bachelor's degree in AI convergence at the University of Ulsan. Her research interests include graph representation learning, biomedical engineering with deep learning, and security.

Si-Yeon Pak

She is currently pursuing a Bachelor's degree in AI convergence at the University of Ulsan. Her research interests include machine learning for communication, graph machine learning, and coding theory.

Jin-Ho Chung

He received B.S., M.S., and Ph.D. degrees in electronics and electrical engineering from the Pohang University of Science and Technology (POSTECH), Pohang, Korea, in 2005, 2007, and 2011, respectively. He was a postdoctoral researcher in Communications and Signal Design Laboratory, Department of Electrical Engineering, POSTECH from March 2011 to February 2013. He was an Assistant Professor at the School of Electrical and Computer Engineering of the Ulsan National Institute of Science and Technology from February 2013 to February 2021. He is currently working as an Associate Professor at the School of Electronic, Electrical, and Computer Engineering at the University of Ulsan. His research interests include information theory for machine learning, physical layer security, and coding theory.

Daehwan Kim

He completed his Ph.D. in computer science and engineering at the Pohang University of Science and Technology in 2011. He is currently a professor at the School of IT Convergence at the University of Ulsan. His main research interests include computer vision, AI, deep learning, and VR/AR.

Yongwan Kim

He completed a B.S. degree (1996) in Electronics Engineering at Inha University, an M.S.E. (1998) in Information and Communications Engineering at GIST, and a Ph.D. (2014) in Computer Science at the Korea Advance Institute of Science and Technology (KAIST), Korea. He joined the Electronics and Telecommunications Research Institute (ETRI) in 1998 and has been working as a principal researcher of the Virtual Reality Research Team since then. His research interests include virtual reality, haptics, and human-computer interaction.