A Generalization of the Parallel Error Correcting Codes

Hideki Yagi[1]
Media Network Center
Waseda University
Shinjuku-ku, Tokyo 169-8050, Japan
Email: yagi@hirasa.mgmt.waseda.ac.jp

Toshiyasu Matsushima
School of Science and Engineering
Waseda University
Shinjuku-ku, Tokyo 169-8555, Japan

Shigeichi Hirasawa
School of Science and Engineering
Waseda University
Shinjuku-ku, Tokyo 169-8555, Japan

Abstract — **This paper generalizes parallel error correcting codes proposed by Alshwede et al. over a type of multiple access channels called a parallel channel. The generalized parallel error correcting codes can handle with more errors compared with the original ones. We show construction methods of independent and non-independent parallel error correcting code and decoding methods. We derive some bounds about the size of respective parallel error correcting code.**

I. Introduction

Coding schemes for multiple access channels have been well-discussed. Especially, for a multiple access adder channel, many studies about code constructions have been conducted [2, 3, 4, 5, 6]. In contrast to the conventional works, R. Ahlswede et al. have considered a new multiple access channel model called a **parallel channel** and discussed coding schemes for this channel [1].

The parallel channel is a bundle of lines through which messages are transmitted parallelly. When messages are transmitted through the channel, highly correlated errors occur in respective lines. For example, in a parallel port of a computer, messages are transmitted through several lines simultaneously and disturbed by magnetic noise, etc. At that time, messages at a time instance may be equally disturbed. Namely, if an error occurs in a line, the probability that an error occurs in its neighbor lines becomes high. Ahlswede et al. have focused on this fact and define a t-**parallel error** which indicates the same errors with the Hamming weight less than or equal to t in all lines of the channel. They have derived necessary and sufficient conditions of code correcting the t-parallel error. They have given code constructions of the optimal parallel error correcting codes with the largest size for given a code length and t. Their work gives a bunch of suggestions, however the channel model in [1] is not sufficient for practical applications.

In this paper, we generalize the concept of Ahlswede's parallel channel, by allowing some random errors besides the same errors in all lines. Subsequently, we derive necessary and sufficient conditions of parallel error correcting codes whose line codes are dependent each other. We show a code construction that achieves the maximal size for a given code length and t. Then, we consider linear parallel error correcting codes whose line codes are independent and derive a bound of the maximal achievable rate (pair of dimensions of all line codes [1, 5]). Although the results of this paper are applicable to a general m senders model for any $m \geq 2$, the case of $m = 2$ is essential and important. Therefore, as discussed in [1], we first focus on the case of $m = 2$, and then we generalize the results to a general m senders model.

This paper is organized as follows: in Sect. II, we describe a new model and some definitions. Next, in Sect. III, we derive necessary and sufficient conditions for non-linear parallel error correcting codes whose line codes are dependent each other. Then in Sect. IV, we discuss linear independent parallel error correcting codes. In Sect. V, we generalize the results in Sect. III, IV for a general m senders model. Finally in Sect. VI, we give the concluding remarks.

II. Model and Definitions

In this section, we describe the channel model of this paper. In this paper, the two senders model is essential and generalization of results of the two senders case to a general $m(\geq 2)$ senders case is not so difficult. Then, we here describe the two senders model and derive results for it.

We denote input alphabets from two senders by $\mathcal{X}$ and $\mathcal{Y}$. In this paper, we assume that the set of the input and output alphabets is a finite field $GF(q)$ where q is a power of a prime.

Assume that a codeword of a code $\mathcal{C} \subset \mathcal{X}^n \times \mathcal{Y}^n$ of length $2n$ is input to the parallel channel where the first n symbols of the codeword are a sender's message and the last n symbols of it are another sender's message. In the channel, an error vector $(\boldsymbol{e}, \boldsymbol{\epsilon}) \in GF^n(q) \times GF^n(q)$ such that $w_H(\boldsymbol{e}) \leq t + s, w_H(\boldsymbol{\epsilon}) \leq t + s$ and $w_H(\boldsymbol{e} - \boldsymbol{\epsilon}) \leq 2s$ occurs and disturbs the input codeword. We call this pair of errors $(\boldsymbol{e}, \boldsymbol{\epsilon})$ a (t, s)-**parallel error**. In this paper, we assume $t \geq s$.

Definition 1 A code $\mathcal{C} \subset \mathcal{X}^n \times \mathcal{Y}^n$ is called an $(n, t, s, |\mathcal{C}|)$ **parallel error correcting code**, in short, an $(n, t, s, |\mathcal{C}|)$ **P-code** over $GF(q)$ if there are no codewords $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v}), \boldsymbol{c}' = (\boldsymbol{u}', \boldsymbol{v}') \in \mathcal{C}$ such that $\boldsymbol{u}, \boldsymbol{u}' \in \mathcal{X}^n$ and $\boldsymbol{v}, \boldsymbol{v}' \in \mathcal{Y}^n$ satisfying

$$\boldsymbol{c} + (\boldsymbol{e}, \boldsymbol{\epsilon}) = \boldsymbol{c}' + (\boldsymbol{e}', \boldsymbol{\epsilon}') \tag{1}$$

[1]This work is supported by Waseda University Grant for Special Research Project No. 2006B-293.

where pairs of errors $(\boldsymbol{e}, \boldsymbol{\epsilon})$ and $(\boldsymbol{e}', \boldsymbol{\epsilon}')$ are (t, s)-parallel errors. □

Definition 2 An $(n, t, s, |\mathcal{C}|)$ P-code $\mathcal{C} \subset \mathcal{X}^n \times \mathcal{Y}^n$ is called **independent**, in short, an $(n, t, s, |\mathcal{C}|)$ **IP-code** if the code $\mathcal{C}$ is a Cartesian product of a subspace $\mathcal{U} \subseteq \mathcal{X}^n$ and a subspace $\mathcal{V} \subseteq \mathcal{Y}^n$. i.e., $\mathcal{C} = \mathcal{U} \times \mathcal{V}$. An $(n, t, s, |\mathcal{C}|)$ IP-code is **linear**, in short, an (n, t, s, k, l) **LIP-code** if $\mathcal{U}$ and $\mathcal{V}$ are linear subspaces with $k = \dim(\mathcal{U})$ and $l = \dim(\mathcal{V})$. □

Note that if $s = 0$, a $(t, 0)$-parallel error $(\boldsymbol{e}, \boldsymbol{\epsilon})$ satisfies $\boldsymbol{e} = \boldsymbol{\epsilon}$ and this model is reduced to that assumed in [1]. Therefore, the above model is a generalized version of that in [1] by allowing additional at most s errors in each line of the channel. The definitions of an $(n, t, s, |\mathcal{C}|)$ P-code, IP-code and an (n, t, s, k, l) LIP-code are identical to those in [1] when $s = 0$.

Throughout this paper, we denote the maximum size of t-error correcting codes of the length n by $A(n, t)$ and the maximum dimension of linear t-error correcting codes of the length n by $L(n, t)$. For any sets $\mathcal{A} \in GF^n(q)$ and $\mathcal{B} \in GF^n(q)$, we define an addition operation of sets as $\mathcal{A} + \mathcal{B} = \{\boldsymbol{a} + \boldsymbol{b} | \, \boldsymbol{a} \in \mathcal{A}, \boldsymbol{b} \in \mathcal{B}\}$.

III. Parallel Error Correcting Code

We derive necessary and sufficient conditions for parallel error correcting codes.

Let $\mathcal{U} \subseteq \mathcal{X}^n$ and $\mathcal{V} \subseteq \mathcal{Y}^n$. For $\mathcal{U}$ and $\mathcal{V}$, let $\mathcal{C}_0$ be the maximal subspace such that $\mathcal{U} = \mathcal{C}_0 + \mathcal{U}_0$ and $\mathcal{V} = \mathcal{C}_0 + \mathcal{V}_0$ for some $\mathcal{U}_0 \subseteq \mathcal{X}^n$, $\mathcal{V}_0 \subseteq \mathcal{Y}^n$. i.e., $\mathcal{U} = \{\boldsymbol{u} = \boldsymbol{x} + \boldsymbol{u}_0 | \, \boldsymbol{x} \in \mathcal{C}_0, \boldsymbol{u}_0 \in \mathcal{U}_0\}$ and $\mathcal{V} = \{\boldsymbol{v} = \boldsymbol{x} + \boldsymbol{v}_0 | \, \boldsymbol{x} \in \mathcal{C}_0, \boldsymbol{v}_0 \in \mathcal{V}_0\}$.

We show the following lemma.

Lemma 1 Define a code $\mathcal{C} \subset \mathcal{X}^n \times \mathcal{Y}^n$ to have codewords

$$\boldsymbol{c} = (\boldsymbol{x} + \boldsymbol{u}_0, \boldsymbol{x} + \boldsymbol{v}_0) \tag{2}$$

where $\boldsymbol{x} + \boldsymbol{u}_0 \in \mathcal{U}, \boldsymbol{x} + \boldsymbol{v}_0 \in \mathcal{V}$ and $\boldsymbol{x} \in \mathcal{C}_0$. The code $\mathcal{C}$ is an $(n, t, s, |\mathcal{C}|)$ P-code if and only if (iff) the following conditions hold:

(i) The subcode $\mathcal{C}_0$ is a $(t + s)$-error correcting code.

(ii) For $\mathcal{U}$, $\mathcal{V}$ given by $\mathcal{C}_0$ in the condition (i), define

$$\mathcal{Z} = \{\boldsymbol{z} = \boldsymbol{u}_0 - \boldsymbol{v}_0 | \, \boldsymbol{u}_0 \in \mathcal{U}_0, \boldsymbol{v}_0 \in \mathcal{V}_0\}. \tag{3}$$

Then $\mathcal{Z}$ is a $(2s)$-error correcting code of the size $|\mathcal{Z}| = |\mathcal{U}_0| \times |\mathcal{V}_0|$.

(**Proof**) We will prove the if part. Assume that the conditions (i) and (ii) hold.

Let the code $\mathcal{C}$ be not an $(n, t, s, |\mathcal{C}|)$ P-code. Then from eq. (1) for $\boldsymbol{c} = (\boldsymbol{x} + \boldsymbol{u}_0, \boldsymbol{x} + \boldsymbol{v}_0), \boldsymbol{c}' = (\boldsymbol{x}' + \boldsymbol{u}_0', \boldsymbol{x}' + \boldsymbol{v}_0') \in \mathcal{C}$, we have

$$\boldsymbol{x} + \boldsymbol{u}_0 + \boldsymbol{e} = \boldsymbol{x}' + \boldsymbol{u}_0' + \boldsymbol{e}', \tag{4}$$

$$\boldsymbol{x} + \boldsymbol{v}_0 + \boldsymbol{\epsilon} = \boldsymbol{x}' + \boldsymbol{v}_0' + \boldsymbol{\epsilon}' \tag{5}$$

where $(\boldsymbol{e}, \boldsymbol{\epsilon})$ and $(\boldsymbol{e}', \boldsymbol{\epsilon}')$ are (t, s)-parallel errors. Suppose that $\boldsymbol{u}_0 \neq \boldsymbol{u}_0'$ or $\boldsymbol{v}_0 \neq \boldsymbol{v}_0'$. Subtracting eq. (5) from eq. (4), we have

$$(\boldsymbol{u}_0 - \boldsymbol{v}_0) - (\boldsymbol{u}_0' - \boldsymbol{v}_0') = (\boldsymbol{e}' - \boldsymbol{\epsilon}') - (\boldsymbol{e} - \boldsymbol{\epsilon}). \tag{6}$$

Since

$$\begin{aligned} d_H(\boldsymbol{u}_0 - \boldsymbol{v}_0, \boldsymbol{u}_0' - \boldsymbol{v}_0') &= d_H(\boldsymbol{e}' - \boldsymbol{\epsilon}', \boldsymbol{e} - \boldsymbol{\epsilon}) \\ &\leq w_H(\boldsymbol{e}' - \boldsymbol{\epsilon}') + w_H(\boldsymbol{e} - \boldsymbol{\epsilon}) \leq 4s \end{aligned} \tag{7}$$

from the definition, eq. (6) implies the set $\mathcal{Z} = \{\boldsymbol{z} = \boldsymbol{u}_0 - \boldsymbol{v}_0\}$ is not a $(2s)$-error correcting code (note that the condition $|\mathcal{Z}| = |\mathcal{U}_0| \times |\mathcal{V}_0|$ implies $\boldsymbol{u}_0 - \boldsymbol{v}_0 \neq \boldsymbol{u}_0' - \boldsymbol{v}_0'$ unless $\boldsymbol{u}_0 = \boldsymbol{u}_0'$ and $\boldsymbol{v}_0 = \boldsymbol{v}_0'$). This contradicts the assumption and $\mathcal{C}$ is an $(n, t, s, |\mathcal{C}|)$ P-code if $\boldsymbol{u}_0 \neq \boldsymbol{u}_0'$ or $\boldsymbol{v}_0 \neq \boldsymbol{v}_0'$.

Next suppose that $\boldsymbol{c} \neq \boldsymbol{c}'$ but $\boldsymbol{u}_0 = \boldsymbol{u}_0'$ and $\boldsymbol{v}_0 = \boldsymbol{v}_0'$. From eqs. (4), (5), we have

$$\boldsymbol{x} - \boldsymbol{x}' = \boldsymbol{e}' - \boldsymbol{e}, \tag{8}$$

$$\boldsymbol{x} - \boldsymbol{x}' = \boldsymbol{\epsilon}' - \boldsymbol{\epsilon}, \tag{9}$$

for $\boldsymbol{x}, \boldsymbol{x}' \in \mathcal{C}_0$. These equations imply that the set $\mathcal{C}_0$ is not a $(t+s)$-error correcting code and this is contradiction to the assumption.

Next, we prove the only-if part. Assume that the code $\mathcal{C}$ is an $(n, t, s, |\mathcal{C}|)$ P-code.

Suppose that the condition (i) does not hold. Then if $\boldsymbol{u}_0 = \boldsymbol{u}_0'$ and $\boldsymbol{v}_0 = \boldsymbol{v}_0'$, there exist $\boldsymbol{x}, \boldsymbol{x}' \in \mathcal{C}_0$ satisfying eqs. (8) and (9), and hence eq. (1). This is contradiction and therefore, the condition (i) holds.

If the condition (ii) does not hold, there exist $\boldsymbol{u}, \boldsymbol{u}' \in \mathcal{U}_0$ and $\boldsymbol{v}, \boldsymbol{v}' \in \mathcal{V}_0$ satisfying eq. (6) and hence, eq. (1) if $\boldsymbol{x} = \boldsymbol{x}'$. This is contradiction to the assumption that $\mathcal{C}$ is a P-code, and therefore, the condition (ii) holds. Note that we need the constraint $|\mathcal{Z}| = |\mathcal{U}_0| \times |\mathcal{V}_0|$ for one-to-one correspondence between a pair $(\boldsymbol{u}_0, \boldsymbol{v}_0) \in \mathcal{U}_0 \times \mathcal{V}_0$ and $\boldsymbol{u}_0 - \boldsymbol{v}_0 \in \mathcal{Z}$. Consequently, the conditions (i), (ii) hold. □

We show the following theorem about the size of the P-code $\mathcal{C}$.

Theorem 1 Let $\mathcal{C}$ be an (n, t, s, M) P-code. Then we have the following statements:

(i) The size M is bounded as

$$M \leq A(n, t + s) \times A(n, 2s). \tag{10}$$

(ii) For $M = A(n, t + s) \times A(n, 2s)$, there exists an (n, t, s, M) P-code.

(**Proof**) We will briefly show the statement (i). Apparently, we have $|\mathcal{C}_0| \leq A(n, t + s)$ and $|\mathcal{Z}| = |\mathcal{U}_0| \times |\mathcal{V}_0| \leq A(n, 2s)$ from the conditions of Lemma 1. Then $|\mathcal{C}| = |\mathcal{C}_0| \times |\mathcal{U}_0| \times |\mathcal{V}_0| \leq A(n, t + s) \times A(n, 2s)$.

Next, we will show that we can construct an (n, t, s, M) P-code which satisfies (ii).

Construction I: Choose any $(t+s)$-error correcting code of the size $A(n,t+s)$ as $\mathcal{C}_0$. We also choose a $(2s)$-error correcting code of the size $A(n,2s)$ as $\mathcal{V}_0$ and let $\mathcal{U}_0 = \emptyset$. We set $\mathcal{U} = \{\boldsymbol{u} = \boldsymbol{x} | \boldsymbol{x} \in \mathcal{C}_0\}$, $\mathcal{V} = \{\boldsymbol{v} = \boldsymbol{x} + \boldsymbol{v}_0 | \boldsymbol{x} \in \mathcal{C}_0, \boldsymbol{v}_0 \in \mathcal{V}_0\}$, and $\mathcal{C} = \mathcal{U} \times \mathcal{V}$.

For $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v}), \boldsymbol{c}' = (\boldsymbol{u}', \boldsymbol{v}') \in \mathcal{C}$, equations

$$\boldsymbol{u} + \boldsymbol{e} = \boldsymbol{u}' + \boldsymbol{e}', \tag{11}$$

$$\boldsymbol{v} + \boldsymbol{\epsilon} = \boldsymbol{v}' + \boldsymbol{\epsilon}', \tag{12}$$

never hold simultaneously since eq. (11) for $\boldsymbol{u} \neq \boldsymbol{u}'$ itself implies $\mathcal{U}(= \mathcal{C}_0)$ is not a $(t+s)$-error correcting code and eq. (11) for $\boldsymbol{u} = \boldsymbol{u}'$ and eq. (12) leads to $\boldsymbol{v}_0 - \boldsymbol{v}_0' = (\boldsymbol{\epsilon}' - \boldsymbol{e}') - (\boldsymbol{\epsilon} - \boldsymbol{e})$ which implies that $\mathcal{V}_0$ is not a $(2s)$-error correcting code. Hence, the code $\mathcal{C}$ is a (t,s) P-code.

Obviously, $M = A(n,t+s) \times A(n,2s)$. Therefore, the code $\mathcal{C}$ is an (n,t,s,M) P-code. □

We here mention a decoding process of the P-code obtained by Construction I. Assume that a codeword $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v}) \in \mathcal{C}$ has been sent and a sequence $\boldsymbol{c}' = \boldsymbol{c} + (\boldsymbol{e}, \boldsymbol{\epsilon})$ is received by the decoder where errors $(\boldsymbol{e}, \boldsymbol{\epsilon})$ are a (t,s)-parallel error. We denote $\boldsymbol{u}' = \boldsymbol{u} + \boldsymbol{e}$ and $\boldsymbol{v}' = \boldsymbol{v} + \boldsymbol{\epsilon}$.

Decoding Algorithm I:

(1) Calculate $\boldsymbol{z} = \boldsymbol{v}' - \boldsymbol{u}'$.

(2) For $\boldsymbol{z}$, perform a decoding algorithm of the code $\mathcal{V}_0$ to find a codeword $\boldsymbol{v}_0$ and an error pattern $\boldsymbol{f} = \boldsymbol{\epsilon} - \boldsymbol{e}$.

(3) Perform a decoding algorithm of the code $\mathcal{U}(= \mathcal{C}_0)$ by erasing symbols of $\boldsymbol{u}'$ in the positions of $\{j | f_j \neq 0\}$ where $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$.

We will show that Decoding Algorithm I finds the transmitted codeword $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v}) \in \mathcal{C}$ if there occurs a (t,s)-parallel error.

Since $\boldsymbol{u} = \boldsymbol{x}$ and $\boldsymbol{v} = \boldsymbol{x} + \boldsymbol{v}_0$, we obtain $\boldsymbol{z} = \boldsymbol{v}' - \boldsymbol{u}' = \boldsymbol{v}_0 + \boldsymbol{\epsilon} - \boldsymbol{e} = \boldsymbol{v}_0 + \boldsymbol{f}$ in the step (1). Since $w_H(\boldsymbol{f}) \leq 2s$ and the code $\mathcal{V}_0$ is a $(2s)$-error correcting code, a conventional decoding algorithm for the code $\mathcal{V}_0$ can correctly find a codeword $\boldsymbol{v}_0$ from $\boldsymbol{z} = \boldsymbol{v}_0 + \boldsymbol{f}$. Then we can obtain the error pattern $\boldsymbol{f}$ by calculating $\boldsymbol{f} = \boldsymbol{z} - \boldsymbol{v}_0$ in the step (2). In the step (3), we regard symbols of the received sequence $\boldsymbol{u}'$ in the positions of $\{j | f_j \neq 0\}$ as erasure symbols. We denote the resultant sequence by $\tilde{\boldsymbol{u}}$. Since the code $\mathcal{U}(= \mathcal{C}_0)$ is a $(t+s)$-error correcting code, it has a minimum distance $d(\mathcal{U}) \geq 2(t+s)+1$ and corrects t errors and $2s$ erasure symbols [8]. Therefore, we can obtain the codeword $\boldsymbol{u} \in \mathcal{U}$ from $\tilde{\boldsymbol{u}}$ and subsequently, $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{v}_0$. Thus, Decoding Algorithm I surely finds $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v})$.

IV. Linear Independent Parallel Error Correcting Code

In this section, we discuss $(n,t,s,|\mathcal{C}|)$ IP-codes $\mathcal{C} = \mathcal{U} \times \mathcal{V}$. We use linear codes as $\mathcal{U} \subseteq \mathcal{X}^n$ and $\mathcal{V} \subseteq \mathcal{Y}^n$. i.e., the code $\mathcal{C}$ becomes an LIP-code.

Lemma 2 For two linear subspaces $\mathcal{U}$ and $\mathcal{V}$, a code $\mathcal{C} = \mathcal{U} \times \mathcal{V}$ is an (n,t,s,k,l) LIP-code with $k = \dim(\mathcal{U})$ and $l = \dim(\mathcal{V})$ iff the following conditions hold:

(i) Let $\mathcal{C}_0 = \mathcal{U} \cap \mathcal{V}$. Then $\mathcal{C}_0$ is a linear $(t+s)$-error correcting code.

(ii) $\mathcal{U} + \mathcal{V} = \{\boldsymbol{u} + \boldsymbol{v} | \boldsymbol{u} \in \mathcal{U}, \boldsymbol{v} \in \mathcal{V}\}$ is a $(2s)$-error correcting code.

(**Proof**) We assume that the conditions (i) and (ii) hold but the code $\mathcal{C}$ be not an LIP-code. First suppose $(\boldsymbol{u} - \boldsymbol{u}') \notin \mathcal{C}_0$ or $(\boldsymbol{v} - \boldsymbol{v}') \notin \mathcal{C}_0$, then $\boldsymbol{u} - \boldsymbol{v} \neq \boldsymbol{u}' - \boldsymbol{v}'$. There exist $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v}), \boldsymbol{c}' = (\boldsymbol{u}', \boldsymbol{v}') \in \mathcal{C}$ and (t,s)-parallel errors $(\boldsymbol{e}, \boldsymbol{\epsilon})$ and $(\boldsymbol{e}', \boldsymbol{\epsilon}')$ which satisfy eqs. (11), (12). Then $\boldsymbol{u} - \boldsymbol{v} - (\boldsymbol{u}' - \boldsymbol{v}') = \boldsymbol{f} - \boldsymbol{f}'$ where $\boldsymbol{f} = \boldsymbol{\epsilon} - \boldsymbol{e}$ and $\boldsymbol{f}' = \boldsymbol{\epsilon}' - \boldsymbol{e}'$. Since $w_H(\boldsymbol{f}) \leq 2s, w_H(\boldsymbol{f}') \leq 2s$ and $\boldsymbol{u} - \boldsymbol{v} \in \mathcal{U} \times \mathcal{V}, \boldsymbol{u}' - \boldsymbol{v}' \in \mathcal{U} \times \mathcal{V}$, this contradicts the assumption that the condition (ii) holds.

Next suppose $(\boldsymbol{u} - \boldsymbol{u}') \in \mathcal{C}_0$ and $(\boldsymbol{v} - \boldsymbol{v}') \in \mathcal{C}_0$. Then eqs. (11), (12) can be expressed as

$$(\boldsymbol{u} - \boldsymbol{u}') - \boldsymbol{0} = \boldsymbol{e}' - \boldsymbol{e}, \tag{13}$$

$$(\boldsymbol{v} - \boldsymbol{v}') - \boldsymbol{0} = \boldsymbol{\epsilon}' - \boldsymbol{\epsilon}. \tag{14}$$

Satisfying eqs. (13), (14) simultaneously implies that the code $\mathcal{C}_0$ is not a $(t+s)$-error correcting code since $\boldsymbol{0} \in \mathcal{C}_0$. This is a contradiction, which proves the if part.

Conversely, assume that the code $\mathcal{C}$ is an (n,t,s,k,l) LIP-code.

If the condition (ii) does not hold, there exist $\boldsymbol{u}, \boldsymbol{u}' \in \mathcal{U}$ and $\boldsymbol{v}, \boldsymbol{v}' \in \mathcal{V}$ satisfying $\boldsymbol{u} - \boldsymbol{v} - (\boldsymbol{u}' - \boldsymbol{v}') = \boldsymbol{f} - \boldsymbol{f}'$. If $\boldsymbol{u} = \boldsymbol{u}'$, this equation implies $\boldsymbol{v}' - \boldsymbol{v} = \boldsymbol{f} - \boldsymbol{f}' = \boldsymbol{\epsilon} - \boldsymbol{\epsilon}'$ since $\boldsymbol{e} = \boldsymbol{e}'$ from eq. (11) and hence, eq. (1) holds. This is contradiction to the assumption that $\mathcal{C}$ is a LIP-code, and therefore, the condition (ii) holds.

Let the condition (i) do not hold. Then there exist $\boldsymbol{u}, \boldsymbol{u}' \in \mathcal{U}$ and $\boldsymbol{v}, \boldsymbol{v}' \in \mathcal{V}$ satisfying $(\boldsymbol{u} - \boldsymbol{u}') \in \mathcal{C}_0$, $(\boldsymbol{u} - \boldsymbol{u}') \in \mathcal{C}_0$ and eqs. (11), (12), which implies eq. (1). This is contradiction and therefore, the condition (i) holds. Therefore, we can show the only if part. □

Although we cannot obtain the optimal IP-code with the maximum size when we consider LIP-codes, we can obtain the pair of achievable rates (pair of dimensions of all line codes [1, 5]) of LIP-codes.

Theorem 2 For given positive integers n, t, s and k_1, k_2, there exists an (n,t,s,k_1,k_2) LIP-code iff k_1, k_2 satisfy

$$k_1 + k_2 \leq L(n,t+s) + L(n,2s) \tag{15}$$

and $k_1 \leq n$, $k_2 \leq n$.

(**Proof**)

We first assume that without loss of genearity, $k_1 \leq n$, $k_2 \leq n$ and $k_1 + k_2 = L(n,t+s) + L(n,2s)$. From Lemma 2, we choose any linear $(t+s)$-error correcting code of the dimension $k = L(n,t+s)$ as the code $\mathcal{C}_0 = \mathcal{U} \cap \mathcal{V}$. Then the proof follows the following construction.

Construction II: We denote k bases of the linear subspace $\mathcal{C}_0$ by $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k$. Furthermore, we choose any linear $(2s)$-error correcting code $\mathcal{C}'$ of the dimension $k' = \dim(\mathcal{C}') = L(n, 2s)$ whose bases include $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k$. We denote other $k' - k$ bases of $\mathcal{C}'$ by $\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_{k'-k}$. Now we divide $\{1, 2, \ldots, k'-k\}$ into a set $\mathcal{I}_1$ and $\mathcal{I}_2$ (with $\mathcal{I}_1 \cap \mathcal{I}_2 = \emptyset$) such that $\{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k\} \cup \{\beta_i | \, i \in \mathcal{I}_1\}$ are bases of $\mathcal{U}$ and $\{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k\} \cup \{\beta_i | \, i \in \mathcal{I}_2\}$ are bases of $\mathcal{V}$. Let $\mathcal{C} = \mathcal{U} \times \mathcal{V}$. Then we have $(k_1 - k) + (k_2 - k) = k' - k$ where $k_1 = \dim(\mathcal{U})$ and $k_2 = \dim(\mathcal{V})$. From Lemma 2, the code $\mathcal{C}$ is an (n, t, s, k_1, k_2) LIP-code and $k_1 + k_2 = k + k' = L(n, t+s) + L(n, 2s)$.

Conversely, we assume that a code $\mathcal{C} = \mathcal{U} \times \mathcal{V}$ is an LIP-code. From Lemma 2, $\mathcal{U} + \mathcal{V}$ and $\mathcal{C}_0 = \mathcal{U} \cap \mathcal{V}$ are a linear $(2s)$-error correcting code and a linear $(t+s)$-error correcting code, respectively. We denote $k = \dim(\mathcal{C}_0)$ and $k' = \dim(\mathcal{U} \times \mathcal{V})$. Then $(k_1 - k) + (k_2 - k) = k' - k$ and we have $k_1 + k_2 = k' + k$. By $|\mathcal{U}| = q^{k_1}$, $|\mathcal{V}| = q^{k_2}$, we have

$$|\mathcal{C}| = |\mathcal{U}| \times |\mathcal{V}| = q^{k_1} \times q^{k_2} = q^{k'+k}. \tag{16}$$

Since $k' \leq L(n, 2s)$, $k \leq L(n, t+s)$, we can show

$$|\mathcal{C}| \leq q^{L(n,t+s)+L(n,2s)}. \tag{17}$$

i.e., eq. (15) holds. □

We here mention a decoding process of the LIP-code obtained by Construction II. Let $\mathcal{U}_0$ and $\mathcal{V}_0$ satisfy $\mathcal{U} = \mathcal{C}_0 + \mathcal{U}_0$ and $\mathcal{V} = \mathcal{C}_0 + \mathcal{V}_0$, respectively. As in Sect. III, we assume that a codeword $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{x} + \boldsymbol{u}_0, \boldsymbol{y} + \boldsymbol{v}_0) \in \mathcal{C}$ with $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}_0, \boldsymbol{u}_0 \in \mathcal{U}_0$ and $\boldsymbol{v}_0 \in \mathcal{V}_0$ has been transmitted and a sequence $\boldsymbol{c}' = \boldsymbol{c} + (\boldsymbol{e}, \boldsymbol{\epsilon})$ is received by the decoder where $(\boldsymbol{e}, \boldsymbol{\epsilon})$ is a (t, s)-parallel error. We denote $\boldsymbol{u}' = \boldsymbol{u} + \boldsymbol{e}$ and $\boldsymbol{v}' = \boldsymbol{v} + \boldsymbol{\epsilon}$.

For a LIP-code $\mathcal{C}$ by Construction II, we denote a generator matrix of the code $\mathcal{C}_0$ by G_0. Similarly, we denote a generator matrix of $\mathcal{U}_0$ and $\mathcal{V}_0$ by G_1 and G_2, respectively. The sizes of G_0, G_1, G_2 are $k \times n, (k_1 - k) \times n, (k_2 - k) \times n$, respectively. Let an overall generator matrix of $\mathcal{U} + \mathcal{V}$ be

$$G = \begin{pmatrix} G_0 \\ G_1 \\ G_2 \end{pmatrix}, \tag{18}$$

and then the rank of G is full.

Decoding Algorithm II:

(1) Calculate $\boldsymbol{z} = \boldsymbol{v}' - \boldsymbol{u}'$.

(2) For $\boldsymbol{z}$, perform a decoding algorithm for the code $\mathcal{U} + \mathcal{V}$ to find a codeword $\boldsymbol{v} - \boldsymbol{u}$ and an error pattern $\boldsymbol{f} = \boldsymbol{\epsilon} - \boldsymbol{e}$.

(3) Calculate

$$\boldsymbol{a} = (a_1, a_2, \ldots, a_{k_1+k_2-k}) = (\boldsymbol{v} - \boldsymbol{u}) G^{\dagger} \tag{19}$$

where $G^{\dagger} = G^T (G G^T)^{-1}$ is a generalized inverse matrix[1] (Moore-Penrose pseudo-insvese matrix [7]) of G and calculate $\boldsymbol{u}_0 = (a_{k+1}, \ldots, a_{k_1-k}) G_1 \in \mathcal{U}_0$ and $\boldsymbol{v}_0 = (a_{k_1-k+1}, \ldots, a_{k_1+k_2-k}) G_2 \in \mathcal{V}_0$.

(4) Calculate $\boldsymbol{u}' - \boldsymbol{u}_0$ and perform a decoding algorithm for the code $\mathcal{C}_0$ by erasing symbols of $\boldsymbol{u}' - \boldsymbol{u}_0$ in the positions of $\{j | f_j \neq 0\}$ where $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$.

(5) Calculate $\boldsymbol{v}' - \boldsymbol{v}_0$ and perform a decoding algorithm for the code $\mathcal{C}_0$ by erasing symbols of $\boldsymbol{v}' - \boldsymbol{v}_0$ in the positions of $\{j | f_j \neq 0\}$ where $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$.

We will show the validity of Decoding Algorithm II that it corrects a (t, s)-parallel error.

Note that $\boldsymbol{z} = \boldsymbol{v}' - \boldsymbol{u}' = \boldsymbol{v} - \boldsymbol{u} + \boldsymbol{f}$ in Step (1) and the equation

$$\boldsymbol{v} - \boldsymbol{u} = (\boldsymbol{y} - \boldsymbol{x}) + \boldsymbol{v}_0 - \boldsymbol{u}_0 = \boldsymbol{a} G \tag{20}$$

holds for some $\boldsymbol{a} \in GF^{k_1+k_2-k}(q)$. Since $w_H(\boldsymbol{f}) \leq 2s$, the decoding algorithm for the code $\mathcal{U} + \mathcal{V}$ finds $\boldsymbol{v} - \boldsymbol{u}$ and $\boldsymbol{f}$ in Step (2). If we multiply the generalized inverse matrix $G^{\dagger}$ to each term of eq. (20) by right,

$$(\boldsymbol{v} - \boldsymbol{u}) G^{\dagger} = \boldsymbol{a} G G^{\dagger} = \boldsymbol{a} \tag{21}$$

where the last equation can be obtained by the definition of $G^{\dagger}$ as $G G^{\dagger} = I$ (I denotes the identity matrix). Therefore, in Step (3), we can obtain $\boldsymbol{a}$ and re-encoding operation generates $\boldsymbol{u}_0 \in \mathcal{U}_0$ and $\boldsymbol{v}_0 \in \mathcal{V}_0$. In Step (4), we calculate $\boldsymbol{u}' - \boldsymbol{u}_0 = \boldsymbol{x} + \boldsymbol{e}$ with $\boldsymbol{x} \in \mathcal{C}_0$. Since the code $\mathcal{C}_0$ has the minimum distance $d(\mathcal{C}_0) \geq 2(t+s) + 1$, this can correct t errors and $2s$ erasure symbols [8]. Then from $\boldsymbol{u}' - \boldsymbol{u}_0$, we can obtain $\boldsymbol{x}$ correctly by regarding the symbols of $\boldsymbol{u}' - \boldsymbol{u}_0$ in $\{j | f_j \neq 0\}$ as erasure symbols. We can show similarly for Step (5) that we can obtain $\boldsymbol{y} \in \mathcal{C}_0$ correctly by regarding the symbols of $\boldsymbol{v}' - \boldsymbol{v}_0$ in $\{j | f_j \neq 0\}$ as erasure symbols. Consequently, we can correct a (t, s)-parallel error.

V. A General Model

In this section, we consider a general $m \geq 2$ senders model and generalize the results in the foregoing sections.

Assume that error sequences $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_m$ where each $\boldsymbol{e}_i$ occurs in the i-th line of the parallel channel. We define a (t, s)-parallel error $(\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_m)$ to satisfy $w_H(\boldsymbol{e}_i) \leq t + s$ and $w_H(\boldsymbol{e}_i - \boldsymbol{e}_j) \leq 2s$ for $1 \leq i \leq m, 1 \leq j \leq m$.

Definition 3 For $m \geq 2$, if the code $\mathcal{C}$ is a subspace of a Cartesian product of m $GF^n(q)$ and no codewords $\boldsymbol{c} = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m), \boldsymbol{c}' = (\boldsymbol{c}'_1, \boldsymbol{c}'_2, \ldots, \boldsymbol{c}'_m) \in \mathcal{C}$ with $\boldsymbol{c}_i, \boldsymbol{c}'_i \in GF^n(q)$ satisfy

$$\boldsymbol{c} + (\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_m) = \boldsymbol{c}' + (\boldsymbol{e}'_1, \boldsymbol{e}'_2, \ldots, \boldsymbol{e}'_m), \tag{22}$$

where $(\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_m)$ and $(\boldsymbol{e}'_1, \boldsymbol{e}'_2, \ldots, \boldsymbol{e}'_m)$ are (t, s)-parallel errors, then the code $\mathcal{C}$ is called an $(n, m, t, s, |\mathcal{C}|)$ P-code. □

[1] The symbol T denotes transposition of a matrix.

An $(n, m, t, s, |\mathcal{C}|)$ P-code is called an IP-code if $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2 \times \cdots \times \mathcal{C}_m$ where $\mathcal{C}_i$ is a subspace of $GF^n(q)$ and called an $(n, m, t, s, \{k_1, k_2, \ldots, k_m\})$ LIP-code if each line code $\mathcal{C}_i$ is a linear code of the dimension k_i.

We can generalize Theorems 1 and 2 to the general m senders case.

Lemma 3 Let $\mathcal{C}_0$ be a subspace of $GF^n(q)$. Define a code $\mathcal{C}$ to have codewords expressed as

$$\boldsymbol{c} = (\boldsymbol{x} + \boldsymbol{u}_1, \boldsymbol{x} + \boldsymbol{u}_2, \ldots, \boldsymbol{x} + \boldsymbol{u}_m) \tag{23}$$

where $\boldsymbol{x} + \boldsymbol{u}_i \in \mathcal{C}_i$ and $\boldsymbol{x} \in \mathcal{C}_0$ for some $\mathcal{C}_0 \subseteq GF^n(q)$. A code $\mathcal{C}$ is an (n, m, t, s, M) P-code iff the following conditions hold:

(i) The common subcode $\mathcal{C}_0$ is a $(t+s)$-error correcting code.

(ii) For any pair $\mathcal{C}_i$ and $\mathcal{C}_j$, define

$$\mathcal{Z}_{i,j} = \{\boldsymbol{u}_i - \boldsymbol{u}_j |\, \boldsymbol{x} + \boldsymbol{u}_i \in \mathcal{C}_i, \boldsymbol{x} + \boldsymbol{u}_j \in \mathcal{C}_j\}. \tag{24}$$

For any $\mathcal{C}_i$, there exists some $\mathcal{C}_j, i \neq j$, such that $\mathcal{Z}_{i,j}$ is a linear $(2s)$-error correcting code. □

Theorem 3 Let $\mathcal{C}$ be an (n, m, t, s, M) P-code. We have the following statements:

(i) The size of $\mathcal{C}$ is bounded by

$$M \leq A(n, t+s) \times A(n, 2s)^{(m-1)}. \tag{25}$$

(ii) For $M = A(n, t+s) \times A(n, 2s)^{(m-1)}$, there exists an (n, m, t, s, M) P-code.

(**Proof**) We will show a construction of an (n, m, t, s, M) P-code whose cardinality achieves (ii). Choose a $(t+s)$-error correcting code with the size $A(n, t+s)$ as $\mathcal{C}_1$. We also choose a $(2s)$-error correcting code $\mathcal{U}$ with the size $A(n, 2s)$. We set $\mathcal{C}_i = \{\boldsymbol{x} + \boldsymbol{u} |\, \boldsymbol{x} \in \mathcal{C}_1, \boldsymbol{u} \in \mathcal{U}\}$ for $2 \leq i \leq m$. Note that for any $\mathcal{C}_i$, $\mathcal{Z}_{i,1}$ is an $(2s)$-error correcting code and the condition (ii) of Lemma 3 holds. Then the code $\mathcal{C}$ is an (n, m, t, s, M) P-code achieving $M = |\mathcal{C}| = A(n, t+s) \times A(n, 2s)^{(m-1)}$. □

Now we consider LIP-codes. Let $\mathcal{C}_1, \ldots, \mathcal{C}_m$ be linear subspaces of $GF^n(q)$ and a code $\mathcal{C}$ be expressed as $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2 \times \cdots \times \mathcal{C}_m$. We denote $\mathcal{C}_0 = \bigcap_{i=1}^m \mathcal{C}_i$.

Lemma 4 A code $\mathcal{C}$ is an $(n, m, t, s, \{k_1, k_2, \ldots, k_m\})$ LIP-code iff the following conditions hold:

(i) The common subcode $\mathcal{C}_0$ is a linear $(t+s)$-error correcting code.

(ii) For any $\mathcal{C}_i$, there exist some $\mathcal{C}_j, i \neq j$, such that $\mathcal{C}_i + \mathcal{C}_j = \{\boldsymbol{c}_i + \boldsymbol{c}_j |\, \boldsymbol{c}_i \in \mathcal{C}_i, \boldsymbol{c}_j \in \mathcal{C}_j\}$ is a linear $(2s)$-error correcting code. □

Theorem 4 For given positive integers n, t, s and $\{k_1, k_2, \ldots, k_m\}$, there exists an LIP-code such that

$$\sum_{i=1}^{m} k_i \leq L(n, t+s) + (m-1)L(n, 2s). \tag{26}$$

(**Proof**) We will show a construction of an $(n, m, t, s, \{k_1, k_2, \ldots, k_m\})$ LIP-code which satisfies eq. (26) with equality. Choose a linear $(t+s)$-error correcting code with the dimension $L(n, t+s)$ as $\mathcal{C}_1$. Choose a linear $(2s)$-error correcting code with the dimension $L(n, 2s)$ which includes $\mathcal{C}_1$ as its subcode and set it to $\mathcal{C}_i, i \geq 2$. Then we have $\mathcal{C}_0 = \bigcap_{i=1}^m \mathcal{C}_i = \mathcal{C}_1$ which satisfies the condition (i) of Lemma 4. We can see that for any $\mathcal{C}_i, i \geq 2$, we have $\mathcal{C}_1 + \mathcal{C}_i = \mathcal{C}_i$ and the condition (ii) of Lemma 3 holds. Then the code $\mathcal{C}$ is an $(n, m, t, s, \{k_1, k_2, \ldots, k_m\})$ LIP-code of the size

$$\begin{aligned} |\mathcal{C}| &= |\mathcal{C}_1| \times |\mathcal{C}_2| \times \cdots \times |\mathcal{C}_m| \\ &= q^{L(n,t+s)+(m-1)L(n,2s)}. \end{aligned} \tag{27}$$

Hence, the code $\mathcal{C}$ has the maximum achievable rate. □

VI. Conclusion

In this paper, we generalized the notion of the parallel channel proposed by Ahlswede et al. by allowing some random errors besides a conventional parallel error. Then we derived necessary and sufficient conditions for non-independent and linear independent parallel error correcting codes. We showed some construction methods for both non-independent and linear independent codes. Decoding algorithms for these codes are based on those of ordinary error correcting codes. Therefore, we can find an efficient algorithm for linear parallel error correcting codes.

As for future works, the probabilistic models of parallel error should be discussed. Conditions of the optimal independent parallel error correcting code for given n, t and s is also to be derived.

References

[1] R. Ahlswede, B. Balkenhol, and N. Cai, "Parallel Error Correcting Codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 4, pp. 959–962, Apr. 2002.

[2] L. Gyorfi, and B. Lacmy, "Signature coding and information transfer for the multiple access adder channel," *Proc. Information Theory Workshop 2004*, pp. 242–246, San Antonio, Texas, Oct. 2004.

[3] J. Cheng, and Y. Watanabe, "A multiuser k-ary code for the noisy multiple-access adder channel," *IEEE Trans. Inf. Theory*, vol. 47, no. 6, pp. 2603–2607, Sept. 2001.

[4] S. Chang and E. J. Weldon, Jr., "Coding for T-User multiple-access channels," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 6, pp. 684–691, Nov. 1979.

[5] T. Kasami and S. Lin, " Bounds on the achievable rates of block coding for a memoryless multiple-access Channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 2, pp. 187–197, Mar. 1978.

[6] K. Tokiwa, H. Matsuda, and H. Tanaka, "A code construction for M-Choose-T communication over the multiple-access adder channel," *IEICE Trans. Fundamentals*, vol.E78-A, no.1, pp. 94–99, Jan. 1995.

[7] G. Strang, *Linear Algebra and Its Applications*, San Diego: Harcourt, Brace, Jovanovich, 1988.

[8] F. J. McWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, Amsterdam, The Netherlands: North-Holland, 1986.