The 29th Symposium on Information Theory
and its Applications (SITA2006)
Hakodate, Hokkaido, Japan, Nov. 28 - Dec. 1, 2006

Decoding Performance of Linear Parallel Error Correcting Codes

Hideki Yagi* Toshiyasu Matsushima† Shigeichi Hirasawa†

Abstract— Parallel error correcting codes have been devised for a new type of multiple access communication where noises of each channel line are correlated each other. This paper analyzes decoding performance of the parallel error correcting codes. We first introduce a simple probabilistic model of the channels. Then we define a notion of bounded distance decoding over a parallel error channel and analyze its performance.

Keywords— parallel error correcting code, parallel channel, linear codes, bounded distance decoding, decoding performance

1 Introduction

Coding schemes for multiple access channels have been well-studied [2, 3, 4, 5, 7]. Recently, R. Ahlswede et al. have proposed a new class of multiple access channels [1]. This channel is called the **parallel channel** and the codes for this channel is refereed to as **parallel error correcting codes**.

The parallel channel is a bundle of m lines through which m 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 correlated magnetic noise, etc. 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 defined 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 [1]. 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.

Subsequently, Yagi et al. [10] have generalized parallel channels by allowing at most s random errors besides the same errors in all lines. They have derived necessary and sufficient conditions of parallel error correcting codes for these channels. They have showed a code construction that achieves the **maximal achievable rate** [1, 5] of linear parallel error correcting codes for a given code length, t and s. Their results simply include those of Ahlswede et al. Although the codes can correct any t-parallel error with s random errors, there has been no performance analysis when more errors occur.

In this paper, we analyze decoding performance of linear parallel error correcting codes. We first define a notion of **bounded distance decoding** of parallel channel. We then derive the probability of decoding error and error detection of the bounded distance decoding, by assuming the number of lines is two. The extension of general m $(m \geq 3)$ is not so difficult.

This paper is organized as follows: in Sect. 2, we briefly review channel model and parallel error correcting codes. Next in Sect. 3, we define bounded distance decoding for a parallel channel and derive the probabilities of correction, decoding error and error detection. Finally in Sect. 4, we give the concluding remarks.

2 Preliminary

In this section, we describe the channel model of this paper and then briefly review the code construction of the parallel error correcting codes in [10].

2.1 Model and Definitions

We denote input alphabets from two lines by $\mathcal{X}$ and $\mathcal{Y}$. In this paper, we assume that $\mathcal{X}$ and $\mathcal{Y}$ 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 line's message and the last n symbols of it are another line's message. In the channel, an error vector $(e, \epsilon) \in GF^{2n}(q)$ occurs and disturbs the input codeword. This pair of errors (e, ϵ) is refereed to as a (t, s)-**parallel error** if it satisfies $w_H(e) \leq t+s$, $w_H(\epsilon) \leq t+s$ and $w_H(e-\epsilon) \leq 2s$. In this paper, we assume $t \geq s$.

Definition 1 For linear subspaces $\mathcal{U} \subseteq \mathcal{X}^n$ and $\mathcal{V} \subseteq \mathcal{Y}^n$ with $k = \dim(\mathcal{U})$ and $l = \dim(\mathcal{V})$, a code $\mathcal{C} = \mathcal{U} \times \mathcal{V}$ is a collection of codewords $c = (u, v)$ such that $u \in \mathcal{U}, v \in \mathcal{V}$. The code $\mathcal{C}$ is called a linear independent (n, t, s, k, l) **parallel error correcting code (LIP-code)** over $GF(q)$ if there are no codewords $c, c' \in \mathcal{C}$ satisfying

$$c + (e, \epsilon) = c' + (e', \epsilon') \qquad (1)$$

where (e, ϵ) and (e', ϵ') are (t, s)-parallel errors. To simplify notation, we sometimes denote just (n, s, t) LIP-codes if the sizes k and l are not necessary. □

The case of $s = 0$ is a channel model assumed in [1], where a parallel error (e, ϵ) satisfies $e = \epsilon$. Thus the above model is a generalized version of that in [1] by allowing s random errors in each line of the channel.

Throughout this paper, for any sets $\mathcal{A} \in GF^n(q)$ and $\mathcal{B} \in GF^n(q)$, we define an addition operation of sets as $\mathcal{A} + \mathcal{B} = \{a + b | \, a \in \mathcal{A}, b \in \mathcal{B}\}$.

* Media Network Center, Waseda University 1-6-1, Nishi Waseda, Shinjuku-ku Tokyo 169-8050 Japan. E-mail: yagi@hirasa.mgmt.waseda.ac.jp

† Department of Management and Systems Eng., School of Science and Engineering, Waseda University 3-4-1, Ohkubo, Shinjuku-ku Tokyo 169-8555 Japan.

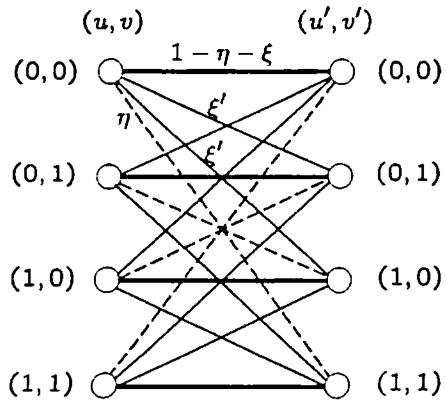

Figure 1: An example of the transition of a binary parallel channel with parameters η and ξ ($\xi' = \xi/2$). The bold line, the solid line, and the dashed line express the error free, the random error, and the parallel error.

2.2 Probabilistic Description of Channel

In this paper, we analyze the decoding performance of the parallel error correcting codes. For this purpose, we introduce the probabilistic model of the parallel channels.

Assume that a codeword $c = (u, v) \in \mathcal{C}$ is transmitted through the parallel channel and the received sequence is denoted by $c' = (u, v) + (e, \epsilon)$. Let $\eta, 0 \leq \eta \leq 1/2$, be a probability of a channel error which occurs both for $u \in \mathcal{U}, v \in \mathcal{V}$, i.e., $e_i = \epsilon_i \neq 0$. Let $\xi, 0 \leq \xi \leq 1/2$, express a probability of a channel error which occurs for either $u \in \mathcal{U}$ or $v \in \mathcal{V}$, i.e., $e_i \neq 0$ or $\epsilon_i \neq 0$. The probability of the error free for both $u \in \mathcal{U}$ and $v \in \mathcal{V}$ is $1 - \eta - \xi$. Fig. 1 expresses an example of the input-output transition of a binary (i.e., $q = 2$) parallel channel with parameters η and ξ ($\xi' = \xi/2$), where (u, v) and (u', v') express the input symbols and the output symbols of the channel, respectively.

2.3 Parallel Error Correcting Code

We review code construction of LIP codes in [10].

Lemma 1 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) $\mathcal{U} + \mathcal{V} = \{u + v \mid u \in \mathcal{U}, v \in \mathcal{V}\}$ is a $(2s)$-error correcting code.

[Construction of LIP-Codes:]

We denote a set of k bases of the linear subspace $\mathcal{C}_0$ by $\mathcal{A} = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$. Furthermore, we choose any linear $(2s)$-error correcting code $\mathcal{C}'$ of the dimension $k' = \dim(\mathcal{C}')$ whose bases include $\mathcal{A}$. We denote other $k' - k$ bases of $\mathcal{C}'$ by $\beta_1, \beta_2, \ldots, \beta_{k'-k}$. 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 $\mathcal{A} \cup \{\beta_i \mid i \in \mathcal{I}_1\}$ are bases of $\mathcal{U}$ and $\mathcal{A} \cup \{\beta_i \mid i \in \mathcal{I}_2\}$ are bases of $\mathcal{V}$. Setting $\mathcal{C} = \mathcal{U} \times \mathcal{V}$, the code $\mathcal{C}$ is an (n, t, s, k_1, k_2) LIP-code from Lemma 1.

For a LIP-code $\mathcal{C}$ by the above construction, 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 $(k + k') \times n$ generator matrix G of $\mathcal{U} + \mathcal{V}$ be arranged so that the first k rows form G_0, and the subsequent $k_1 - k$ rows form G_1.

We here mention a decoding process of the LIP-codes. 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. We here assume that a codeword $c = (u, v) = (x + u_0, y + v_0) \in \mathcal{C}$ with $x, y \in \mathcal{C}_0, u_0 \in \mathcal{U}_0$ and $v_0 \in \mathcal{V}_0$ has been transmitted and a sequence $c' = (u', v') = c + (e, \epsilon)$ is received by the decoder where (e, ϵ) is a (t, s)-parallel error.

[The Two-Stages Decoding Algorithm:]

(1-1) Calculate $z = v' - u'$.

(1-2) For z, perform a decoding algorithm for the code $\mathcal{U} + \mathcal{V}$ to find a codeword $v - u$ and an error pattern $f = \epsilon - e$.

(2-1) Calculate

$$a = (a_1, a_2, \ldots, a_{k_1+k_2-k}) = (v - u)G^\dagger \quad (2)$$

where $G^\dagger = G^T(GG^T)^{-1}$ is a generalized inverse matrix[1] (Moore-Penrose pseudo-inverse matrix [8]) of G and calculate $u_0 = (a_{k+1}, \ldots, a_{k_1-k})G_1 \in \mathcal{U}_0$ and $v_0 = (a_{k_1-k+1}, \ldots, a_{k_1+k_2-k})G_2 \in \mathcal{V}_0$.

(2-1) Calculate $u' - u_0$ and perform a decoding algorithm for the code $\mathcal{C}_0$ by erasing symbols of $u' - u_0$ in the positions of $\{j \mid f_j \neq 0\}$ where $f = (f_1, f_2, \ldots, f_n)$.

(2-3) Calculate $v' - v_0$ and perform a decoding algorithm for the code $\mathcal{C}_0$ by erasing symbols of $v' - v_0$ in the positions of $\{j \mid f_j \neq 0\}$ where $f = (f_1, f_2, \ldots, f_n)$.

The decoding algorithm consists of two-stages. The steps of the first stage correspond to (1-1) and (1-2) and the steps of the second stage are (2-1)–(2-3).

3 Performance of Bounded-Distance Decoding

In this section, we analyze the performance of (n, t, s) LIP-codes.

3.1 Bounded-Distance Decoding

We define bounded-distance decoding of (n, t, s) LIP-codes.

Let $\tau = |\mathcal{S}(e) \cap \mathcal{S}(\epsilon)|$, $\sigma_u = |\mathcal{S}(e) \setminus (\mathcal{S}(e) \cap \mathcal{S}(\epsilon))|$ and $\sigma_v = |\mathcal{S}(\epsilon) \setminus (\mathcal{S}(e) \cap \mathcal{S}(\epsilon))|$ where $\mathcal{S}(\cdot)$ denotes the support of a sequence. If a received sequence c' is decoded by the two-stages decoding algorithm, we can estimate not only (t, s)-parallel errors but any pair (e, ϵ) which satisfies

$$\tau + \lceil (\sigma_u + \sigma_v)/2 \rceil \leq t + s, \quad (3)$$

$$\sigma_u + \sigma_v \leq 2s. \quad (4)$$

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

It can be easily seen that any (t, s)-parallel errors satisfy both eqs. (3) and (4).

Definition 2 Consider a decoding algorithm satisfying the following conditions:

(i) it can correctly estimate the parallel errors satisfying both eqs. (3) and (4).

(ii) it miscorrects the parallel errors not satisfying eqs. (3) nor (4).

We call this decoding algorithm (t, s)-**bounded distance decoding** (BDD) over parallel channels. □

When a received sequence c' is decoded by an algorithm of the BDD, the results are (1) we can correctly decode the error (**correction**), (2) we cannot decode the error but can detect it (**error detection**), and (3) we misccrect the error (**decoding error**). In order to analyze the performance of the (t, s)-BDD, we have to calculate probabilities of the above three cases.

It is apparent the decoding region of this algorithm includes that of a (t, s)-BDD algorithm since it satisfies the condition (i). Then the question is if it performs better than the (t, s)-BDD. The following lemma and proposition answer this question.

Lemma 2 If the first stage of the two-stages decoding algorithm miscorrects the error, the two-stages decoding cannot succeed.

Proposition 1 The two-stages decoding algorithm performs as (t, s)-BDD.

(Proof) We will show the condition (ii) holds. If the two-stages decoding miscorrects the error, either of the following two cases holds: (a) the first stage miscorrects it, or (b) the first stage succeeds, but the second stage miscorrects it. From Lemma 2, if eq. (4) does not hold and the first stage miscorrects the error, the total decoding miscorrects it. If eq. (4) holds but eq. (3) does not hold, the second stage miscorrects it. Therefore the two-stages decoding algorithm satisfies the condition (ii). □

3.2 Probability of Correction

If we want to calculate the probability of correction, it suffice to simply calculate the probability of the events of eqs. (3) and (4). It is apparent that the probability of correction of the (t, s)-BDD is given by

$$P_C = \sum_{j=0}^{2s} \Pr(\mathcal{F}_{C,j}) \Pr(\mathcal{E}_C | \mathcal{F}_{C,j}) \tag{5}$$

where $\mathcal{F}_{C,j}$ denotes a set of error patterns $f = e - \epsilon$ ($e \in \mathcal{X}, \epsilon \in \mathcal{Y}$) satisfying eq. (4) and $\sigma_u + \sigma_v = j$, and $\mathcal{E}_C$ denotes a set of error patterns $e \in \mathcal{X}$ satisfying eq. (3).

We can obtain the probability $\Pr(\mathcal{F}_{C,j})$ by

$$\Pr(\mathcal{F}_{C,j}) = \binom{n}{j} \xi^j (1-\xi)^{n-j} \tag{6}$$

for $0 \le j \le 2s$.

We show the following proposition about the the conditional probability $\Pr(\mathcal{E}_C | \mathcal{F}_{C,j})$.

Proposition 2 Let $\psi(t, s, j) = (t+s) - \lceil j/2 \rceil$. Then the conditional probability $\Pr(\mathcal{E}_C | \mathcal{F}_{C,j})$ is given by

$$\Pr(\mathcal{E}_C | \mathcal{F}_{C,j}) = \sum_{i=0}^{\psi(t,s,j)} \binom{n-j}{i} \tilde{\eta}^i (1-\tilde{\eta})^{n-i-j} \tag{7}$$

where $\tilde{\eta} = \eta/(1-\xi)$.

From eq. (5), we can calculate the probability P_C by eqs. (6) and (7). Lemma 1 and eq. (5), (6) and (7) show that the BDD over a parallel channel is regarded as a combination of the two kinds of BDD over random error channels. Namely, the first stage is BDD over a random error channel with the crossover probability ξ and the second stage is one with the crossover probability $\tilde{\eta}$.

3.3 Probability of Decoding Error

We here derive the probability of decoding error of the two-stages decoding algorithm (BDD). The the overall probability of decoding error of the two-stages decoding algorithm is $P_E = P_E^{(1)} + P_E^{(2)}$ where $P_E^{(1)}$ denotes the probability of the first stage decoding error and $P_E^{(2)}$ denotes the probability that the first stage succeeds but the second stage miscorrects the error.

[Probability of the First Stage Error]

The derivation of the probability $P_E^{(1)}$ is the same as that in a q-ary random error channel with the crossover probability ξ. For binary case, see [6], etc. We denote the weight profile of the $(2s)$-error correcting code $\mathcal{U}+\mathcal{V}$ by $\{A_j\}$, where A_j expresses the number of codewords of the Hamming weight j.

For non-negative integers i, j, δ, let $\mathcal{F}(i, j, \delta)$ be a set of two integers (μ, γ) such that $\gamma \le \mu$, $2\mu - \gamma = j - i + \delta$ and $\min\{2n - i - j + \gamma, i + j\} \ge \delta \ge |i - j|$. The probability of the first stage decoding error is given by

$$P_E^{(1)} = \sum_{i=2s+1}^{n} \sum_{j=1}^{n} \sum_{\delta=0}^{2s} \bar{\xi}^i (1-\xi)^{n-i} \phi(i, j, \delta) A_j \tag{8}$$

where $\bar{\xi} = \xi/(q-1)$ and

$$\phi(i, j, \delta) = \sum_{(\mu,\gamma) \in \mathcal{F}(i,j,\delta)} (q-2)^\gamma (q-1)^{\delta-\mu} \times \binom{j}{\mu} \binom{\mu}{\gamma} \binom{n-j}{\delta-\mu}. \tag{9}$$

[Probability of the Second Stage Error]

We use the fact that if the first stage decoding succeeds and the decoding in the step (2-2) succeeds, then the decoding in the step (2-3) also succeeds. The probability of the second stage decoding error can be obtained by deriving the probability of the decoding error in the step (2-2).

Assume that the first stage decoding succeeds and we correctly obtain $f = e - \epsilon$. Define $\sigma = w_H(f)$. Let $B_{i,\lambda}$ denote a set of error patterns $e \in \mathcal{X}$ with the Hamming weight $w_H(e) = i$ and $|\mathcal{S}(e) \cap \mathcal{S}(f)| = \lambda$ in a decoding region of other codewords $x \in \mathcal{C}_0$ than the

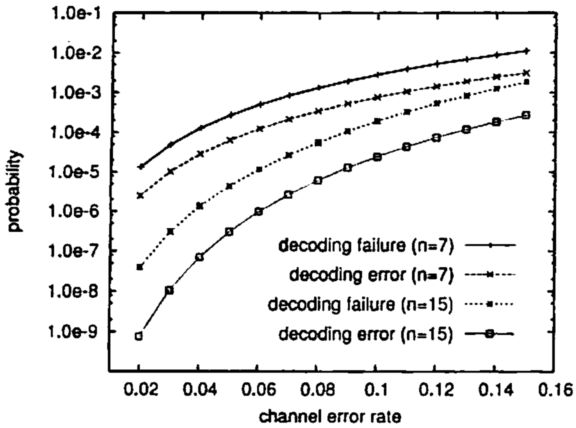

Figure 2: Probabilities of decoding error and decoding failure with for (7, 2, 1) and (15, 4, 2) LIP codes.

transmitted codeword. We denote the weight profile of the $(t+s)$-error correcting code C_0 by $\{\tilde{A}_j\}$, where $\tilde{A}_j$ expresses the number of codewords of the Hamming weight j. For non-negative integers i_x, j_x, δ_x and i_w, j_w, δ_w, let $\mathcal{F}_\nu(i_\nu, j_\nu, \delta_\nu)$ for $\nu \in \{x, w\}$ be a set of two integers (μ_ν, γ_ν) such that $\mu_\nu \geq \gamma_\nu$, $2\mu_\nu - \gamma_\nu = j_\nu - i_\nu + \delta_\nu$ and $\min\{2n_\nu - i_\nu - j_\nu + \gamma_\nu, i_\nu + j_\nu\} \geq \delta_\nu \geq |i_\nu - j_\nu|$. Define $n_x = n - \sigma$, $n_w = \sigma$, and

$$\psi_\nu(i_\nu, j_\nu, \delta_\nu) = \sum_{(\mu_\nu, \gamma_\nu) \in \mathcal{F}_\nu(i_\nu, j_\nu, \delta_\nu)} (q-2)^{\gamma_\nu}(q-1)^{\delta_\nu - \mu_\nu} \times \binom{j_\nu}{\mu_\nu}\binom{\mu_\nu}{\gamma_\nu}\binom{n_\nu - j_\nu}{\delta_\nu - \mu_\nu} \quad (10)$$

for $\nu \in \{x, w\}$.

Then the probability of the second-stage error is given by

$$P_E^{(2)} = \sum_{\sigma=0}^{2s} \sum_{i=t+s+1}^{n} \sum_{\lambda=0}^{\sigma} B_{i,\lambda} \bar{\eta}^{i-\lambda} \bar{\xi}^{\sigma} (1-\eta-\xi)^{n-\sigma-i+\lambda} \quad (11)$$

where $\bar{\eta} = \eta/(q-1)$ and

$$B_{i,\lambda} = \sum_{j=1}^{n} \sum_{j_w=0}^{\sigma} \sum_{\delta=0}^{t+s} \sum_{\delta_w=0}^{\sigma} \binom{j}{j_w}\binom{n-j}{\sigma-j_w} \times \psi_x(i-\lambda, j-j_w, \delta-\delta_w)\psi_w(\lambda, j_w, \delta_w)\tilde{A}_j. \quad (12)$$

3.4 Numerical Examples

We illustrate the probabilities of BDD over a parallel channel, using (7, 2, 1, 1, 3) and (15, 4, 2, 3, 7) LIP codes whose constituent codes are maximum-distance separable (MDS) codes [6, 9]. We show the decoding error probability and the decoding failure probability (i.e., the sum of probabilities of decoding error and error detection) for the both codes in Fig. 2. We set $\xi/\eta = 1/2$ and the horizontal axis indicates the sum of the channel error rates $(\eta + \xi)$.

4 Conclusion

In this paper, we analyzed the decoding performance of the generalized parallel error correcting codes devised by Ahlswede et al. and Yagi et al. We first introduced a probabilistic model of parallel channels. We showed that the two-stages decoding algorithm for the parallel error correcting codes is a combination of BDD over random error channels. Then we can use conventional analytical techniques for a random error channel to analyze the decoding performance. We derived the probabilities of correction and decoding error (and hence, error detection).

As for future works, the maximum likelihood decoding performance of the parallel error correcting codes should be derived.

Acknowledgement

H. Yagi wishes to thank Dr. M. Kobayashi at Shonan Institute of Technology for his valuable comments. This work is partly supported by Waseda University Grant for Special Research Project No. 2006B-293.

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] H. Imai, *Coding Theory* (in Japanese), Tokyo, Japan, IEICE, Mar. 1990.

[7] 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.

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

[9] F. J. McWilliams and N. J. A. Sloane, *The theory of error correcting codes*. Amsterdam, The Netherlands: North-Holland, 1986.

[10] Y. Yagi, T. Matsushima, and S. Hirasawa, "A generalization of the parallel error correcting codes," to be presented in *Proc. IEEE Inf. Theory Workshop*, Chengdu, China, Oct. 2006.