Size of 1-Error-Detecting Codes in Three Interactive Transmissions

Zhiqing Xiao, Yunzhou Li, Limin Xiao, and Jing Wang
Tsinghua University, Beijing, 100084, P. R. China
Email: xzq.xiaozhiqing@gmail.com

***Abstract*—This paper considers the error-detecting codes between two nodes. There are three transmissions between these two nodes: node A and node B. The first transmission can transmit one symbol within the alphabet $\{0, 1, \ldots, q_1 - 1\}$ from node A to node B; the second transmission can transmit one symbol within the alphabet $\{0, 1, \ldots, q_2 - 1\}$ from node B to node A; and the third transmission can transmit one symbol within the alphabet $\{0, 1, \ldots, q_3 - 1\}$ from node A to node B. One of the three transmissions may be erroneous. We prove that the maximum size of all 1-error-detecting codes over these three transmissions is $\min\{q_1, q_2 (q_3 - 1)\}$.**

I. Introduction

Interaction and feedback can enhance the robustness of communication systems. When some transmissions are erroneous, interactive codes can help resist the errors.

One of the most conspicuous problems to consider the error-resilient capability of interactive codes is finding the maximum size of z-error-detecting/correcting codes in given transmissions.

Schulman first considered error-resilient interactive codes in [1], [2]. In these models, a constant proportion of identical bi-direction transmissions are erroneous, and they tried to design the direction of each transmission and the behaviors of both nodes to carry on a task. They finally designed simulators to convert any non-error-resilient interactive codes to error-resilient ones. Follow-up works include improving the tolerable error rate [3] and constructing/decoding tree codes efficiently [4], [5]. All of them discussed the number of transmissions asymptotically.

In our previous paper [6], we mathematically reintroduced the concepts of z-error-detecting/correcting codes, and derived some upper bounds and lower bounds on the maximum size of z-error-detecting/correcting codes through given transmissions. Not asymptotically, our discussion focused on the exact value of the size. Additionally, we also provided an 1-error-correcting instance where the upper bound and lower bound match.

Remarkably, paper [6] predetermined the number of transmissions, the direction and the alphabet of each transmission, and the maximum number of erroneous transmissions. That is, all resources are allocated *a prior*. Such assumption is meaningful since the thorough discussion upon fixed resources is a preliminary for resource allocation.

Unfortunately, no general expressions of the maximum size have been derived so far, so finding the maximum size is still an open problem.

This paper will focus on the simplest case: *three interactive transmissions*. In the three interactive transmissions, both the first transmission and the third transmission are from node A to node B, while the second transmission is from node B to node A. We hope that we can obtain some intuitions from this simplest case.

In fact, the only nontrivial result on the error-detecting/correcting capability of three interactive transmissions model is the maximum size of 1-error-detecting codes. The reason why others are trival is twofold: (i) If there are no errors in these transmissions, the transmission capability equals the summation of the capabilities of the two feedforward transmissions. (ii) Since there are only two feedforward transmissions, there are no ways to correct arbitrary ≥ 1 transmission errors or detect arbitrary ≥ 2 transmission errors. Due to these two reasons, finding the 1-error-detecting capability of three interactive transmissions suffices to fully characterize the error-detecting/correcting capability of three interactive transmissions.

Paper Overview: This paper fully characterizes the error-detecting/correcting capability of three interactive transmissions by deriving the exact expression of the maximum size of 1-error-detecting codes over arbitrary three interactive transmissions. Section II formulates the problem. Section III presents the main result. Section IV proves the main result. Section V draws the conclusion.

II. System Model

A. Three Interactive Transmissions

There are three transmissions between node A and node B (see Fig. 1). The direction of the first transmission and the third transmission is from A to B, while the second transmission is from B to A. Each transmission is associated with an alphabet, one symbol of which can be transmitted in that transmission. Without loss of generality, we assume that the alphabets of the three transmissions are $\mathcal{Q}_1 = \{0, 1, \ldots, q_1 - 1\}$ ($q_1 \geq 2$), $\mathcal{Q}_2 = \{0, 1, \ldots, q_2 - 1\}$ ($q_2 \geq 2$), and $\mathcal{Q}_3 = \{0, 1, \ldots, q_3 - 1\}$ ($q_3 \geq 2$), respectively.

B. Interactive Code

An *interactive code* in three interactive transmissions is defined by

- a finite message set $\mathcal{M}$,
- 3 encoders:

$$\mathsf{Enc}_1 \colon \mathcal{M} \to \mathcal{Q}_1$$

978-1-4799-8088-8/15/$31.00 ©2015 IEEE

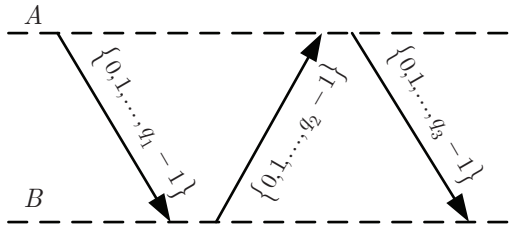

Fig. 1. Diagram of three interactive transmissions.

$$\mathsf{Enc}_2 \colon \mathcal{Q}_1 \to \mathcal{Q}_2$$

$$\mathsf{Enc}_3 \colon \mathcal{Q}_2 \times \mathcal{M} \to \mathcal{Q}_3,$$

and

- a decoder:

$$\mathsf{Dec} \colon \mathcal{Q}_1 \times \mathcal{Q}_3 \to \mathcal{M} \bigcup \{\varepsilon\},$$

where $\varepsilon \notin \mathcal{M}$ a symbol that indicates the existence of errors.

Node A wants to send a message $M \in \mathcal{M}$ to node B by the three transmissions. The cardinality of the message set is called the *size* of the code. In the total transmission procedure, the three transmissions are used in sequence.

Three encoders are:

- *Encoder 1 (at node A):* Determine the transmitted symbol in the first transmission according to the message M, i.e.,

$$X_1 = \mathsf{Enc}_1(M),$$

where $X_1 \in \mathcal{Q}_1$.

- *Encoder 2 (at node B):* Determine the transmitted symbol in the second transmission according to the symbol Y_1 that B just received, i.e.,

$$X_2 = \mathsf{Enc}_2(Y_1),$$

where $X_2 \in \mathcal{Q}_2$.

- *Encoder 3 (at node A):* Determine the transmitted symbol in the third transmission according to the message M and the symbol Y_2 that A just received, i.e.,

$$X_3 = \mathsf{Enc}_3(Y_2, M),$$

where $X_3 \in \mathcal{Q}_3$.

The decoder is:

- *Decoder (at node B):* Either recover a message or report errors according to the symbols that B has received: i.e.,

$$\hat{M} = \mathsf{Dec}(Y_1, Y_3),$$

where $\hat{M} \in \mathcal{M} \bigcup \{\varepsilon\}$.

All encoders and the decoder are deterministic.

C. Error Detecting and Error Correcting

If a transmission is erroneous, its output $Y_i \in \mathcal{Q}_i$ does not equal its input $X_i \in \mathcal{Q}_i$, that is,

$$Y_i \neq X_i;$$

otherwise, $Y_i = X_i$.

Definition 1 (z-Error-Detecting): A code in three interactive transmissions is *z-error-detecting* iff the following two properties are met:

(I) $\hat{M} = M$ when $X_1X_2X_3 = Y_1Y_2Y_3$;

(II) $\hat{M} = M$ or $\hat{M} = \varepsilon$ when $d_H(X_1X_2X_3, Y_1Y_2Y_3) \leq z$, where

$$d_H(X_1X_2X_3, Y_1Y_2Y_3) = |\{i \in \{1,2,3\} : X_i \neq Y_i\}|$$

is the Hamming distance between $X_1X_2X_3$ and $Y_1Y_2Y_3$.

The definition of z-error-detecting is provided in the sequel by the way:

Definition 2 (z-Error-Correcting): A code in three interactive transmissions is *z-error-correcting* iff $\hat{M} = M$ when $d_H(X_1X_2X_3, Y_1Y_2Y_3) \leq z$.

III. Main Result

As mentioned, we want to find the maximum size of 1-error-correcting codes through the three interactive transmissions in general. That is, given the three transmission alphabets, we want to find the largest message set over all 1-error-correcting codes through these three interactive transmissions.

Theorem 1: The maximum size of 1-error-detecting codes through three interactive transmissions is

$$\min\{q_1, q_2(q_3-1)\},$$

where $q_1, q_2, q_3 \geq 2$ is the cardinality of the three transmission alphabets.

The maximum size of z-error-detecting/correcting codes through three interactive transmissions are summarized in Table I.

TABLE I. Summary of maximum sizes of z-error-detecting/correcting codes through three interactive transmissions

Error Number z	Size of Error-Detecting Codes	Size of Error-Correcting Codes
0	q_1q_3	q_1q_3
1	$\min\{q_1, q_2(q_3-1)\}$	1
≥ 2	1	1

IV. Proof of the Main Result

A. Outline of the Proof

The outline to prove Theorem 1 is twofold: On the one hand, we need to prove that the maximum size of 1-error-detecting codes is $\leq \min\{q_1, q_2(q_3-1)\}$; on the other hand, we need to prove that the maximum size of 1-error-detecting codes is $\geq \min\{q_1, q_2(q_3-1)\}$. The specific way to prove the maximum size $\leq \min\{q_1, q_2(q_3-1)\}$ is: We first prove that for any code whose size is $> q_1$ or $> q_2(q_3-1)$ is not 1-error-detecting, then assert that the size of any

1-error-detecting code is both $\leq q_1$ and $\leq q_2(q_3-1)$. Therefore, the maximum size of 1-error-detecting codes is $\leq \min\{q_1, q_2(q_3-1)\}$. The specific way to prove the maximum size $\geq \min\{q_1, q_2(q_3-1)\}$ is: we first construct a code whose size is $\min\{q_1, q_2(q_3-1)\}$, then prove that the code is 1-error-detecting. Therefore, there exists an 1-error-detecting code whose size is $\min\{q_1, q_2(q_3-1)\}$, which leads to the maximum size $\geq \min\{q_1, q_2(q_3-1)\}$.

B. Not 1-Error-Detecting

Definition 3 (Codeword): For a message $m \in \mathcal{M}$, let a *codeword* of m be the symbol sequence in all transmissions when the original message is m and there are no errors. Let $\mathsf{c}_i(m)$ denote the entry of the codeword in the i-th transmission.

Lemma 1: For any code whose size $> q_1$, it is not 1-error-detecting.

Proof: Suppose there exists a code whose size $> q_1$. Fix the code. Due to the Pigeonhole Principle, there exist two distinct messages $\bar{m}, \tilde{m} \in \mathcal{M}$ such that $\mathsf{c}_1(\bar{m}) = \mathsf{c}_1(\tilde{m})$. Consider the two cases:

(Case I) The decoder satisfies $\bar{m} \neq \mathsf{Dec}(\mathsf{c}_1(\bar{m}), \mathsf{c}_3(\bar{m}))$. That is, when the inputs of the decoder are $\mathsf{c}_1(\bar{m})$ and $\mathsf{c}_3(\bar{m})$, the output of the decoder is either a message other than $\bar{m}$ or the error-indicating symbol ε. In this case, when A is to send message $\bar{m}$, the adversary does nothing. According to the definition of the codeword, the decoder receives $\mathsf{c}_1(\bar{m})$ and $\mathsf{c}_3(\bar{m})$. Since $\bar{m} \neq \mathsf{Dec}(\mathsf{c}_1(\bar{m}), \mathsf{c}_3(\bar{m}))$, the output of the decoder is not $\bar{m}$. According to the first part of Definition 1, the code is not 1-error-detecting.

(Case II) The decoder satisfies $\bar{m} = \mathsf{Dec}(\mathsf{c}_1(\bar{m}), \mathsf{c}_3(\bar{m}))$. That is, when the inputs of the decoder are $\mathsf{c}_1(\bar{m})$ and $\mathsf{c}_3(\bar{m})$, the output of the decoder is exactly $\bar{m}$. In this case, when A is to send message $\tilde{m}$, the adversary maliciously changes the third transmission from $\mathsf{c}_3(\tilde{m})$ to $\mathsf{c}_3(\bar{m})$. Consequently, the inputs of the decoder become $\mathsf{c}_1(\bar{m})$ and $\mathsf{c}_3(\bar{m})$ (note that we have $\mathsf{c}_1(\bar{m}) = \mathsf{c}_1(\tilde{m})$), and the output of the decoder becomes $\bar{m}$. That is, the output of the decoder is an erroneous message. According to the second part of Definition 1, the code is not 1-error-detecting.

Therefore, any code whose size $> q_1$ is not 1-error-detecting. ∎

Lemma 2: For any code whose size $> q_2(q_3-1)$, it is not 1-error-detecting.

Proof: Suppose there exists a code whose size $> q_2(q_3-1)$. Fix the code. According to the Pigeonhole Principle, there exists a $\theta \in \{0, 1, \ldots, q_2-1\}$ such that the set $\mathcal{M}_\theta = \{m \in \mathcal{M} : \mathsf{c}_2(m) = \theta\}$ satisfies $|\mathcal{M}_\theta| > q_3 - 1$. Consider the following two cases:

(Case I) There exist two distinct messages $\bar{m}, \tilde{m} \in \mathcal{M}_\theta$ such that $\mathsf{c}_3(\bar{m}) = \mathsf{c}_3(\tilde{m})$. This case can be further divided into two subcases:

(Case I.A) The decoder satisfies $\bar{m} \neq \mathsf{Dec}(\mathsf{c}_1(\bar{m}), \mathsf{c}_3(\bar{m}))$. In this subcase, when A is to send $\bar{m}$, the adversary does nothing. It is easy to verify that the decoder does not output $\bar{m}$, which violates the first part of Definition 1.

(Case I.B) The decoder satisfies $\bar{m} = \mathsf{Dec}(\mathsf{c}_1(\bar{m}), \mathsf{c}_3(\bar{m}))$. In this subcase, when A is to send message $\tilde{m}$, the adversary maliciously changes the first transmission from $\mathsf{c}_1(\tilde{m})$ to $\mathsf{c}_1(\bar{m})$. The decoder outputs $\bar{m}$. That is, the recovered message is an erroneous message, which violates the second part of Definition 1.

(Case II) There do not exist two distinct messages $\bar{m}, \tilde{m} \in \mathcal{M}_\theta$ such that $\mathsf{c}_3(\bar{m}) = \mathsf{c}_3(\tilde{m})$. Since $|\mathcal{M}_\theta| > q_3 - 1$, we can easily assert that

$$\{\mathsf{c}_3(m) : m \in \mathcal{M}_\theta\} = \{0, 1, \ldots, q_3-1\}. \tag{1}$$

Now we fix a message $m \in \mathcal{M} \backslash \mathcal{M}_\theta$. Let $\widehat{c}_3 = \mathsf{Enc}_3(\theta, m)$. Due to equation (1) There exists a message $\widehat{m} \in \mathcal{M}_\theta$ such that $\widehat{c}_3 = \mathsf{c}_3(\widehat{m})$. Since $m \notin \mathcal{M}_\theta$ and $\widehat{m} \in \mathcal{M}_\theta$, we have $m \neq \widehat{m}$. Obviously, the codeword of $\widehat{m}$ is $\mathsf{c}_1(\widehat{m})\, \theta\, \widehat{c}_3$.

(Case II.A) The decoder satisfies $\widehat{m} = \mathsf{Dec}(\mathsf{c}_1(\widehat{m})\, \widehat{c}_3)$. In this subcase, when A is to send m, the adversary maliciously changes the symbol in the first transmission from $\mathsf{c}_1(m)$ to $\mathsf{c}_1(\widehat{m})$. Consequently, the symbols in these three transmissions become $\mathsf{c}_1(\widehat{m})\, \theta\, \widehat{c}_3$, and the decoder outputs $\widehat{m}$. Since $m \neq \widehat{m}$, the code is not 1-error-detecting.

(Case II.B) The decoder satisfies $\widehat{m} \neq \mathsf{Dec}(\mathsf{c}_1(\widehat{m})\, \widehat{c}_3)$. In this subcase, when A is to send $\widehat{m}$, the adversary does nothing. Then the inputs of the decoder is $\mathsf{c}_1(\widehat{m})\, \widehat{c}_3$, and the output of the decoder is not $\widehat{m}$. Therefore, the code is not 1-error-detecting.

In all aforementioned cases, the code is not 1-error-detecting. Therefore, any code whose size is $> q_2(q_3-1)$ is not 1-error-detecting. ∎

Using Lemma 1 and 2, we can assert that the size of any 1-error-detecting code is both $\leq q_1$ and $\leq q_2(q_3-1)$. Therefore, the maximum size of 1-error-detecting codes is upper bounded by $\min\{q_1, q_2(q_3-1)\}$.

C. Construct an 1-Error-Detecting Code

Lemma 3: There exists an 1-error-detecting code whose size is $\min\{q_1, q_2(q_3-1)\}$.

Code Construction: Let $a = \min\{q_1, q_2(q_3-1)\}$ and $a' = q_3 - 1$. We have $a/a' \leq q_2$. Now we consider a code whose message set is $\mathcal{M} = \{0, 1, \ldots, a-1\}$:

- *Encoder 1:* $\mathsf{Enc}_1(M) = M$
- *Encoder 2:* $\mathsf{Enc}_2(Y_1) = \lfloor Y_1/a' \rfloor$
- *Encoder 3:* $\mathsf{Enc}_3(Y_2, M) = \begin{cases} M \bmod a', & Y_2 = \lfloor M/a' \rfloor \\ a', & Y_2 \neq \lfloor M/a' \rfloor \end{cases}$
- *Decoder:* $\mathsf{Dec}(Y_1, Y_3) = \begin{cases} Y_1, & Y_1 \bmod a' = Y_3 \\ \varepsilon, & Y_1 \bmod a' \neq Y_3. \end{cases}$

Now we prove that this code is 1-error-detecting:

Proof: (I) Now we prove $\hat{M} = M$ or $\hat{M} = \varepsilon$ when $d_H(X_1X_2X_3, Y_1Y_2Y_3) \leq 1$.

(Case i) $Y_1 = X_1$: Since $\mathsf{Dec}(Y_1, Y_3) = Y_1$ or $\mathsf{Dec}(Y_1, Y_3) = \varepsilon$, so we have $\hat{M} = M$ or $\hat{M} = \varepsilon$.

(Case ii) $Y_1 \neq X_1$: Therefore, $\lfloor Y_1/a' \rfloor \neq \lfloor X_1/a' \rfloor$ or $Y_1 \bmod a' \neq X_1 \bmod a'$. In addition, we have $Y_2 = X_2$ and $Y_3 = X_3$.

(Subcase ii.a) $\lfloor Y_1/a' \rfloor \neq \lfloor X_1/a' \rfloor$: Since $Y_2 = X_2 = \lfloor Y_1/a' \rfloor$ and $\lfloor M/a' \rfloor = \lfloor X_1/a' \rfloor$, $Y_2 \neq \lfloor M/a' \rfloor$. Hence, $Y_3 = X_3 = a' \neq Y_1 \bmod a'$. Therefore, $\hat{M} = \varepsilon$.

(Subcase ii.b) $Y_1 \bmod a' \neq X_1 \bmod a'$: Since $Y_3 = X_3 = M \bmod a' = X_1 \bmod a'$ or $Y_3 = X_3 = a'$, we have $Y_1 \bmod a' \neq Y_3$. Therefore, $\hat{M} = \varepsilon$.

(II) Now we prove $\hat{M} = M$ when $X_1X_2X_3 = Y_1Y_2Y_3$. When there are no errors, $Y_1 = X_1 = M$, $Y_2 = X_2 = \lfloor M/a' \rfloor$, and $Y_3 = X_3 = M \bmod a'$, so we have $\hat{M} = Y_1 = M$.

Thus far, we have proved that this code is 1-error-detecting. ■

Since there exists an 1-error-detecting code whose size exactly equals the upper bound $\min\{q_1, q_2(q_3 - 1)\}$, the maximum size of 1-error-detecting codes is $\min\{q_1, q_2(q_3 - 1)\}$. That completes the proof of Theorem 1.

V. Conclusion and Further Work

In this paper, we characterized the fundamental limitation of error-resilient codes in three interactive transmissions, and derived the maximum size of 1-error-detecting codes. On the one hand, we gave an upper bound on the size of all 1-error-detecting codes; on the other hand, we constructed an 1-error-correcting code whose size equals the upper bound.

As mentioned, finding the maximum size of error-detecting/correcting codes in arbitrary number of interactive transmissions is still an open problem. Further works include extending the result in this paper to general number of transmissions.

Acknowledgment

This work was supported by the National Basic Research Program of China under Grant 2013CB329002, the National High Technology Research and Development Program of China under Grant 2014AA01A703, the National Science and Technology Major Project under Grant 2013ZX03004007, the Program for NCET in University under Grant NCET-13-0321, the International Science and Technology Cooperation Program under Grant 2012DFG12010, and the Tsinghua Research Funding under Grant 2010THZ03-2.

We thank Xiaohao Yang and Shenghao Yang for valuable suggestions on improving this paper.

References

[1] L. Schulman, "Communication on noisy channels: A coding theorem for computation," in *IEEE Symp. Foundations of Computer Science*, Oct. 1992, pp. 724–733.

[2] ——, "Deterministic coding for interactive communication," in *ACM Symp. Theory of Computing*, Jun. 1993, pp. 747–756.

[3] M. Braverman and A. Rao, "Towards coding for maximum errors in interactive communication," in *ACM Symp. Theory of Computing*, Jun. 2011, pp. 159–166.

[4] R. Gelles, A. Moitra, and A. Sahai, "Efficient and explicit coding for interactive communication," in *IEEE Symp. Foundations of Computer Science*, Oct. 2011, pp. 768–777.

[5] M. Braverman, "Towards deterministic tree code constructions," in *Proc. Innovations in Theoretical Computer Science Conference*, Jan. 2012, pp. 161–167.

[6] Z. Xiao, Y. Li, M. Zhao, and J. Wang, "Interactive code to correct and detect omniscient Byzantine adversaries," in *IEEE Inf. Theory Workshop*, Nov. 2014, pp. 45–49.