Multiple Object Identification Coding

Hirosuke Yamamoto, *Fellow, IEEE,* and Masashi Ueda

***Abstract*—In the case of ordinary identification coding, a code is devised to identify a single object among N objects. But, in this paper, we consider a coding problem to identify K objects at once among N objects in the both cases that K objects are ranked or not ranked. By combining Moulin-Koetter scheme with the ε-almost strongly universal class of hash functions used in Kurosawa-Yoshida scheme, an efficient and explicit coding scheme is proposed for K-multiple object identification (K-MOID) coding. Furthermore, it is shown that the K-MOID capacity $C_{K\text{-MOID}}$, which is the maximum achievable coding rate in the K-MOID coding, is equal to the ordinary channel capacity, and the proposed scheme can attain $C_{K\text{-MOID}}$.**

***Index Terms*—Identification coding, channel coding, multiple objects, passive feedback, common randomness.**

I. Introduction

CONSIDER a case such that we must inform many receivers about a winner, who is selected among them, via a stationary discrete memoryless channel. If each receiver is interested only in whether he/she is the winner or not, but is not interested in who wins when he/she is not the winner, an identification code (ID code) can be used to transmit the information efficiently. It is known for discrete memoryless channels (DMCs) that the decoding error probability of each receiver can become arbitrarily small if $R < C$, where C is the ordinary channel capacity of transmission coding and R is the ID coding rate defined by $R = (\log\log N)/n$ for the number of receivers N and the code length n [1]-[3]. In other words, the ID capacity C_{ID}, the maximum achievable R in ID coding, is equal to the channel capacity C.

Although the ID codes shown in [1]-[3] are not practical, explicit constructions of ID codes are studied in [4]-[6]. Verdú and Wei [4] showed that an ID code for a noisy channel can be constructed by concatenating an ID code for the noiseless channel and a transmission code (an ordinary error correcting code) for the noisy channel. They also gave an explicit ID code for the noiseless channel by using a constant weight binary matrix based on Reed-Solomon codes. Furthermore, Kurosawa and Yoshida [5] showed that a more efficient ID code for the noiseless channel can be constructed by generating the binary matrix based on ε-almost strongly universal (ε-ASU) classes of hash functions, and Moulin and Koetter [6] proposed another construction scheme of ID codes based on Reed-Solomon codes, which is efficient if common randomness can be used among the sender and receivers.

H. Yamamoto is with the Department of Complex Science and Engineering, the University of Tokyo, Kashiwa-shi, Chiba, 277-8561 Japan. (e-mail: hirosuke@ieee.org).

M. Ueda was with the Department of Mathematical Informatics, the University of Tokyo. He is currently with NS Solutions Corporation, Japan. (e-mail: ueda.masashi.fx6@jp.nssol.nssmc.com).

This work was presented in part at the 2014 IEEE international symposium on Information Theory. This work was supported in part by JSPS KAKENHI Grant Numbers 26630169 and 25289111.

In this paper, we consider the case that there are K winners among N receivers. In this case, we can send the information of winners by using an ordinary ID code K times. But, the coding rate is decreased to R/K. If we construct an ordinary ID code for $\tilde{N} = \binom{N}{K}$ and assign $\binom{N-1}{K-1}$ indices to each receiver, we can send the information with the same coding rate R as the case of $K = 1$. However, the type II decoding error probability becomes very large because each receiver must decode the received word for all $\binom{N-1}{K-1}$ indices. This means that the type II decoding error probability becomes $\binom{N-1}{K-1}$ times as large as the case of $K = 1$.

We note that Ahlswede [7][8] studied *K-Identification*. Let $\mathcal{N}$ and $\mathcal{K}_i$ be the set and a subset of all receivers, respectively, where $|\mathcal{N}| = N$ and $|\mathcal{K}_i| = K$, and $|\cdot|$ represents the cardinality of a set. Then, it is assumed in the K-identification problem that each receiver i knows the set $\mathcal{K}_i$, a codeword is encoded from only one $\hat{i} \in \mathcal{N}$, and each receiver i wants to know whether $\hat{i} \in \mathcal{K}_i$ or $\hat{i} \notin \mathcal{K}_i$. In [9], the K-Identification is further generalized to *Generalized Identification*, in which each receiver i not only finds out whether $\hat{i} \in \mathcal{K}_i$ or $\hat{i} \notin \mathcal{K}_i$, but also identifies $\hat{i}$ if $\hat{i} \in \mathcal{K}_i$. But, it is still assumed in the Generalized Identification that each receiver i knows $\mathcal{K}_i$ and a codeword is encoded from only one $\hat{i} \in \mathcal{N}$. In contrast, we assume in our coding problem that any receiver does not know $\mathcal{K}(\subset \mathcal{N})$, which is the set of winners selected at the sender side, a codeword is encoded from $\mathcal{K}$, and each receiver i wants to know whether $i \in \mathcal{K}$ or $i \notin \mathcal{K}$. So, since our coding problem is quite different from K-Identification and Generalized Identification, we cannot use their coding schemes for our coding problem.

We call our identification coding problem Multiple Object Identification (MOID) to distinguish from K-Identification and Generalized Identification, and the aim of this paper is to realize an explicit construction of efficient MOID codes.

In this paper, we show that an efficient and explicit MOID code can be constructed by combining Moulin-Koetter scheme [6] with the ε-ASU class of hash functions used in Kurosawa-Yoshida scheme [5]. For the proposed scheme, we derive the achievable region of coding rate and exponents of type I and type II decoding error probabilities for DMCs. As a result we show that the K-MOID capacity $C_{K\text{-MOID}}$, which is the maximum achievable coding rate in K-MOID coding, is equal to the channel capacity C, hence $C_{K\text{-MOID}}$ does not depend on K, and the proposed scheme can attain $C_{K\text{-MOID}}$ for any fixed K.

In Sections 2 and 3, we treat the cases that K winners are not ranked and are ranked, respectively.

For simplicity we first assume that K is fixed. But the case of variable K is considered in Section II-G. Furthermore, in Sections II-E and II-F, we treat the cases that the noiseless feedback channel and common randomness can be used be-

tween the sender and receivers. An ordinary error correcting code is called a transmission code to distinguish from an ID code in this paper, and the combined MOID coding with transmission coding is treated in Section II-D.

II. MOID CODE WITHOUT RANKING

A. Definition of MOID codes

Let $\mathcal{N} \equiv \{1, 2, \cdots, N\}$ be the set of objects and let $\mathcal{K}$ be a subset of $\mathcal{N}$, which is selected at the sender side. For simplicity, *objects* are called *receivers* in the following.

The sender sends binary information $u_i \in \mathcal{U} \equiv \{\mathrm{T}, \mathrm{F}\}$ to each receiver i such that $u_i = \mathrm{T}$ if $i \in \mathcal{K}$ and $u_i = \mathrm{F}$ if $i \notin \mathcal{K}$. In other words, $\mathcal{K}$ can be represented as follows:

$$\mathcal{K} \equiv \{i : u_i = \mathrm{T}, i \in \mathcal{N}\}. \tag{1}$$

For simplicity, we assume that $K \equiv |\mathcal{K}| \geq 1$ is fixed. Let $\mathcal{Z} \equiv \{\mathcal{K}\}$ be the set of all possible $\mathcal{K}$. Then we note that $|\mathcal{Z}|$ is given by $\binom{N}{K}$, and the ordinary ID coding corresponds to the case of $K = 1$.

The channel is a DMC W with input alphabet $\mathcal{X}$ and output alphabet $\mathcal{Y}$. For simplicity, we assume that the channel input is binary, i.e. $|\mathcal{X}| = 2$. But, the results can easily be extended to the case of $|\mathcal{X}| \geq 2$. We also assume that the encoder φ of an MOID code can use a random number v which takes a value of $\mathcal{V} = \{1, 2, \cdots, |\mathcal{V}|\}$. Then, the encoder φ to identify K receivers can be defined as follows:

$$\varphi : \mathcal{Z} \times \mathcal{V} \to \mathcal{X}^n, \tag{2}$$

where n is the code length, and a codeword x^n is generated by $x^n = \varphi(\mathcal{K}, v)$ from MOID information $\mathcal{K} \in \mathcal{Z}$ and random number $v \in \mathcal{V}$. This means that the encoder φ is a stochastic encoder for a given $\mathcal{K}$. The decoder ψ_i of receiver i, which outputs T or F, is defined as follows:

$$\psi_i : \mathcal{Y}^n \to \mathcal{U}. \tag{3}$$

An MOID code $(\varphi, \psi_1, \psi_2, \cdots, \psi_N)$ is called a K-MOID code if $K = |\mathcal{K}|$.

The coding rate $R_K^{(n)}$ of a K-MOID code is defined by[1]

$$R_K^{(n)} \equiv \frac{1}{n} \log \log N. \tag{4}$$

Next we consider the decoding error probabilities of a K-MOID code. Type I decoding error probability and its exponent are defined as follows:

$$\lambda_1^{(n)}(i|\mathcal{K}) \equiv \Pr\{\psi_i(\varphi(\mathcal{K}, V)) = \mathrm{F}\} \quad \text{for } i \in \mathcal{K}, \tag{5}$$

$$\lambda_1^{(n)} \equiv \max_{\mathcal{K} \in \mathcal{Z}} \max_{i \in \mathcal{K}} \lambda_1^{(n)}(i|\mathcal{K}), \tag{6}$$

$$E_1^{(n)} \equiv -\frac{1}{n} \log \lambda_1^{(n)}, \tag{7}$$

where $\lambda_1^{(n)}(i|\mathcal{K})$ represents the decoding error probability of receiver $i \in \mathcal{K}$, $\lambda_1^{(n)}$ is the worst of $\lambda_1^{(n)}(i|\mathcal{K})$, and $E_1^{(n)}$ is the exponent of $\lambda_1^{(n)}$.

[1]The base of logarithm is always 2 in this paper.

Similarly, type II decoding error probability is defined by

$$\lambda_2^{(n)}(i|\mathcal{K}) \equiv \Pr\{\psi_i(\varphi(\mathcal{K}, V)) = \mathrm{T}\} \quad \text{for } i \notin \mathcal{K}, \tag{8}$$

$$\lambda_2^{(n)} \equiv \max_{\mathcal{K} \in \mathcal{Z}} \max_{i \notin \mathcal{K}} \lambda_2^{(n)}(i|\mathcal{K}), \tag{9}$$

$$E_2^{(n)} \equiv -\frac{1}{n} \log \lambda_2^{(n)}, \tag{10}$$

where $\lambda_2^{(n)}(i|\mathcal{K})$ is the decoding error probability of receiver $i \notin \mathcal{K}$, $\lambda_2^{(n)}$ is the worst of $\lambda_2^{(n)}(i|\mathcal{K})$, and $E_2^{(n)}$ is the exponent of $\lambda_2^{(n)}$.

A triplet (R, E_1, E_2) is said to be achievable by a coding scheme if the coding scheme can satisfy the following inequalities:

$$\liminf_{n \to \infty} R_M^{(n)} \geq R, \tag{11}$$

$$\liminf_{n \to \infty} E_1^{(n)} \geq E_1, \tag{12}$$

$$\liminf_{n \to \infty} E_2^{(n)} \geq E_2. \tag{13}$$

The K-MOID capacity $C_{K\text{-MOID}}$ is defined as the maximum achievable R in K-MOID coding, i.e.,

$$C_{K\text{-MOID}} \equiv \max\{R \mid (R, E_1, E_2) \text{ is achievable}\}. \tag{14}$$

Remark 1: When $K = 1$, the K-MOID code coincides with the ordinary ID code. Hence, coding rate $R_K^{(n)}$, error exponents $E_1^{(n)}$ and $E_2^{(n)}$, and $C_{K\text{-MOID}}$ also coincide with the ones of the ordinary ID code and C_{ID}, respectively.

For $K = 1$, the following triplet is achievable by the first Verdú-Wei coding scheme [4, Proposition 4] and Kurosawa-Yoshida coding scheme [5]:

$$(R, E_1, E_2) = \left(\left(1 - \frac{3}{\ell}\right) r, E(r), \min\left\{\frac{r}{\ell}, E(r)\right\}\right), \quad 0 < r < C, \quad \ell = 3, 4, 5, \cdots, \tag{15}$$

where $E(r)$ is the reliability function (or the error exponent) of DMC W in transmission coding with coding rate r, C is the ordinary channel capacity of W given by $C = \max_{P_X} I(X;Y)$, and r and ℓ are parameters that we can select freely. Furthermore, the following triplet is also achievable by the second Verdú-Wei coding scheme [4, Proposition 5] and Moulin-Koetter coding scheme [6]:

$$(R, E_1, E_2) = \left(\rho r, E(r), \min\left\{\left(\frac{1}{2} - \rho\right) r, E(r)\right\}\right), \quad 0 < r < C, \quad 0 \leq \rho \leq \frac{1}{2}, \tag{16}$$

where r and ρ are parameters.

It is known for $K = 1$ that (R, E_1, E_2) must satisfy the following theorem.

Theorem 1 ([1, Theorem 2] [4, Theorem 4]): If (R, E_1, E_2) is achievable and $E_1 > 0$ for a DMC W, then

$$R + 2E_2 \leq C. \tag{17}$$

This bound is tight if either (a) the channel W is noiseless or (b) $E_1 \to 0_+$, and hence $C_{\mathrm{ID}} = C$.

Note from (15) and (16) that the former and latter coding schemes must satisfy $R + 3E_2 \leq C$ and $R + E_2 \leq C/2$,

respectively, for any DMC, and can attain $R + 3E_2 = C$ and $R + E_2 = C/2$, respectively, for the noiseless channel, which has $E(r) = \infty$ and $r = C$. Furthermore, for any DMC, the former coding schemes can attain the ID capacity $C_{\rm ID}$ by setting r sufficiently close to C and l sufficiently large. On the other hand, R cannot become larger than $C/2$ in the latter coding schemes. But, the latter coding schemes have larger E_2 than the former coding schemes in low R because they satisfy $\max_{\ell} E_2 = r/3$ and $\max_{\rho} E_2 = r/2$, respectively.

It is worth noting that (17) also holds for $K \geq 2$.

B. K-repeated coding of known ID codes

An MOID code for a noisy channel can be constructed by concatenating an MOID code for the noiseless channel and a transmission code for the noisy channel in the same way as the ordinary ID coding [4]. So, we first review the known coding schemes for the noiseless channel in the case of the ordinary ID coding, i.e, $K = 1$.

In Verdú-Wei coding schemes [4] and Kurosawa-Yoshida coding scheme [5], an $N \times |\mathcal{V}|$ binary matrix $(b_{i,v})$ is used for ID coding, where $i \in \mathcal{N}$ and $v \in \mathcal{V}$, and each i-th vector $(b_{i,1}, b_{i,2}, \cdots, b_{i,|\mathcal{V}|})$ of the matrix is distributed to receiver i in advance. Random number v is selected uniformly over $\mathcal{V}_i \equiv \{v | b_{i,v} = 1\}$ when ID information is i, and the index of v in $\mathcal{V}$ is used as the codeword. Each decoder $\psi_{\hat{i}}$ outputs T or F if $b_{\hat{i},v} = 1$ or $b_{\hat{i},v} = 0$, respectively. The binary matrix $(b_{i,v})$ is determined based on a concatenated code of Reesd-Solomon codes in Verdú-Wei schemes or based on ε-ASU classes of hash functions in Kurosawa-Yoshida scheme. Refer [4] and [5] for more details.

The above coding schemes can be extended to the K-MOID coding by replacing a single v with a K dimensional vector $(v_1, v_2, \cdots, v_K)$, where $v_j \in \mathcal{V}_{i_j} \subset \mathcal{V}$ for $\mathcal{K} = \{i_1, i_2, \cdots, i_K\}$. But, since the code length becomes K times long and hence the coding rate decreases to $1/K$ for the noiseless channel, these K-repeated coding schemes have the following triplet from (15) and (16): [2]

$$(R, E_1, E_2) = \left(\left(1 - \frac{3}{\ell}\right) \frac{r}{K}, E(r), \min\left\{ \frac{r}{K\ell}, E(r) \right\} \right), \quad 0 < r < C, \quad \ell = 3, 4, 5, \cdots, \tag{18}$$

or

$$(R, E_1, E_2) = \left(\frac{\rho r}{K}, E(r), \min\left\{ \left(\frac{1}{2} - \rho\right) \frac{r}{K}, E(r) \right\} \right), \quad 0 < r < C, \quad 0 \leq \rho \leq \frac{1}{2}. \tag{19}$$

As a result, the K-repeated coding schemes attain $R + 3E_2 = C/K$ or $R + E_2 = C/(2K)$ for the noiseless channel, and must satisfy $R + 3E_2 \leq C/K$ or $R + E_2 \leq C/(2K)$ for any DMC. Hence, R cannot become larger than C/K or $C/(2K)$, which tends to zero as K becomes large.

In Moulin-Koetter coding scheme [6], the codeword of ID information i consists of $(v, c_v(i))$ where $c_v(i)$ is the v-th symbol of the i-th codeword of Reed-Solomon code over GF(2^m). Random number v is selected uniformly over $\mathcal{V} = \{1, 2, \cdots, |\mathcal{V}|\}$, where $|\mathcal{V}|$ is the code length of the Reed-Solomon code. Each decoder $\psi_{\hat{i}}$ outputs T or F if $c_v(\hat{i}) = c$ or $c_v(\hat{i}) \neq c$, respectively, for a received codeword (v, c). This coding scheme can be extended to the K-MOID coding by replacing the codeword $(v, c_v(i))$ with $(v, c_v(i_1), c_v(i_2), \cdots, c_v(i_K))$. But, since the code length of Reed-Solomon code is given by $|\mathcal{V}| = 2^m$, v and $c_v(i)$ must satisfy $\|v\| = \|c_v(i)\|$ in their scheme, where $\|a\|$ represents the bit length of a. This means that the length of the extended Moulin-Koetter coding scheme becomes $(K + 1)/2$ times longer and the coding rate decreases to $2/(K + 1)$. Therefore the triplet is given by

$$(R, E_1, E_2) = \left(\frac{2\rho}{K+1} r, E(r), \min\left\{ \frac{1 - 2\rho}{K+1} r, E(r) \right\} \right), \quad 0 < r < C, \quad 0 \leq \rho \leq \frac{1}{2}. \tag{20}$$

As a result, the extended Moulin-Koetter coding scheme attains $R + E_2 = C/(K + 1)$ for the noiseless channel, and must satisfy $R + E_2 \leq C/(K + 1)$ for any DMC. Hence, R cannot become larger than $C/(K+1)$, which tends to zero as K becomes large.

C. Construction of efficient MOID codes

In order to construct an efficient MOID code, we use a codeword $(v, h_v(i))$ instead of $(v, c_v(i))$, where $h_v(i)$ is an ε-ASU class of hash functions satisfying $\|v\| \gg \|h_v(i)\|$. In this case, even if we extend the codeword $(v, h_v(i))$ to $(v, h_v(i_1), h_v(i_2), \cdots, h_v(i_K))$ for the K-MOID coding, the coding rate does not decrease significantly.

Now we describe our coding scheme for the MOID coding. We use the ε-ASU class of hash functions $\mathcal{H} = \{h_l\}$ used in Kurosawa-Yoshida scheme [5], which satisfies the following relations for $h_l : \mathcal{A} \to \mathcal{B}$.

$$|\{h_l \in \mathcal{H} : h_l(\alpha) = \beta\}| = \frac{|\mathcal{H}|}{|\mathcal{B}|}, \quad \text{for } \forall \alpha \in \mathcal{A}, \forall \beta \in \mathcal{B}, \tag{21}$$

$$|\{h_l \in \mathcal{H} : h_l(\alpha_1) = \beta_1, h_l(\alpha_2) = \beta_2\}| \leq \varepsilon \frac{|\mathcal{H}|}{|\mathcal{B}|}, \quad \text{for } \forall \alpha_1, \alpha_2 \in \mathcal{A}, \alpha_1 \neq \alpha_2, \forall \beta_1, \beta_2 \in \mathcal{B}\ . \tag{22}$$

Then the following lemma holds.

Lemma 1 ([5, Corollary 3.1]): If there exists an error-correcting code over GF(q^k) such that the code length is n_0, the minimum Hamming distance is d, and the number of codewords is M, then we can construct an ε-ASU class of hash functions $\mathcal{H}$ that satisfies

$$|\mathcal{A}| = M, \tag{23}$$

$$|\mathcal{B}| = q, \tag{24}$$

$$|\mathcal{H}| = n_0 q^2, \tag{25}$$

$$\varepsilon = \frac{k}{q} + 1 - \frac{d}{n_0}. \tag{26}$$

[2] $E(r)$ is not divided by K because $E(r)$ comes from the transmission coding and is not related to the ID coding for the noiseless channel. Refer the proof of Theorem 2.

In order to construct a K-MOID code, we set $\mathcal{A}$ and $\mathcal{H}$ as $\mathcal{A} = \mathcal{N}$ ($|\mathcal{A}| = N$) and $|\mathcal{H}| = |\mathcal{V}|$, respectively. Let f and g be the encoder and decoder, respectively, of a transmission code for noisy channel W such that $f : \mathcal{V} \times \beta^K \to \mathcal{X}^n$ and $g : \mathcal{Y}^n \to \mathcal{V} \times \beta^K$. Then, we construct K-MOID code $(\varphi, \psi_1, \psi_2, \cdots, \psi_N)$ as follows:

Coding Scheme 1:

Encoder φ :

For $\mathcal{K} = \{i_1, i_2, \cdots, i_K\} \subset \mathcal{N}$,

$$\varphi(\mathcal{K}, v) \equiv f(v, h_v(i_1), h_v(i_2), \cdots, h_v(i_K)). \quad (27)$$

Decoder ψ_i:

$$\psi_i(y^n) \equiv \begin{cases} \mathrm{T}, & \text{if } h_{\hat{v}}(i) = \beta_j \text{ holds} \\ & \quad \text{for some } j,\ 1 \le j \le K \\ \mathrm{F}, & \text{otherwise} \end{cases}$$
$$\text{for } (\hat{v}, \beta_1, \beta_2, \cdots, \beta_K) = g(y^n), \quad (28)$$

where v is a random number distributed uniformly over $\mathcal{V}$.

This K-MOID code satisfies the following theorem.

Theorem 2: The following triplet is achievable by Coding Scheme 1:

$$(R, E_1, E_2) = \left(\left(1 - \frac{K+3}{K+\ell}\right) r, E(r), \min\left\{ \frac{r}{K+\ell}, E(r) \right\} \right), \quad 0 < r < C, \quad \ell = 3, 4, 5, \cdots. \quad (29)$$

Proof: First we construct a K-MOID code with code length n_0 for the binary noiseless channel by using the ε-ASU class of hash functions given in Lemma 1. If we use (q^k, q^t)-Reed-Solomon code with $q = 2^m$ as an error-correcting code in Lemma 1, which has $n_0 = q^k$, $d = q^k - q^t + 1$, and $M = (q^k)^{q^t}$, we obtain the ε-ASU class of hash functions that satisfies

$$|\mathcal{A}| = N = q^{kq^t}, \quad (30)$$
$$|\mathcal{B}| = q \quad (\mathcal{B} = \mathrm{GF}(q)), \quad (31)$$
$$|\mathcal{V}| = |\mathcal{H}| = q^{k+2}, \quad (32)$$
$$\varepsilon = \frac{k}{q} + \frac{q^t - 1}{q^k} \le \frac{1}{q}\left(k + \frac{q^t}{q^{k-1}}\right), \quad (33)$$

where $t \le k-1$ because it must hold that $\varepsilon \to 0$ as $m \to \infty$ (i.e., $q \to \infty$).

Then, from (31), (32), and $q = 2^m$, the code length $n_0 = \|(v, h_v(i_1), h_v(i_2), \cdots, h_v(i_K))\|$ is given by

$$n_0 = \log|\mathcal{V}| + K\log|\mathcal{B}| = (k + 2 + K)m. \quad (34)$$

Hence, from (30) and (34), the coding rate of this code satisfies

$$\begin{aligned} R_K^{(n_0)} &= \frac{1}{n_0}\log\log N \\ &= \frac{1}{n_0}\log\left\{kq^t \log q\right\} \\ &= \frac{1}{n_0}\left\{tm + \log k + \log m\right\} \\ &= \frac{t}{k+2+K} + \frac{1}{n_0}(\log k + \log m) \\ &= \frac{t}{k+2+K} + O\left(\frac{\log n_0}{n_0}\right). \end{aligned} \quad (35)$$

Since the optimal t that maximizes (35) for $1 \le t \le k-1$ is $t = k-1$, we can attain the following coding rate:

$$\begin{aligned} R_K^{(n_0)} &= \frac{k-1}{k+2+K} + O\left(\frac{\log n_0}{n_0}\right) \\ &= 1 - \frac{K+3}{k+2+K} + O\left(\frac{\log n_0}{n_0}\right). \end{aligned} \quad (36)$$

Next we evaluate the decoding error probabilities. In the case of the noiseless channel, every ψ_i always outputs T if $i \in \mathcal{K}$. Hence for any $\mathcal{K} \in \mathcal{Z}$ and any $i \in \mathcal{K}$, $\lambda_1^{(n_0)}(i|\mathcal{K}) = 0$. This means that $\lambda_1^{(n_0)} = 0$ and $E_1^{(n_0)} = \infty$.

For $\mathcal{K} = \{i_1, i_2, \cdots, i_K\}$ and $i \notin \mathcal{K}$, $\lambda_2^{(n_0)}(i|\mathcal{K})$ is bounded as follows:

$$\begin{aligned} \lambda_2^{(n_0)}(i|\mathcal{K}) &= \Pr\left\{ \bigcup_{j=1}^{K} (h_V(i) = h_V(i_j)) \right\} \\ &\le \sum_{j=1}^{K} \Pr\left\{h_V(i) = h_V(i_j)\right\} \\ &= K\frac{\sum_{\beta\in\mathcal{B}} |\{h_v : h_v(i) = h_v(i_j) = \beta\}|}{|\mathcal{V}|} \\ &\le \varepsilon K, \end{aligned} \quad (37)$$

where the first and second inequalities hold from the union bound and (22), respectively. Since this bound does not depend on $\mathcal{K}$ and $i \notin \mathcal{K}$, $\lambda_2^{(n)}$ has the same bound:

$$\lambda_2^{(n_0)} \le \varepsilon K. \quad (38)$$

Next we evaluate $E_2^{(n)}$, the exponent of $\lambda_2^{(n)}$. From (10), (33), (34), and (38), $E_2^{(n_0)}$ has the following bound for $t \le k-1$:

$$\begin{aligned} E_2^{(n_0)} &\ge -\frac{1}{n_0}\{\log K + \log\varepsilon\} \\ &\ge -\frac{1}{n_0}\left\{\log K - \log q + \log\left(k + \frac{q^t}{q^{k-1}}\right)\right\} \\ &= \frac{1}{k+2+K} - \frac{1}{n_0}\left\{\log K + \log\left(k + \frac{q^t}{q^{k-1}}\right)\right\} \\ &= \frac{1}{k+2+K} - O\left(\frac{\log k}{n_0}\right). \end{aligned} \quad (39)$$

Setting $\ell = k+2$, $\ell = 3, 4, \cdots$, and $m \to \infty$, i.e. $n_0 \to \infty$, in (36) and (39), we note that the following triplet is achievable for the binary noiseless channel:

$$(R, E_1, E_2) = \left(1 - \frac{K+3}{K+\ell},\ \alpha,\ \frac{1}{K+\ell}\right), \quad (40)$$

where $\alpha > 0$ is an arbitrarily large constant.

Next we treat the case of a DMC W. If we transmit $(v, h_v(i_1), h_v(i_2), \cdots, h_v(i_K))$ via W by using the best transmission code (f, g) of W with coding rate r, $0 < r < C$, then the code length n is given by $n = n_0/r$ and the decoding error probability of the transmission code is upper bounded by $2^{-nE(r)}$, where $E(r)$ and C are the reliability function and the channel capacity of W, respectively. Hence, the total error probability $\lambda_j^{(n)}$, $j = 1, 2$, is bounded as follows:

$$\lambda_j^{(n)} \le 2^{-n_0 E_j^{(n_0)}} + 2^{-nE(r)} \le 2 \cdot 2^{-n \min\{r E_j^{(n_0)}, E(r)\}}. \tag{41}$$

From (40) and (41), the triplet given by (29) is achievable. Q.E.D.

From (29), Coding Scheme 1 must satisfy $R + (K+3)E_2 \le C$ for any DMC, and attain $R + (K+3)E_2 = C$ for the noiseless channel. Furthermore, for any DMC, R can be enlarged to C by setting r sufficiently close to C and ℓ sufficiently large. Hence, by combining this result with (17), we obtain the following corollary.

Corollary 1: The K-MOID capacity $C_{K\text{-MOID}}$ is given by

$$C_{K\text{-MOID}} = C. \tag{42}$$

Coding Scheme 1 can attain $C_{K\text{-MOID}}$, and this is a big advantage over the other schemes treated in Section II-B, which cannot attain $C_{K\text{-MOID}}$. We note from (42) that the K-MOID capacity $C_{K\text{-MOID}}$ does not depend on K.

Remark 2: Corollary 1 can also be proved by modifying the coding scheme used in [2, Section III]. But, such proof can show only the existence of a MOID code that achieves $C_{K\text{-MOID}}$. On the other hand, we showed in this paper that $C_{K\text{-MOID}}$ can be achieved by an explicit MOID coding scheme.

Remark 3: In (29), we have $R = 0$ when $\ell = 3$. In this case, $R_K^{(n)} \equiv (\log\log N)/n$ tends to zero as $n \to 0$. But, $\widehat{R}_K^{(n)} \equiv (\log N)/n$ does not tend to zero because it holds from (30), (34), $q = 2^m$, and $r = n_0/n$ that for $t = k - 1 = \ell - 3 = 0$,

$$\begin{aligned} \widehat{R}_K^{(n)} &= \frac{\log N}{n} \\ &= \frac{kq^t \log q}{n} \\ &= \frac{m}{(3+K)m/r} \\ &= \frac{r}{3+K}. \end{aligned} \tag{43}$$

Hence, $\ell = 3$ can be used in the case such that we require relatively large E_2 but we do not need huge N.

Remark 4: From Theorem 2, Coding Scheme 1 achieves for $K = 1$ that

$$\begin{aligned} &(R, E_1, E_2) \\ &\quad = \left(\left(1 - \frac{4}{1+\ell} \right) r, E(r), \min\left\{ \frac{r}{1+\ell}, E(r) \right\} \right), \\ &\qquad 0 < r < C, \quad \ell = 3, 4, 5, \cdots. \end{aligned} \tag{44}$$

This triplet is a little worse than (15), which is the triplet of the first Verdú-Wei coding scheme and the Kurosawa-Yoshida coding scheme. But, for $K \ge 2$, Coding Scheme 1 can attain the K-MOID capacity although the other schemes cannot attain it. Furthermore, Coding Scheme 1 also has advantages for $K \ge 1$ if the encoder and decoders can use common randomness or a noiseless feedback channel as shown in Sections II-E and II-F.

D. K-MOID Coding with a Transmission Message

It is shown in [3] that an ID code can send a transmission message in addition to an ID message at once. Actually ID codes given in [4]–[6] can realize such coding. In the case of Coding Scheme 1, we note from (28) that random number v can be decoded by $g(y^n)$ at each decoder ψ_i. This means that we can send information v to receivers with a K-MOID message $\mathcal{K}$. Hence, if we assign v to a transmission message, which is distributed uniformly over $\mathcal{V}$, instead of the random number, then we can send receivers the transmission message v with the K-MOID message.

In this case, the coding rate $R_T^{(n)}$ of the transmission message is given by

$$\begin{aligned} R_T^{(n)} &\equiv \frac{1}{n} \log |\mathcal{V}| \\ &= \frac{n_0}{n} \frac{1}{n_0} \log |\mathcal{V}| \\ &= r \frac{\ell}{\ell + K}, \quad \ell = 3, 4, \cdots \end{aligned} \tag{45}$$

from (32), (34), and $r = n_0/n$. Hence, by setting r sufficiently close to C and ℓ sufficiently large, Coding Scheme 1 can attain the channel capacity for transmission coding and the K-MOID capacity for MOID coding at once.

E. K-MOID Coding with Common Randomness

If the encoder and decoders can use common randomness, e.g. a good pseudo random number generator, we do not need to send some or all bits of random number v in the same way as Moulin-Koetter scheme [6, Section 8].

Assume that we can use n_{0c}-bit common randomness, and define the rate of the common randomness by $R_{0c} = n_{0c}/n_0$ where, from (34), $n_0 = (\ell + K)m$ and $0 \le n_{0c} \le \ell m$ for $k + 2 = \ell = 3, 4, \cdots$. Hence, we have $0 \le R_{0c} \le \ell/(\ell + K)$. Since we do not need send $n_{0c} = R_{0c} n_0$ bits, the code length for the noiseless channel can be shortened to $n_0 - n_{0c} = n_0(1 - R_{0c})$ bits. Hence, we have from (29) that

$$\begin{aligned} &(R, E_1, E_2) \\ &\quad = \left(\left(1 - \frac{K+3}{K+\ell} \right) \frac{r}{1 - R_{0c}}, E(r), \right. \\ &\qquad\qquad \left. \min\left\{ \frac{1}{K+\ell} \frac{r}{1 - R_{0c}}, E(r) \right\} \right), \\ &\qquad 0 < r < C, \quad \ell = 3, 4, 5, \cdots. \end{aligned} \tag{46}$$

Now consider the case of maximum R_{0c}, i.e. $R_{0c} = \ell/(\ell+K)$. In this case, (R, E_1, E_2) is maximized and (46) becomes

$$(R, E_1, E_2) = \left(\frac{\ell-3}{K} r, E(r), \min\left\{ \frac{r}{K}, E(r) \right\} \right), \quad 0 < r < C, \quad \ell = 3, 4, 5, \cdots. \tag{47}$$

Hence, R can be enlarged arbitrarily by setting ℓ sufficiently large. This property comes from the fact that $\|h_v(i)\|/\|v\| \to 0$ as $\ell \to \infty$.

Note that Verdú-Wei schemes, Kurosawa-Yoshida scheme, and their K-repeated coding schemes treated in Section II-B cannot use common randomness because random number v must be selected over $\mathcal{V}_i$, which depends on ID message i. In the case of the extended Moulin-Koetter scheme, the codeword $(v, c_v(i_1), c_v(i_2), \cdots, c_v(i_K))$ can be shorten to $(c_v(i_1), c_v(i_2), \cdots, c_v(i_K))$ if common randomness can be used. But, the improvement of coding rate is only $K/(K+1)$ because $\|v\| = \|c_v(i_j)\|$ holds for all i_j. Hence, Coding Scheme 1 is much more efficient than the known coding schemes when common randomness can be used for MOID coding.

When $R_{0c} = \ell/(\ell+K)$, the following R can be achieved by setting $r \to C$ in (47):

$$R = \frac{\ell-3}{K} C = \left(\frac{R_{0c}}{1-R_{0c}} - \frac{3}{K} \right) C. \tag{48}$$

On the other hand, it is known from [10, Theorem 2] that the ID capacity for $K = 1$ with common randomness is equal to the sum of C and the bits of common randomness per channel symbol. In our case, this ID capacity is given by

$$C_{\text{ID}} = C + \frac{n_{c0}}{(n_0 - n_{0c})/C} = \left(\frac{1}{1-R_{0c}} \right) C. \tag{49}$$

Note that $C_{K\text{-MOID}} \le C_{\text{ID}}$. Hence, we can conclude by comparing (48) with (49) that Coding scheme 1 almost attains the K-MOID capacity when R_{0c} is close to 1, i.e. ℓ is sufficiently large.

F. K-MOID Coding with Noiseless Feedback

It is shown in [2] that if we can use a passive noiseless feedback channel such that the encoder can know the channel output Y_t at each time $t = 1, 2, \cdots, n-1$, then the ID capacity is given by

$$C_{\text{ID}}^{\text{f,d}} \equiv \max_{x \in \mathcal{X}} H(W(\cdot|x)) \quad \text{if the encoder is deterministic,} \tag{50}$$

$$C_{\text{ID}}^{\text{f,s}} \equiv \max_{P \in \mathcal{P}(\mathcal{X})} H(P \cdot W) \quad \text{if the encoder is stochastic.} \tag{51}$$

Here $W(\cdot|\cdot)$ is the transition probability of the forward channel W, $\mathcal{P}(\mathcal{X})$ is the set of input probability distributions, and $P \cdot W$ is the output probability distribution for input probability distribution $P \in \mathcal{P}(\mathcal{X})$.

Coding scheme 1 can attain $C_{\text{ID}}^{\text{f,d}}$ and $C_{\text{ID}}^{\text{f,s}}$ as follows. We first send $x^{\tilde{n}}$, where x_t, $t = 1, 2, \cdots, \tilde{n}$, is the optimal fixed input $\tilde{x}$ that achieves the maximum of (50) in the deterministic case, or is generated by the optimal input probability distribution $\tilde{P}$ that achieves the maximum of (51) in the stochastic case. Then the encoder and decoders can obtain random number v from the corresponding channel output $y^{\tilde{n}}$ by using the interval algorithm for random number generation [11]. After v is obtained at the encoder and decoders, the encoder sends $(h_v(i_1), h_v(i_2), \cdots, h_v(i_M))$ by a transmission code with code length $n^* = Km/r$.

In order to obtain v uniformly distributed over $\{0, 1, 2, \cdots, 2^{\ell m} - 1\}$ by the interval algorithm, we use variable length $\tilde{n}$. Then the expected length $\mathrm{E}[\tilde{n}]$ is bounded as follows [11, Theorem 3]:

$$\frac{\ell m}{H} \le \mathrm{E}[\tilde{n}] \le \frac{1}{H} \left(\ell m + \log 2(|\mathcal{Y}| - 1) + \frac{h(p_{\max})}{1 - p_{\max}} \right), \tag{52}$$

where $p_{\max} = \max_{y \in \mathcal{Y}} P_Y(y)$, $h(\cdot)$ is the binary entropy function, and $H = H(W(\cdot|\tilde{x}))$ or $H = H(\tilde{P} \cdot W)$ if the encode is deterministic or stochastic, respectively.

In this case, coding rate R', which is defined by $R' = (\log\log N)/(\mathrm{E}[\tilde{n}] + n^*)$, satisfies that

$$R' = \frac{\log\log N}{\mathrm{E}[\tilde{n}] + n^*} = \frac{(\ell-3)m + \log(\ell-2) + \log m}{\mathrm{E}[\tilde{n}] + Km/r} \to H \quad \text{as } m \to \infty \text{ and } \ell \to \infty, \tag{53}$$

where the second equality holds from (30), $t = k - 1 = \ell - 3$, and $n^* = Km/r$. Hence, Coding Scheme 1 can attain $C_{\text{ID}}^{\text{f,d}}$ and $C_{\text{ID}}^{\text{f,s}}$ for K-MOID coding if variable length coding is allowed.

In the above, we used the interval algorithm to realize an explicit coding scheme. But, if we do not require an explicit coding scheme, we can use the same coding technique shown in [2] to obtain v with ℓm bits, which needs code length $\tilde{n} = \ell m/H + o(\tilde{n})$. Refer [2] for more details. In this case, we have that

$$R = \frac{\log\log N}{\tilde{n} + n^*} = \frac{(\ell-3)m + \log(\ell-2) + \log m}{\ell m/H + o(\tilde{n}) + Km/r} \to H \quad \text{as } m \to \infty \text{ and } \ell \to \infty, \tag{54}$$

Hence, the K-MOID capacity with feedback is given by $C_{K\text{-MOID}}^{fd} = C_{ID}^{fd}$ and $C_{K\text{-MOID}}^{fs} = C_{ID}^{fs}$.

G. MOID Coding with variable K

In the above subsections, we assumed for simplicity that K is fixed and known. But, if K is variable and the decoders do not know K, the encoder must send the information of K to the decoders. For instance, this can be realized if we define the encoder φ as $\varphi(\mathcal{K}, v) = f(K, v, h_v(i_1), h_v(i_2), \cdots, h_v(i_K))$ instead of (27).

If the maximum value of K, $K_{\max}$, is given, K can be represented by $\lceil \log K_{\max} \rceil$ bits. If $K_{\max}$ is not known, K can

be represented by Elias δ code [12], the length of which is not larger than $1+\log K+2\log(1+\log K)$ bits. Since these additional bits can be ignored compared with $n_0=(\ell+K)m$ as $m\to\infty$, Theorem 2 still holds even if K is variable. However, we note from (35) that $\log\log N\approx(\ell-3)m$. Hence, K must satisfy that $\log K\ll n_0=(\ell+K)m=\log\log N-(K-3)m<\log\log N$, which means

$$\lim_{m\to\infty}\frac{K}{\log N}=0. \tag{55}$$

Furthermore, from (29), R and E_2 decrease to zero as K becomes large for fixed r and ℓ.

III. MOID CODE WITH RANKING

A. Definition of RMOID codes

In Section II, we assumed that selected K receivers are not ranked. But, in this section, we consider the case that K receivers are ranked. Let $\boldsymbol{K}\equiv(i_1,i_2,\cdots,i_K)$, where i_j stands for the receiver of rank j. Then, encoder $\tilde{\varphi}$ and decoder $\tilde{\psi}_i$ for K ranked receivers can be defined as follows:

$$\tilde{\varphi}:\tilde{\mathcal{Z}}\times\mathcal{V}\to\mathcal{X}^n \tag{56}$$

$$\tilde{\psi}_i:\mathcal{Y}^n\to\{1,2,\cdots,K,\mathrm{F}\}, \tag{57}$$

where $\tilde{\mathcal{Z}}=\{\boldsymbol{K}\}$, which is the set of all possible $\boldsymbol{K}$, and F means "outside of the ranking". We call this code K-RMOID (ranked-multiple-object identification) code.

Although we can consider many types of errors for this K-RMOID code $(\tilde{\varphi},\tilde{\psi}_1,\tilde{\psi}_2,\cdots,\tilde{\psi}_N)$, we group the errors into only two types. To simplify notation, we treat F as rank $K+1$. Then, the type I (resp. II) error is defined as the error such that a decoded rank of a receiver is larger (resp. smaller) than the true rank of the receiver.

Let $\tilde{\lambda}_1^{(n)}$ and $\tilde{\lambda}_2^{(n)}$ be the worst probability of type I and II errors, respectively. Then, they can be represented as follows:

$$\tilde{\lambda}_1^{(n)}(i_j|\boldsymbol{K})\equiv\Pr\{\tilde{\psi}_{i_j}(\tilde{\varphi}(\boldsymbol{K},V))>j\} \tag{58}$$

$$\tilde{\lambda}_1^{(n)}\equiv\max_{\boldsymbol{K}\in\tilde{\mathcal{Z}}}\max_{i_j}\tilde{\lambda}_1^{(n)}(i_j|\boldsymbol{K}), \tag{59}$$

$$\tilde{\lambda}_2^{(n)}(i_j|\boldsymbol{K})\equiv\Pr\{\tilde{\psi}_{i_j}(\tilde{\varphi}(\boldsymbol{K},V))<j\}, \tag{60}$$

$$\tilde{\lambda}_2^{(n)}\equiv\max_{\boldsymbol{K}\in\tilde{\mathcal{Z}}}\max_{i_j}\tilde{\lambda}_2^{(n)}(i_j|\boldsymbol{K}). \tag{61}$$

Furthermore, the error exponents of $\tilde{\lambda}_1^{(n)}$ and $\tilde{\lambda}_2^{(n)}$ are defined by

$$\tilde{E}_1^{(n)}\equiv-\frac{1}{n}\log\tilde{\lambda}_1^{(n)}, \tag{62}$$

$$\tilde{E}_2^{(n)}\equiv-\frac{1}{n}\log\tilde{\lambda}_2^{(n)}. \tag{63}$$

Remark 5: From the definition of decoder $\tilde{\psi}_i$ given by (57), we note that $\tilde{\lambda}_1^{(n)}(i_{K+1}|\boldsymbol{K})=\tilde{\lambda}_2^{(n)}(i_1|\boldsymbol{K})=0$. This means that we can exclude receivers with rank $j=K+1$ (i.e. F) and the receiver with rank $j=1$ in the maximization $\max_{i_j}$ of (59) and (61), respectively. Hence, we can easily check that the type I and II errors defined in this section coincide with the ordinary ones in the case of $K=1$. Furthermore, if all ranks j, $1\le j\le K$, are treated as the same rank, (60) and (61) coincide with (6) and (9), respectively. Therefore, the definition of type I and II errors given by (58)-(61) are reasonable.

A triplet $(R,\tilde{E}_1,\tilde{E}_2)$ is said to be achievable by a coding scheme if the following inequalities can be satisfied by the coding scheme:

$$\liminf_{n\to\infty}R_M^{(n)}\ge R, \tag{64}$$

$$\liminf_{n\to\infty}\tilde{E}_1^{(n)}\ge\tilde{E}_1, \tag{65}$$

$$\liminf_{n\to\infty}\tilde{E}_2^{(n)}\ge\tilde{E}_2. \tag{66}$$

The K-RMOID capacity $C_{K\text{-RMOID}}$ is defined as the maximum achievable R in K-RMOID coding, i.e.,

$$C_{K\text{-RMOID}}\equiv\max\{R\mid(R,E_1,E_2)\text{ is achievable in }K\text{-MOID coding}\}. \tag{67}$$

Obviously, it holds that $C_{K\text{-RMOID}}\le C_{K\text{-MOID}}$.

B. Construction of efficient RMOID codes

For $\boldsymbol{K}=(i_1,i_2,\cdots,i_K)$, we define a code $(\tilde{\varphi},\tilde{\psi}_1,\tilde{\psi}_2,\cdots,\tilde{\psi}_N)$ as follows:

Coding Scheme 2:

$$\tilde{\varphi}(\boldsymbol{K},v)\equiv f(v,h_v(i_1),h_v(i_2),\cdots,h_v(i_K)) \tag{68}$$

$$\tilde{\psi}_i(y^n)\equiv\begin{cases}j, & \text{if } h_{\hat{v}}(i)\ne\beta_l,\ l=1,2,\cdots,j-1\\ & \text{and } h_{\hat{v}}(i)=\beta_j\\ \mathrm{F}, & \text{if } h_{\hat{v}}(i)\ne\beta_l,\ l=1,2,\cdots,K\end{cases}$$
$$\text{for }(\hat{v},\beta_1,\beta_2,\cdots,\beta_M)=g(y^n) \tag{69}$$

The encoder $\tilde{\varphi}$ is the same as the encoder φ of Coding Scheme 1 defined in (27). But the order of $h_v(i_j)$ in f of $\tilde{\varphi}$ represents the rank of receivers while the order of $h_v(i_j)$ has no meaning in the case of φ defined in (27).

As shown in (69), each decoder $\tilde{\psi}_i$ first checks whether or not receiver i is rank 1. If so, $\tilde{\psi}_i$ outputs 1. Otherwise $\tilde{\psi}_i$ next checks whether or not receiver i is rank 2. If so, $\tilde{\psi}_i$ outputs 2. Otherwise $\tilde{\psi}_i$ checks whether or not receiver i is rank 3. This procedure repeats until rank becomes K. Finally, if receiver i is not rank K, $\tilde{\psi}_i$ outputs F .

This code $(\tilde{\varphi},\tilde{\psi}_1,\tilde{\psi}_2,\cdots,\tilde{\psi}_N)$ satisfies the following theorem.

Theorem 3: The following triplet is achievable by Coding Scheme 2 for K-RMOID coding:

$$(R,E_1,E_2)=\left(\left(1-\frac{K+3}{K+\ell}\right)r,E(r),\min\left\{\frac{r}{K+\ell},E(r)\right\}\right),\quad 0\le r\le C,\quad \ell=3,4,5,\cdots. \tag{70}$$

Proof: First we consider the case of the noiseless channel. For each rank j, $j=1,2,3,\cdots,K$, $\tilde{\lambda}_1^{(n)}(i_j|\boldsymbol{K})$ can be evaluated as follows:

$$\tilde{\lambda}_1^{(n)}(i_j|\boldsymbol{K})=\Pr\left\{\bigcap_{l=1}^{j}(h_V(i_j)\ne h_V(i_l))\right\}=0, \tag{71}$$

where the last equality holds because $h_V(i_j) = h_V(i_l)$ is satisfied at $l = j$.

Next we derive an upper bound of $\tilde{\lambda}_2^{(n)}(i_j|\boldsymbol{K})$ for receiver i_j with rank j. We have

$$\begin{aligned}\tilde{\lambda}_2^{(n)}(i_j|\boldsymbol{K}) &= \Pr\left\{\bigcup_{l=1}^{j-1}\left(h_V(i_j) = h_V(i_l)\right)\right\} \\ &\le \sum_{l=1}^{j-1}\Pr\left\{h_V(i_j) = h_V(i_l)\right\} \\ &\le \varepsilon(j-1) \le \varepsilon K, \end{aligned} \tag{72}$$

where the second inequality can be proved in the same way as (37).

$\tilde{\lambda}_1^{(n)}(i_j|\boldsymbol{K})$ and the bound of $\tilde{\lambda}_2^{(n)}(i_j|\boldsymbol{K})$ are the same as $\lambda_1^{(n)}(i|\mathcal{K})$ and the bound of $\lambda_2^{(n)}(i|\mathcal{K})$ treated in Section II, respectively. This means that the lower bounds of $\tilde{E}_1^{(n)}$ and $\tilde{E}_2^{(n)}$ are the same as the lower bounds of $E_1^{(n)}$ and $E_2^{(n)}$ derived in Section II, respectively. Hence, if (R, E_1, E_2) is achievable for code $(\varphi, \psi_1, \psi_2, \cdots, \psi_N)$, it is also achievable for code $(\tilde{\varphi}, \tilde{\psi}_1, \tilde{\psi}_2, \cdots, \tilde{\psi}_N)$. Therefore, Theorem 3 holds from Theorem 2.

Q.E.D.

In the same way as Coding Scheme 1, we can show that the coding rate R of Coding Scheme 2 can attain C. On the other hand, it holds that $C_{K\text{-RMOID}} \le C_{K\text{-MOID}} = C$. Hence, we obtain the following corollary.

Corollary 2: The K-RMOID capacity $C_{K\text{-RMOID}}$ is given by

$$C_{K\text{-RMOID}} = C. \tag{73}$$

Remark 6: The same arguments treated in Sections II-D to II-G also hold for K-RMOID code $(\tilde{\varphi}, \tilde{\psi}_1, \tilde{\psi}_2, \cdots, \tilde{\psi}_N)$.

IV. Conclusion

In this paper, we defined the MOID coding and we proposed efficient and explicit MOID coding schemes for non-ranked and ranked cases. We derived the achievable triplet of coding rate and exponents of type I and type II error probabilities, and we proved that both the K-MOID capacity and the K-RMOID capacity are equal to the ordinary channel capacity. Furthermore, we considered the MOID coding with common randomness, noiseless passive feedback, transmission coding, and variable K coding.

Acknowledgment

The authors would like to thank anonymous reviewers for useful comments and Mr. Takuya Ban for useful discussions.

References

[1] R. Ahlswede and G. Dueck, "Identification via channels," *IEEE Transactions on Information Theory*, vol. 35, no. 1, pp. 15–29, Jan. 1989.

[2] R. Ahlswede and G. Dueck, "Identification in the Presence of Feedback – A Discovery of New Capacity Formulation," *IEEE Transactions on Information Theory*, vol. 35, no. 1, pp. 30–36, Jan. 1989.

[3] T. S. Han and S. Verdú, "New result in the theory of identification via channels," *IEEE Transactions on Information Theory*, vol. 38, no. 1, pp. 14–25, Jan. 1992.

[4] S. Verdú and V. K. Wei, "Explicit construction of optimal constant-weight codes for identification via channels," *IEEE Transactions on Information Theory*, vol. 39, no. 1, pp. 30–36, Jan. 1993.

[5] K. Kurosawa and T. Yoshida, "Strongly universal hashing and identification codes via channels," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp.2091–2095, June 1999.

[6] P. Moulin and R. Koetter, "A framework for the design of good watermark identification codes," *SPIE Proceedings 6072*, Security, Steganography, and Watermarking of Multimedia Contents VIII, pp. 60721H-1–60721H-10, Jan. 2006.

[7] R. Ahlswede, "Introduction," General theory of information transfer and combinatorics, LCNS4123, Springer, pp. 1-44, 2006

[8] R. Ahlswede, "General theory of information transfer: Updated," Discrete Applied Mathematics, Elsevier, vol. 156, pp. 1348–1388, 2008.

[9] R. Ahlswede, B. Balkenhol, and C.Kleinewächter, "Identification for sources," General theory of information transfer and combinatorics, LCNS4123, Springer, pp. 51-61, 2006

[10] Y. Steinberg, and N. Merhav, "Identification in the Presence of Side Information with Application to Watermarking," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1410–1422, May 2001.

[11] T.S. Han and M. Hoshi, "Interval Algorithm for Random Number Gerenation," *IEEE Transactions on Information Theory*, vol. 43, no. 2, pp. 599–611, March 1997.

[12] P. Elias, "Universal codewords sets and representations of the integers," *IEEE Transactions on Information Theory*, vol. IT21, no. 2, pp. 194–203, March 1975

[13] H. Yamamoto and M. Ueda, "Identification codes to identify multiple objects," 2014 IEEE International Symposium on Information Theory, pp. 1241–1245, 2014

Hirosuke Yamamoto (S'77–M'80–SM'03–F'11) was born in Wakayama, Japan, in 1952. He received the B.E. degree from Shizuoka University, Shizuoka, Japan, in 1975 and the M.E. and Ph.D. degrees from the University of Tokyo, Tokyo, Japan, in 1977 and 1980, respectively, all in electrical engineering. In 1980, he joined Tokushima University. He was an Associate Professor at Tokushima University from 1983 to 1987, the University of Electro-Communications from 1987 to 1993, and the University of Tokyo from 1993 to 1999. Since 1999, he has been a Professor at the University of Tokyo and is currently with the department of Complexity Science and Engineering at the university. In 1989-1990, he was a Visiting Scholar at the Information Systems Laboratory, Stanford University, Stanford, CA. His research interests are in Shannon theory, data compression algorithms, and information theoretic cryptology.

Dr. Yamamoto served as the Chair of IEEE Information Theory Society Japan Chapter in 2002–2003, the TPC Co-Chair of the ISITA2004, the TPC Chair of the ISITA2008, the president of the SITA (Society of Information Theory and its Applications) in 2008–2009, the president of the ESS (Engineering Sciences Society) of IEICE in 2012–2013, an Associate Editor for Shannon Theory, the IEEE TRANSACTIONS ON INFORMATION THEORY in 2007–2010, Editor-in-Chief for the IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences in 2009–2011. He is a Fellow of the IEICE.

Masashi Ueda was born in Hyogo, Japan in 1988. He received the B.E and M.E degrees in mathematical engineering and mathematical informatics from the University of Tokyo, Japan, in 2012 and 2014, respectively. In 2014, he joined NS Solutions Corporation. He studied the subject of this paper for the M.E. degree.