Identification Codes to Identify Multiple Objects

Hirosuke Yamamoto
Department of Complexity Science & Engineering
The University of Tokyo
Kashiwa-shi, Chiba, Japan
Email: hirosuke@ieee.org

Masashi Ueda
Department of Mathematical Informatics
The University of Tokyo
Bunkyo-Ku, Tokyo, Japan
Email: uyeda@it.k.u-tokyo.ac.jp

Abstract—In the case of ordinary identification coding, a code is devised to identify one object among \(N\) objects. But, in this paper, we consider an identification coding problem to identify \(M\) objects at once among \(N\) objects in the both cases that \(M\) objects are or are not ranked. By combining Kurosawa-Yoshida scheme with Moulin-Koetter scheme, an efficient identification code is proposed, which can attain high coding rate and error exponents compared with the case that an ordinary identification code is used \(M\) times.

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 or not he/she is the winner, 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 that the decoding error probability of each receiver can be arbitrarily small if \(R < C\), where \(C\) is the channel capacity, \(R\) is the coding rate of the ID code defined by \(R = \log(\log N)/n\), and the code length \(n\) [1][2].

Verdú and Wei [3] 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 ID code for the noiseless channel by using a constant weight matrix based on Reed-Solomon codes. Furthermore, Kurosawa and Yoshida [4] showed that a more efficient ID code for the noiseless channel can be constructed by using \(\varepsilon\)-almost strongly universal classes of hash functions, and Moulin and Koetter [5] 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.

In this paper, we consider the case that there are \(M\) winners among \(N\) receivers. In this case, we can send the information of winners by using an ordinary ID code \(M\) times. But, the coding rate is decreased to \(R/M\). If we construct an ordinary ID code for \(N = \binom{N}{M}\) and each receiver has \(\binom{N-1}{M-1}\) indices, we can send the information with the same coding rate \(R\) as the case of \(M = 1\). However, the Type II decoding error probability becomes very large because the probability is \(\binom{M-1}{N-1}\) times as large as the case of \(M = 1\).

In this paper, we show that an efficient ID code can be constructed for the case of \(M\) winners by combining Kurosawa-Yoshida coding scheme and Moulin-Koetter coding scheme. We derive the achievable region of coding rate and the exponents of Type I and II decoding error probabilities.

In Sections 2 and 3, we treat the cases that \(M\) winners are not ranked and are ranked, respectively.

II. ID CODE TO IDENTIFY MULTIPLE OBJECTS WITHOUT RANKINGS

A. Definition of M-ID code

Let \(u_i \in U \equiv \{T, F\}\) be binary information to be sent to each receiver \(i \in I \equiv \{1, 2, \ldots, N\}\), and we define \(z\) as

\[
z \equiv \{i : u_i = T, i \in I\},
\]

which is the set of winners, i.e., the receivers that will be sent \(u_i = T\). We assume for simplicity that \(M \equiv |z| \geq 1\) is fixed, where \(|\cdot|\) represents the cardinality of a set. (See Remark 6 for the case that \(M\) is not fixed.) Let \(Z \equiv \{z\}\) be the set of all \(z\). Then we note that \(|Z|\) is given by \(\binom{N}{M}\), and the ordinary ID coding corresponds to the case of \(M = 1\).

For channel input and output alphabets \(X\) and \(Y\), we define the encoder to identify \(M\) receivers as follows.

\[
\varphi : Z \times V \rightarrow X^n,
\]

where \(n\) is the code length. The codeword \(x^n\) is generated by \(x^n = \varphi(z, v)\) from ID information \(z\) and a random number \(v \in V = \{1, 2, \ldots, |V|\}\). This means that the encoder \(\varphi\) is a stochastic encoder for a given \(z\). The decoder \(\psi_i\) of receiver \(i\), which outputs \(T\) or \(F\), is defined as follows.

\[
\psi_i : Y^n \rightarrow U_i.
\]

We call a code \((\varphi, \psi_1, \psi_2, \ldots, \psi_N)\) an \(M\)-ID code.

The coding rate \(R_M^{(n)}\) of an \(M\)-ID code is defined by

\[
R_M^{(n)} \equiv \frac{1}{n} \log \log N.
\]

Next we consider the decoding error probabilities of an \(M\)-ID code. The type I decoding error probability and its exponent are defined as follows.

\[
\lambda_1^{(n)}(i|z) \equiv \Pr\{\psi_i(\varphi(z, V)) = F\} \quad \text{for } i \in z,
\]

\[
\Lambda_1^{(n)} \equiv \max_{z \in Z} \max_{i \in z} \lambda_1^{(n)}(i|z),
\]

\[
E_1^{(n)} \equiv -\frac{1}{n} \log \Lambda_1^{(n)}.
\]

The base of logarithm is always 2.
where $\lambda_1^n(i|z)$ represents the decoding error probability of receiver $i \in z$, and $\lambda_1^n$ is the worst case of $\lambda_1^n(i|z)$. $E_1^n$ is the exponent of $\lambda_1^n$.

Similarly, the type II decoding error probability is defined by
\[
\lambda_2^n(i|z) = \Pr\{\psi_i(\varphi(z, V)) = T\} \text{ for } i \notin z,
\]
\[
\lambda_2^n = \max_{z \in \mathcal{Z}} \max_{i \notin z} \lambda_2^n(i|z),
\]
\[
E_2^n = -\frac{1}{n} \log \lambda_2^n,
\]
where $\lambda_2^n(i|z)$ is the decoding error probability of receiver $i \notin z$, $\lambda_2^n$ is the worst case of $\lambda_2^n(i|z)$, 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 following inequalities can be satisfied by the coding scheme.
\[
\liminf_{n \to \infty} R_n^M \geq R
\]
\[
\liminf_{n \to \infty} E_n^M \geq E_1
\]
\[
\liminf_{n \to \infty} E_n^M \geq E_2
\]

In the case of $M = 1$, the following triplet is achievable by Verdú-Wei coding scheme [3] and Kurosawa-Yoshida coding scheme [4].
\[
\left(1 - \frac{3}{7}\right) r, E(r), \min\left\{\frac{r}{7}, E(r)\right\},
\]
\[
0 < r < C, \quad \ell = 3, 4, 5, \cdots,
\]
where $E(r)$ is the reliability function of a discrete memoryless channel, $C$ is the capacity of the channel, and $r$ and $\ell$ are parameters we can select freely. Furthermore, the following triplet is achievable by Verdú-Wei coding scheme [3] and Moulin-Koetter coding scheme [5].
\[
(r, E(r), \min\{(1/2 - \rho)r, E(r)\}),
\]
\[
0 < r < C, \quad 0 \leq \rho \leq 1/2,
\]
where $r$ and $\rho$ are parameters.

B. Code construction and its performance

In the same way as Kurosawa-Yoshida scheme [4], we use $\varepsilon$-almost strongly universal classes of hash functions $\mathcal{H} = \{h_i\}$ to construct an $M$-ID code, that satisfies the following relations for $h_i: A \to B$.
\[
|\{h_i \in \mathcal{H} : h_i(\alpha) = \beta\}| = \frac{\lvert \mathcal{H} \rvert}{\lvert B \rvert}
\]
for all $\alpha \in A, \forall \beta \in B$
\[
|\{h_i \in \mathcal{H} : h_i(\alpha_1) = \beta_1, h_i(\alpha_2) = \beta_2\}| \leq \varepsilon \frac{\lvert \mathcal{H} \rvert}{\lvert B \rvert}
\]
for all $\alpha_1, \alpha_2 \in A, \alpha_1 \neq \alpha_2, \forall \beta_1, \beta_2 \in B$

In order to construct an $M$-ID code, we set $\mathcal{A}$ and $\mathcal{H}$ as $\mathcal{A} = I (\lvert \mathcal{A} \rvert = N)$ and $\lvert \mathcal{H} \rvert = \lvert \mathcal{V} \rvert$, respectively. Let $f$ and $g$ be the encoder and decoder, respectively, of a transmission code (i.e., an ordinary error correcting code). Then, for $z = \{i_1, i_2, \ldots, i_M\}$, we construct $M$-ID code $(\varphi, \psi_1, \psi_2, \ldots, \psi_N)$ as follows.

Coding Scheme 1:
\[
\varphi(z, v) = f(v, h_0(i_1), h_0(i_2), \ldots, h_0(i_M))
\]
\[
\psi_i(y^n) \equiv \begin{cases} T, & \text{if } a \text{ satisfies } h_0(i) = \beta_j \\ F, & \text{otherwise} \end{cases}
\]
where $v$ is the uniform random number over $V$.

Then this $M$-ID code satisfies the following theorem.

Theorem 1: The following triplet is achievable by Coding Scheme 1 for $M$-ID coding.
\[
\left(1 - \frac{M + 3}{M + \ell}\right) r, E(r), \min\left\{\frac{r}{M + \ell}, E(r)\right\},
\]
\[
0 < r < C, \quad \ell = 3, 4, 5, \cdots
\]

Proof First we consider the case that $z$ is sent to receivers via the binary noiseless channel by an $M$-ID code with block length $n_0$.

We use Kurosawa-Yoshida’s $\varepsilon$-strongly universal classes of hash functions given in [4]. Setting $n_0 = q^k$ and $d = q^k - q^\ell + 1$ in [4, Corollary 3.1], we have for $q = 2^m$
\[
|\mathcal{A}| = N = q^{kq^t},
\]
\[
|\mathcal{B}| = GF(q) (|\mathcal{B}| = q),
\]
\[
|\mathcal{V}| = |\mathcal{H}| = q^{k+2},
\]
\[
\varepsilon = \frac{k}{q} + \frac{q^t - 1}{q^k} \leq \frac{1}{q} \left( k + \frac{q^t}{q^{k-1}} \right),
\]
where $t \leq k - 1$ because it must hold that $\varepsilon \to 0$ as $m \to \infty$ (i.e., $q \to \infty$).

Then, from (22), (23), and $q = 2^m$, the binary code length of $(v, h_0(i_1), h_0(i_2), \ldots, h_0(i_M))$ is given by
\[
n_0 = \log |\mathcal{V}| + M \log |\mathcal{B}| = (k + 2 + M)m.
\]

Hence, from (21) and (25), the coding rate of this code satisfies
\[
R_{M}^{(n_0)} = \frac{1}{n_0} \log \log N
\]
\[
= \frac{1}{n_0} \log \left( kq^t \log q \right)
\]
\[
= \frac{1}{n_0} \left( tm + \log k + \log m \right)
\]
\[
= \frac{t}{k + 2 + M} + \frac{1}{n_0} \left( \log k + \log m \right)
\]
\[
= \frac{t}{k + 2 + M} + O \left( \frac{\log n_0}{n_0} \right).
\]
Since the optimal $t$ that maximizes (26) for $1 < t < k - 1$ is $t = k - 1$, we can attain the following coding rate.

$$R_{M}^{(n)} = \frac{k - 1}{k + 2 + M} + O\left(\frac{\log n_{0}}{n_{0}}\right) = 1 - \frac{M + 3}{k + 2 + M} + O\left(\frac{\log n_{0}}{n_{0}}\right) \quad (27)$$

Next we consider the decoding error probabilities. In the case of the noiseless channel, every $\psi_1$ always outputs T if $i \in z$. Hence for any $z \in Z$ and any $i \in z$, $\Lambda^{(n)}_{1}(i|z) = 0$. This means that $\lambda^{(n)}_1 = 0$ and $E^{(n)}_1 = \infty$.

For $z = \{i_1, i_2, \ldots, i_M\}$ and $i \notin z$, $\Lambda^{(n)}_2(i|z)$ is bounded as follows.

$$\Lambda^{(n)}_2(i|z) = \Pr{\left(M \sum_{j=1}^{M} \{h_{V}(i) = h_{V}(i_j)\}\right)} \leq \Pr{\left(M \sum_{j\in B} \{h_{V}(i) = h_{V}(i_j)\}\right)} = M \sum_{\delta \in B} |\{h_{V}(i) = h_{V}(i_j) = \beta\}| \leq \varepsilon M, \quad (28)$$

where the first and second inequalities hold from the union bound and (17), respectively. Since this bound does not depend on $z$ and $i \notin z$, $\Lambda^{(n)}_2$ has the same bound.

$$\Lambda^{(n)}_2 \leq \varepsilon M \quad (29)$$

Next we evaluate $E^{(n)}_2$, the exponent of $\Lambda^{(n)}$. From (10), (24), (25), and (29), $E^{(n)}_2$ has the following bound for $t \leq k - 1$.

$$E^{(n)}_2 \geq \frac{1}{n_{0}} \{\log M + \log \varepsilon\} \geq \frac{1}{n_{0}} \{\log M - \log q + \log \left(k + \frac{q^*}{q^* - 1}\right)\} = \frac{1}{k + 2 + M} - \frac{1}{n_{0}} \{\log M + \log \left(k + \frac{q^*}{q^* - 1}\right)\} = \frac{1}{k + 2 + M} - O\left(\frac{\log k}{n_{0}}\right) \quad (30)$$

Letting $\ell = k + 2$, $\ell = 3, 4, \ldots$, and $n_{0} \to \infty$ in (27) and (30), the following triplet is achievable for the noiseless channel.

$$\left(1 - \frac{M + 3}{M + \ell}, a, \frac{1}{M + \ell}\right), \quad (31)$$

where $a > 0$ is an arbitrarily large constant.

Next consider the case of noisy channels. If we transmit $(v, h_v(i_1), h_v(i_2), \ldots, h_v(i_M))$ via a noisy channel by using the best transmission code $(f, g)$ 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 $E(r)$ is the reliability function of the channel and $C$ is the channel capacity. Hence, the total error probability $\lambda^{(n)}_j$, $j = 1, 2$, is bounded as follows.

$$\lambda^{(n)}_j \leq 2^{-nE^{(n)}_1} + 2^{-nE(r)} \leq 2^{-n \min\{rE^{(n)}_1, E(r)\}} \quad (32)$$

Hence, from (31) and (32), the triple given by (20) is achievable.

Q.E.D.

Remark 1: If we use Verdú-Wei’s ID code or Kurosawa-Yoshida’s ID code $M$ times, the following triplet is achievable from (14).

$$\left(1 - \frac{3}{\ell + 1}, E(r), \frac{r}{\ell M}, \min\left\{\frac{r}{\ell M}, E(r)\right\}\right), \quad 0 \leq r \leq C, \quad \ell = 3, 4, 5, \ldots \quad (33)$$

But, this triplet is much worse than (20) for $M \geq 2$.

Remark 2: In the case of $M = 1$, the following triplet is achievable by Coding Scheme 1 from Theorem 1.

$$\left(1 - \frac{4}{\ell + 1}, E(r), \min\left\{\frac{r}{\ell M}, E(r)\right\}\right), \quad 0 < r < C, \quad \ell = 3, 4, 5, \ldots \quad (34)$$

This triplet is a little worse than (14). But our coding scheme can attain a high performance for $M \geq 2$. Furthermore, our scheme has advantages shown in Remarks 4 and 5 for $M \geq 1$.

Remark 3: It is shown in [2] that an ID code can send a usual transmission message in addition to an ID message at the same time. Actually ID codes given by [3]–[5] can realize such coding. Similarly, our coding scheme can also send a transmission message and an ID message at the same time by using a transmission message $v$, instead of the random number, uniformly distributed over $V$. In this case, the coding rate of the transmission message is given by $R^{(n)}_T \equiv \frac{1}{n} \log |V| = \frac{1}{n_{0}} \frac{1}{n_{0}} \log |V| = \frac{r}{\ell M}, \quad \ell = 3, 4, \ldots, \quad \text{from (23) and (25).}$

Hence, by letting $r \to C$ and $\ell$ sufficiently large, we can attain $\lim_{n \to \infty} R^{(n)}_T = C$ in addition to $\lim_{n \to \infty} R^{(n)}_M = C$ at the same time.

Remark 4: If the encoder and decoders share common randomness, we don’t need to send $v$ in the same way as Moulin-Koetter scheme. In this case, the code length $n^*$ becomes $n^* = Mn/r$ from (25), and the coding rate and the error exponents are multiplied by

$$\frac{n}{n^*} = \frac{\ell + M}{M}, \quad \ell = 3, 4, \ldots \quad (35)$$

compared with (20). This means that by using sufficiently large $\ell$, $R_1$ and $E_1$ can become arbitrarily large and $E_2$ satisfies $E_2 = r/M$ for $0 < r < C$.

Remark 5: It is shown in [6] that if we can use a passive noiseless feedback channel such that the encoder can know the channel output $Y_t$ at each time $t = 1, 2, \ldots, n - 1$.
following coding rate can be achieved.

\[
\max_{x \in X} H(W(\cdot| x)) \quad \text{if the encoder is deterministic.} \quad (36)
\]

\[
\max_{P \in \mathcal{P}(X)} H(P \cdot W) \quad \text{if the encoder is stochastic.} \quad (37)
\]

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

The above coding rates, (36) and (37), can be achieved by our coding scheme as follows. We first send \( x^0 \), where \( x_t, t = 1, 2, \ldots, n \), is the optimal input \( \tilde{x} \) that achieves the maximum of (36) in the deterministic case, or is generated by the optimal input probability distribution \( \hat{P} \) that achieves the maximum of (37). Then the encoder and decoders can obtain random number \( v \) from the corresponding channel output \( y^n \) by making the use of interval algorithm for random number generation [7]. Next the encoder sends \( (h_v(i_1), h_v(i_2), \ldots, h_v(i_M)) \) by a transmission code with code length \( n^* = Mm/r \). In order to achieve a fixed rate of \( v \), we use variable \( \tilde{n}_v \) and we set \( E[\tilde{n}] = \ell m/H(W(\cdot| \tilde{x})) \) or \( E[\tilde{n}] = \ell m/H(P \cdot W) \). Since \( n^*/E[\tilde{n}] \to 0 \) as \( \ell \to \infty \), we attain (36) and (37) for \( R = (\log \log N)/E[\tilde{n}] + n^* \) by using sufficiently large \( \ell \).

Remark 6: In the above, we assumed for simplicity that \( M \) is fixed and given. If the deciders cannot know \( M \), it is necessary to send \( f(M, v, h_v(i_1), h_v(i_2), \ldots, h_v(i_M)) \) instead of (18).

In the case that the maximum value of \( M, M_{\text{max}} \), is given, \( M \) can be represented by \([\log M_{\text{max}}]\) bits, and the additional coding rate is given by \([\log M_{\text{max}}]/n \) which can be ignored for sufficiently large \( n \). In the case that \( M_{\text{max}} \) is not known, \( M \) can be represented by Elias \( \delta \) code [8], the length of which is not larger than \( 1 + \log M + 2 \log(1 + \log M) \) bits. Hence, if \( M \) satisfies that \((\log M)/n \to 0 \) as \( n \to \infty \), we can ignore the additional coding rate of Elias \( \delta \) code. Therefore, Theorem 1 still holds for these cases.

Corollary 1: The \( M \)-ID code constructed by Coding Scheme I can attain

\[
\lim_{n \to \infty} R^{(n)}_M = C, \quad (38)
\]

\[
\lim_{n \to \infty} \lambda_1^{(n)} = 0, \quad (39)
\]

\[
\lim_{n \to \infty} \lambda_2^{(n)} = 0. \quad (40)
\]

Proof: For an arbitrarily given \( \xi > 0 \), we select \( r \) and \( \ell \) that satisfy the following inequalities.

\[
C \left( 1 - \frac{\xi}{2} \right) < r < C \quad (41)
\]

\[
\frac{M + 3}{M + \ell} < \frac{\xi}{2} \quad (42)
\]

Then, for sufficiently large \( n \), coding rate \( R^{(n)}_M \) satisfies \( (1 - M+3)/(M+\ell) \) satisfies

\[
C(1 - \xi) < R^{(n)}_M < C. \quad (43)
\]

From (41), we have \( E(r) > 0 \). Obviously \( \frac{M+3}{M+\ell} > 0 \). Hence (39) and (40) hold because their exponents are positive. Since the above holds for any \( \xi > 0 \), (38) is obtained by setting \( \xi \to 0 \) as \( n \to \infty \).

Q.E.D.

Remark 7: In order to attain (38), \( \ell \) must be sufficiently large and \( r \) must be sufficiently close to \( C \). This means that \( E_1 \to 0 \) and \( E_2 \to 0 \) even though (39) and (40) hold.

III. ID CODE TO IDENTIFY MULTIPLE OBJECTS WITH RANKINGS

A. Definition of \( M \)-ranked ID code

In the previous section, we assumed that selected \( M \) receivers are not ranked. But, in this section, we consider the case that \( M \) receivers are ranked. Let \( z \equiv (i_1, i_2, \ldots, i_M) \), where \( i_j \) is the receiver with rank \( j \). Then, encoder \( \bar{\varphi} \) and decoder \( \psi_i \) for \( M \) ranked receivers can be defined as follows.

\[
\bar{\varphi} : \tilde{Z} \times \mathcal{V} \to \mathcal{X}^n \quad (44)
\]

\[
\psi_i : \mathcal{X}^n \to \{1, 2, \ldots, M, F\}, \quad (45)
\]

where \( \tilde{Z} \) is the set of all \( z \).

Although we can consider many types of errors for this code \( (\bar{\varphi}, \psi_1, \psi_2, \ldots, \psi_N) \), we group the errors into only two types. To simplicity notation, we treat \( F \) as rank \( M + 1 \). Then, the type I (resp. II) error is defined as an error such that a decoded receiver is larger (resp. smaller) than the correct rank of the receiver.

Let \( \bar{\lambda}_1^{(n)} \) and \( \bar{\lambda}_2^{(n)} \) be the worst probability of type I and II errors, respectively. Then, they are defined as follows.

\[
\bar{\lambda}_1^{(n)}(i_j|z) \equiv \Pr\{\bar{\psi}_i(\bar{\varphi}(z, V)) > j\} \quad (46)
\]

\[
\bar{\lambda}_1^{(n)} \equiv \max_{i_j} \bar{\lambda}_1^{(n)}(i_j|z), \quad (47)
\]

\[
\bar{\lambda}_2^{(n)}(i_j|z) \equiv \Pr\{\bar{\psi}_i(\bar{\varphi}(z, V)) < j\}. \quad (48)
\]

\[
\bar{\lambda}_2^{(n)} \equiv \max_{i_j} \bar{\lambda}_2^{(n)}(i_j|z). \quad (49)
\]

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

\[
\bar{E}_1^{(n)} \equiv -\frac{1}{n} \log \bar{\lambda}_1^{(n)}, \quad (50)
\]

\[
\bar{E}_2^{(n)} \equiv -\frac{1}{n} \log \bar{\lambda}_2^{(n)}. \quad (51)
\]

Remark 8: From the definition of decoder \( \bar{\psi}_i \) given by (45), we note that \( \bar{\lambda}_1^{(n)}(i_{M+1}|z) = \bar{\lambda}_2^{(n)}(i_1|z) = 0 \). This means that we can exclude receivers with \( j = M + 1 \) (i.e. \( F \)) and the receiver with \( j = 1 \) in the maximization \( \max \) of (47) and (49), 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 \( M = 1 \). Furthermore, if all ranks \( j, 1 \leq j \leq M \), are treated as the same rank, (48) and (49) coincide with (6) and (9), respectively. Therefore, the definition of type I and II errors given by (46)-(49) are reasonable.
A triplet \((R, \bar{E}_1, \bar{E}_2)\) is said to be achievable by a coding scheme if the following inequalities can be satisfied by the coding scheme:

\[
\liminf_{n \to \infty} R_i^{(n)} \geq R, \\
\liminf_{n \to \infty} \bar{E}_1^{(n)} \geq \bar{E}_1, \\
\liminf_{n \to \infty} \bar{E}_2^{(n)} \geq \bar{E}_2
\]

(52) (53) (54)

B. Code construction and its performance

For each rank \(l\), \(i\), we define a code \((\hat{v}, \hat{v}_1, \hat{v}_2, \ldots, \hat{v}_N)\) as follows.

**Coding Scheme 2:**

\[
\hat{v}(z, v) \equiv f(v, h_v(i_1), h_v(i_2), \ldots, h_v(i_M))
\]

(55)

\[
\hat{v}_i(y^n) \equiv \begin{cases} j, & \text{if } h_v(i) \neq \beta_l, l = 1, 2, \ldots, j - 1 \\
& \text{and } h_v(i) = \beta_j \\
F, & \text{if } h_v(i) \neq \beta_l, l = 1, 2, \ldots, M \\
& \text{for } (\hat{v}, \beta_1, \beta_2, \ldots, \beta_M) = g(y^n)
\end{cases}
\]

(56)

The encoder \(\hat{v}\) is the same as the encoder \(v\) defined in (18) in Coding Scheme 1. But the order of \(h_v(i)\) in \(f\) of \(\hat{v}\) represents the rank of receiver while the order of \(h_v(i)\) has no meaning in the case of \(v\). As defined in (56), each decoder \(\hat{v}_i\) first checks whether or not receiver \(i\) is rank 1. If so, \(\hat{v}_i\) outputs 1. Otherwise \(\hat{v}_i\) checks whether or not receiver \(i\) is rank 2. If so, \(\hat{v}_i\) outputs 2. Otherwise \(\hat{v}_i\) checks whether or not receiver \(i\) is rank 3. This procedure repeats to rank \(M\). Finally \(\hat{v}_i\) outputs \(F\) if receiver \(i\) is not rank \(M\).

This code \((\hat{v}, \hat{v}_1, \hat{v}_2, \ldots, \hat{v}_N)\) satisfies the following theorem.

**Theorem 2:** The following triplet is achievable by Coding Scheme 2 for \(M\)-ranked ID coding.

\[
\frac{1 - \frac{M + 3}{M + \ell}}{\min \left\{ \frac{r}{M + \ell}, E(r) \right\}}, \quad 0 \leq r \leq C, \quad \ell = 3, 4, 5, \ldots
\]

(57)

**Proof** First we consider the case of the noiseless channel. For each rank \(j\), \(j = 1, 2, 3, \ldots, M\), \(\bar{\lambda}_1^{(n)}(i_j|z)\) can be evaluated as follows.

\[
\bar{\lambda}_1^{(n)}(i_j|z) = \Pr \left\{ \bigcap_{j=1}^{j-1} (h_v(i_j) \neq h_v(i)) \right\}
\]

(58)

where the last equality holds because \(h_v(i_j) = h_v(i)\) is satisfied at \(l = j\).

Next we derive an upper bound of \(\bar{\lambda}_2^{(n)}(i_j|z)\) for receiver \(i_j\) with rank \(j\).

\[
\bar{\lambda}_2^{(n)}(i_j|z) = \Pr \left\{ \bigcup_{j=1}^{j-1} (h_v(i_j) = h_v(i)) \right\}
\]

(59)

where the second inequality can be proved similarly to (28). \(\bar{\lambda}_2^{(n)}(i_j|z)\) and the bound of \(\bar{\lambda}_2^{(n)}(i_j|z)\) are the same as \(\lambda_1^{(n)}(i_j|z)\) and the bound of \(\lambda_2^{(n)}(i_j|z)\) treated in Section II, respectively. This means that the lower bounds of \(\bar{E}_1^{(n)}\) and \(\bar{E}_2^{(n)}\) are the same as the lower bounds of \(E_1^{(n)}\) and \(E_2^{(n)}\) derived in Section II, respectively. Hence, the triplet of rate and error exponents for code \((\hat{v}, \hat{v}_1, \hat{v}_2, \ldots, \hat{v}_N)\) is achievable if it is achievable for code \((\hat{v}, \hat{v}_1, \hat{v}_2, \ldots, \hat{v}_N)\). Therefore, Theorem 2 holds from Theorem 1.

Q.E.D.

**Corollary 2:** The \(M\)-ranked ID code constructed by Coding Scheme 2 can attain

\[
\lim_{n \to \infty} R_i^{(n)} = C, \\
\lim_{n \to \infty} \bar{\lambda}_1^{(n)} = 0, \\
\lim_{n \to \infty} \bar{\lambda}_2^{(n)} = 0
\]

(60) (61) (62)

**Proof** Corollary 2 can be proved in the same way as Corollary 1.

Q.E.D.

**Remark 9:** Remarks 1–7 also hold for \(M\)-ranked ID code \((\hat{v}, \hat{v}_1, \hat{v}_2, \ldots, \hat{v}_N)\).

ACKNOWLEDGMENT

This work was supported in part by JSPS KAKENHI Grant Numbers 25289111 and 26630169.

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] T. S. Han and S. Verdù, “New result in the theory of identification via channels,” IEEE Transactions on Information Theory, vol. 38, no. 1, pp. 14–25, Jan. 1992.
[3] S. Verdù 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.
[4] K. Kurosawa and T. Yoshida, “Strongly universal hashing and identification codes,” IEEE Transactions on Information Theory, vol. 45, no. 6, pp. 2091–2095, June 1999.
[5] 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.
[6] 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.
[7] T.S. Han and M. Hoshi, “Interval Algorithm for Random Number Generation,” IEEE Transactions on Information Theory, vol. 43, no. 2, pp. 599–611, March 1997.
[8] P. Elias, “Universal codewords sets and representations of the integers,” IEEE Transactions on Information Theory, vol. IT21, no. 2, pp. 194–203, March 1975.