様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　５　月　２４　日現在

機関番号：　１２６０１
研究種目：　挑戦的萌芽研究
研究期間：　2014～2016
課題番号：　２６６３０１６９

研究課題名（和文）複数人を一度に識別可能な効率のよい同定符号の構成法

研究課題名（英文）Construction schemes of efficient identification codes to identify multiple objects at once

研究代表者

山本　博資（Yamamoto, Hirosuke）

東京大学・大学院新領域創成科学研究科・教授

研究者番号：３０１３６２１２

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：従来の同定符号(ID Code)は，N個の中から選ばれた一つの対象を同定するための符号であるが，本研究では，N個の対象から一度にK個の対象を，順序無しで同定するK多重同定(K-MOID)符号および順序付きで同定するK多重順序付き同定(K-RMOID)符号を考え，その具体的な構成方法を与えるとともに，雑音のある通信路に対するそれらの符号の符号化レートの上限が通常の通信路容量や通常のID容量と一致することを，理論的に明らかにした．さらに，無雑音通信路の場合に対して，逆問題を考え，K-MOID(K-RMOID)符号の符号化レートおよび復号誤り指数が満たさなければならない条件式を与えた．

研究成果の概要（英文）：In the ordinal ID (Identification) coding, one object is identified among N object. But, in this research, we treated the K-MOID (K-multiple-object identification) coding and K-RMOID (K-ranked-multiple-object identification)) coding such that K objects and K ranked objects, respectively, are identified at once among N objects. We proposed practical code construction schemes for K-MOID and K-RMOID coding, and we showed by using these codes that the K-MOID and R-MOID capacities for a noisy channel are equal to the ordinary channel capacity of the channel. Furthermore, we also studied the converse problem of K-MOID and K-RMOID coding, and we derived some conditions that any K-MOID and R-MOID code must satisfy for the coding rate and the decoding error exponents of the first and second kinds of errors.

研究分野：　情報理論

キーワード：　同定符号　MOID符号　RMOID符号　通信路符号化　シャノン理論

1　研究開始当初の背景

同定符号 (Identification Code)[1] は，N 人の受信者の中から一人が選ばれ，N 人の各受信者ごとに，その人が選ばれたか否かという 2 値情報を任意に小さい誤り確率で知らせるための符号化法である．例えば，一人が当選する宝くじの当選結果を N 人に伝える場合などに使用できる．しかし，当選者が K 人いる場合や，K 人が，1 等, 2 等, $\cdots$, K 等というように順位がついている場合に，通常の同定符号を用いて当選結果を伝送すると，その同定符号を K 回繰り返して使用しなくてはならず，効率が悪い．

そこで，本研究では，K 人を一度に同定するための同定符号 (K-Multimple-Object Identification Code, K-MOID 符号) および K 人を順序付きで一度に同定するための同定符号 (K-Ranked-Multiple-Object Identification Code, K-RMOID 符号) を新たに定義し，その具体的な符号の構成法およびそれらの符号に対して成り立つ符号化定理に関する研究を行ったものである．

2　研究の目的

本研究では，K-MOID 符号化および K-RMOID 符号化問題に対する順定理と逆定理を取り扱う．順定理では，各符号の効率のよい符号構成法を提案し，それらの符号を雑音のある通信路に用いた場合に達成可能な符号化レートの上限である K-MOID 符号化容量および K-RMOID 符号化容量を導出する．また，達成可能な符号化レートと復号誤り指数の内界を求める．

K-MOID 符号化および K-RMOID 符号化問題に対する逆定理は，非常に難しい問題になるため，通信路として無雑音通信路を考え，その場合に対する符号化レートと復号誤り指数の外界を導出する．

3　研究の方法

本研究は，(a)K-MOID 符号および K-RMOID 符号の概念の提案，(b) 具体的な K-MOID , K-RMOID 符号の構成法の提案, (c) それらの符号で達成可能な符号化レート，誤り指数，同定符号化容量の導出, (d) 無雑音通信路に対する逆定理の導出などからなる．本研究は，理論的な研究であるため，得られた成果を国際シンポジウム等で発表すると共に，他の研究者と議論を行い，それらを通じて得られた知見に基づき理論の改良を行った．

なお，(a)–(c) の研究に関しては 2014 年 3 月まで当研究室の大学院生であった上田真士氏，(d) の研究に関してはロシア科学アカデミー通信問題研究所の Marat V. Burnashev 博士の協力の下に行った．

4　研究成果

(1) K-MOID 符号化問題の定式化 [4]

$\mathcal{N} \equiv \{1, 2, \cdots, N\}$ を受信者の集合とし，$\mathcal{K}(\subset \mathcal{N})$ を送信者側で選ばれた当選者の集合とする．送信者は，各受信者に 2 値情報 $u_i \in \mathcal{U} \equiv \{\mathrm{T}, \mathrm{F}\}$ を一度に送信する．ここで，$i \in \mathcal{K}$ のとき $u_i = \mathrm{T}$，$i \notin \mathcal{K}$ のとき $u_i = \mathrm{F}$ とする．言い換えると，$\mathcal{K}$ は次式で表現できる．

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

簡単のため，$K \equiv |\mathcal{K}| \geq 1$ は固定されているものとし，$\mathcal{Z} \equiv \{\mathcal{K}\}$ を可能な $\mathcal{K}$ の全ての集合とする．このとき，$\mathcal{Z}$ のサイズ $|\mathcal{Z}|$ は $|\mathcal{Z}| = \binom{N}{K}$ で与えられる．$K = 1$ の場合が，通常の同定符号に相当する．

通信路は，入力アルファベット $\mathcal{X}$ と出力アルファベット $\mathcal{Y}$ を持つ離散無記憶通信路 (DMC) とする．簡単のため，以下では通信路入力は 2 値とする．つまり，$|\mathcal{X}| = 2$ とする．さらに，MOID 符号の符号器 φ は，$\mathcal{V} = \{1, 2, \cdots, |\mathcal{V}|\}$ 上の値をとる乱数 v を使用できるものとする．このとき，符号器 φ は次のように定義される．

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

ここで，n は符号長であり，MOID 情報 $\mathcal{K} \in \mathcal{Z}$ から，符号語 x^n が $x^n = \varphi(\mathcal{K}, v)$ により生成される．また，受信者 i の復号器は，次のように定義される．

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

$K = |\mathcal{K}|$ に対する MOID 符号 $(\varphi, \psi_1, \psi_2, \cdots, \psi_N)$ を，K-MOID 符号と呼ぶ．

K-MOID 符号の符号化レート $R_K^{(n)}$ を次式で定義する (対数の底は常に 2 とする)．

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

次に，K-MOID 符号の第 1 種復号誤り確率と誤り指数を次のように定義する．

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

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

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

ここで，$\lambda_1^{(n)}(i|\mathcal{K})$ は $i \in \mathcal{K}$ である受信者の復号誤り確率であり，$\lambda_1^{(n)}$ は $\lambda_1^{(n)}(i|\mathcal{K})$ の最悪値，$E_1^{(n)}$ は $\lambda_1^{(n)}$ の指数である．

同様に，第２種復号誤り確率と誤り指数を次のように定義する．

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

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

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

ある MOID 符号化方式が式 (11)–(13) を満たすとき，その符号化方式において (R,E_1,E_2) は「達成可能 (achievable)」という．

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

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

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

K-MOID 容量 $C_{K\text{-MOID}}$ は，K-MOID 符号化における達成可能な符号化レート R の最大値として次のように定義する．

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

$K=1$ のとき，K-MOID 符号は通常の同定符号と一致し，$R_K^{(n)}$, $E_1^{(n)}$ と $E_2^{(n)}$, 容量 $C_{K\text{-MOID}}$ は，通常の同定符号の符号化レート，復号誤り指数，同定容量と一致する．

(2) K-RMOID 符号化問題の定式化 [4]

K-RMOID 符号化では，K 人の受信者に $1,2,\cdots,K$ の順位がつけられる．$\boldsymbol{K}\equiv(i_1,i_2,\cdots,i_K)$ とし，i_j が順位 j の受信者とする．また，簡単のため，K 人に入っていない受信者の順位を $K+1$ とする．このとき，符号器 $\tilde{\varphi}$ と復号器 $\tilde{\psi}_i$ を次のように定義する．

$$\tilde{\varphi} : \tilde{\mathcal{Z}}\times\mathcal{V}\to\mathcal{X}^n \tag{15}$$

$$\tilde{\psi}_i : \mathcal{Y}^n \to \{1,2,\cdots,K,K+1\}, \tag{16}$$

ここで，$\tilde{\mathcal{Z}}=\{\boldsymbol{K}\}$ は，可能な $\boldsymbol{K}$ の全ての集合である．この符号を K-RMOID (ranked-multiple-object identification) 符号という．

K-RMOID 符号に対して，様々な種類の誤りを考えることができるが，ここでは，全ての誤りを 2 種類の誤りに分類し，本当の順位より低い順位に誤る誤りを第 1 種の誤り，本当の順位のより高い順位に誤る誤りを第 2 種の誤りとする．また，第 1 種誤りと第 2 種誤りの最悪値を，それぞれ $\tilde{\lambda}_1^{(n)}$ と $\tilde{\lambda}_2^{(n)}$ とする．つまり，下記のように定義する．

$$\tilde{\lambda}_1^{(n)}(i_j|\boldsymbol{K}) \equiv \Pr\{\tilde{\psi}_{i_j}(\tilde{\varphi}(\boldsymbol{K},V))>j\} \tag{17}$$

$$\tilde{\lambda}_1^{(n)} \equiv \max_{\boldsymbol{K}\in\tilde{\mathcal{Z}}}\max_{i_j}\tilde{\lambda}_1^{(n)}(i_j|\boldsymbol{K}), \tag{18}$$

$$\tilde{\lambda}_2^{(n)}(i_j|\boldsymbol{K}) \equiv \Pr\{\tilde{\psi}_{i_j}(\tilde{\varphi}(\boldsymbol{K},V))<j\}, \tag{19}$$

$$\tilde{\lambda}_2^{(n)} \equiv \max_{\boldsymbol{K}\in\tilde{\mathcal{Z}}}\max_{i_j}\tilde{\lambda}_2^{(n)}(i_j|\boldsymbol{K}). \tag{20}$$

さらに，$\tilde{\lambda}_1^{(n)}$ と $\tilde{\lambda}_2^{(n)}$ の誤り指数を次式で定義する．

$$\tilde{E}_1^{(n)} \equiv -\frac{1}{n}\log\tilde{\lambda}_1^{(n)}, \tag{21}$$

$$\tilde{E}_2^{(n)} \equiv -\frac{1}{n}\log\tilde{\lambda}_2^{(n)}. \tag{22}$$

RMOID 符号化方式が式 (23)–(25) を満たすとき，その符号化方式において (R,E_1,E_2) は「達成可能 (achievable)」という．

$$\liminf_{n\to\infty} R_M^{(n)} \geq R, \tag{23}$$

$$\liminf_{n\to\infty} \tilde{E}_1^{(n)} \geq \tilde{E}_1, \tag{24}$$

$$\liminf_{n\to\infty} \tilde{E}_2^{(n)} \geq \tilde{E}_2. \tag{25}$$

K-RMOID 容量 $C_{K\text{-RMOID}}$ は，達成可能な R の最大値として次のように定義される．

$$C_{K\text{-RMOID}} \equiv \max\{R \mid (R,E_1,E_2) \text{ is achievable in } K\text{-RMOID coding}\}. \tag{26}$$

(3) K-MOID 符号および K-RMOID 符号の構成法 [4]

次に，MOID 符号と RMOID 符号に関して，本研究で提案した符号構成法を説明する．

MOID 符号を構成するために，式 (27),(28) の条件を満たすハッシュ関数「$h_l:\mathcal{A}\to\mathcal{B}$」の ε-ASU クラス $\mathcal{H}=\{h_l\}$ を用いる．

$$|\{h_l\in\mathcal{H} : h_l(\alpha)=\beta\}| = \frac{|\mathcal{H}|}{|\mathcal{B}|}, \quad \text{for } \forall\alpha\in\mathcal{A},\forall\beta\in\mathcal{B}, \tag{27}$$

$$|\{h_l\in\mathcal{H} : h_l(\alpha_1)=\beta_1, h_l(\alpha_2)=\beta_2\}| \leq \varepsilon\frac{|\mathcal{H}|}{|\mathcal{B}|}, \quad \text{for } \forall\alpha_1,\alpha_2\in\mathcal{A},\alpha_1\neq\alpha_2,\forall\beta_1,\beta_2\in\mathcal{B}\ . \tag{28}$$

Kurosawa-Yoshida[3] は，ハッシュ関数の ε-ASU クラスの構成法に関して次の補助定理を示している．

補助定理 1 ([3, Corollary 3.1]) 符号長 n_0，最小ハミング距離 d を持つ $\mathrm{GF}(q^k)$ 上の誤り訂正符号を用いて，下記の条件を満たすハッシュ関数の ε-ASU クラス $\mathcal{H}$ を構成できる．

$$|\mathcal{A}| = M, \tag{29}$$

$$|\mathcal{B}| = q, \tag{30}$$

$$|\mathcal{H}| = n_0q^2, \tag{31}$$

$$\varepsilon = \frac{k}{q}+1-\frac{d}{n_0}. \tag{32}$$

K-MOID 符号を構成するために，$\mathcal{A}$ および $\mathcal{H}$ をそれぞれ $\mathcal{A}=\mathcal{N}(|\mathcal{A}|=N)$ および $|\mathcal{H}|=|\mathcal{V}|$ とする．また，

$f : \mathcal{V} \times \beta^K \to \mathcal{X}^n$ と $g : \mathcal{Y}^n \to \mathcal{V} \times \beta^K$ を，雑音を有する通信路 W に対する伝送符号の符号器と復号器とする．このとき，K-MOID 符号 $(\varphi, \psi_1, \psi_2, \cdots, \psi_N)$ を以下のように構成する．

符号化方式 1

符号器 φ :

$$\text{For } \mathcal{K} = \{i_1, i_2, \cdots, i_K\} \subset \mathcal{N},$$
$$\varphi(\mathcal{K}, v) \equiv f(v, h_v(i_1), h_v(i_2), \cdots, h_v(i_K)). \tag{33}$$

復号器 ψ_i:

$$\psi_i(y^n) \equiv \begin{cases} \mathrm{T}, & \text{if } h_{\hat{v}}(i) = \beta_j \text{ holds} \\ & \quad \text{for some } j,\ 1 \le j \le K \\ \mathrm{F}, & \text{otherwise} \end{cases}$$
$$\text{for } (\hat{v}, \beta_1, \beta_2, \cdots, \beta_K) = g(y^n), \tag{34}$$

ここで，v は，$\mathcal{V}$ 上の一様乱数である．

さらに，K-RMOID 符号を次のように構成する．

符号化方式 2

$$\tilde{\varphi}(\boldsymbol{K}, v) \equiv f(v, h_v(i_1), h_v(i_2), \cdots, h_v(i_K)) \tag{35}$$
$$\tilde{\psi}_i(y^n) \equiv \begin{cases} j, & \text{if } h_{\hat{v}}(i) \ne \beta_l,\ l = 1, 2, \cdots, j-1 \\ & \quad \text{and } h_{\hat{v}}(i) = \beta_j \\ K+1, & \text{if } h_{\hat{v}}(i) \ne \beta_l,\ l = 1, 2, \cdots, K \end{cases}$$
$$\text{for } (\hat{v}, \beta_1, \beta_2, \cdots, \beta_M) = g(y^n) \tag{36}$$

(5) 達成可能領域 [4]

上記の K-MOID 符号（符号化方式 1 ）および K-RMOID 符号 (符号化方式 2 ）に対して，次の定理が成り立つ（証明は [4] を参照せよ）．

定理 1　符号化方式 1 と 2 の両方とも，符号化レートおよび誤り指数に関して，次の三つ組を達成できる．

$$(R, E_1, E_2) = \left(\left(1 - \frac{K+3}{K+\ell}\right) r, E(r), \min\left\{ \frac{r}{K+\ell}, E(r) \right\} \right),$$
$$0 < r < C, \quad \ell = 3, 4, 5, \cdots. \tag{37}$$

ここで，$E(r)$ は通常の誤り訂正符号で達成できる誤り指数である．

この定理より，次の系が成り立つ．

系 1　通常の通信路容量 C に対して，K-MOID 容量 $C_{K\text{-MOID}}$ および K-RMOID 容量 $C_{K\text{-MOID}}$ は次式を満たす．

$$C_{K\text{-MOID}} = C_{K\text{-RMOID}} = C. \tag{38}$$

さらに，次のことを示すことができる．

MOID 符号化および RMOID 符号化において，同定情報と同時に通常の伝送情報を符号化レート

$$R_T = r \frac{\ell}{\ell + K}, \quad \ell = 3, 4, \cdots \tag{39}$$

で伝送することができる．また，符号器と復号器で共通乱数 (common randomness) を利用できる場合は，次の三つ組が達成可能である．

$$(R, E_1, E_2) = \left(\frac{\ell - 3}{K} r, E(r), \min\left\{ \frac{r}{K}, E(r) \right\} \right),$$
$$0 < r < C, \quad \ell = 3, 4, 5, \cdots. \tag{40}$$

これらの拡張に関しても，詳細は文献 [4] を参照せよ．

(4) 逆定理 [5]

雑音を有する一般の通信路に対する MOID 符号化の逆定理の証明は非常に難しいため，ここでは通信路が無雑音の場合を考える．また，K の値のレート R_K を次式で定義する．

$$R_K \equiv \lim_{n \to \infty} \frac{1}{n} \log K \tag{41}$$

このとき，任意の K-MOID 符号および K-RMOID 符号の符号化レート R ，第 1 種の復号誤り指数 E_1，第 2 種の復号誤り指数 E_2 は次式を満たさなければならない．

$$\min\{E_1, E_2\} \le \frac{\log |\mathcal{X}| - R - R_K}{2} \tag{42}$$

証明は文献 [5] を参照せよ．

＜引用文献＞

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

[2] H. Yamamoto, M. Ueda, “Multiple object Identification coding,” *IEEE Transactions on Information Theory*, vol. 61, no.8, pp. 4269-4276, Aug. 2015

[3] 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.

[4] H. Yamamoto and M. Udeda, “Multople Object Identification Coding,” *IEEE Transactions on Information Theory*, vol. 61, no. 8, pp. 4269–4276, Aug. 2015

[5] M. Burnashev and H. Yamamoto, “On Optimal Error Exponents in Noiseless Channel Identification,” IEEE Int. Symp. on Inform. Theory, June 25–30, 2017, Aachen, Germany

5　主な発表論文等

[雑誌論文] (計 1 件)

① Hirosuke Yamamoto, Masashi Ueda, “Multiple object Identification coding,” *IEEE Transactions on Information Theory*, vol. 61, no.8, pp. 4269-4276, August 2015 （査読有）

[学会発表]（計２件)

① Hirosuke Yamamoto, Masashi Ueda, “Identification Codes to Identify Multiple Objects,” 2014 IEEE International Symposium on Information Theory, pp. 1241-1245, June 29–July 4, 2014, Honolulu, Hawaii, USA （査読有）

② Marat V. Burnashev, Hirosuke Yamamoto, “On Optimal Error Exponents in Noiseless Channel Identification,” 2017 IEEE International Symposium on Information Theory, June 25–30, 2017, Aachen, Germany（査読有）

[図書]（計 0 件)

[産業財産権]

○ 出願状況（計 0 件)

○ 取得状況（計 0 件)

[その他]

なし

6　研究組織

(1)　研究代表者

山本 博資 (YAMAMOTO, Hirosuke)

東京大学・大学院新領域創成科学研究科・教授

研究者番号：３０１３６２１２

(4)　研究協力者

上田真士（UEDA, Masashi）

BURNASHEV, Marat V.（ロシア科学アカデミー，通信問題研究所）