[4] A. Khinchin, *Mathematical Foundations of Information Theory*. New York, NY, USA: Dover, 1957.
[5] G. Hardy, "Weierstrass's non-differentiable function," *Trans. Amer. Math. Soc.*, vol. 17, no. 3, pp. 301–325, 1916.
[6] S. Furuichi, "On uniqueness theorems for Tsallis entropy and Tsallis relative entropy," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3638–3645, Oct. 2005.

Corrections to "Hash Property and Coding Theorems for Sparse Matrices and Maximum-Likelihood Coding"

Jun Muramatsu, *Senior Member, IEEE*, and
Shigeki Miyake, *Member, IEEE*

There is a flaw in the statement of [2, Lemma 5], which is used in the proof of [2, Ths. 4, 6, and 7]. More precisely, it might be impossible to construct $\mathcal{T}(\boldsymbol{v})$ satisfying the assumption of the lemma when there is $\boldsymbol{u}' \notin \mathcal{T}_{U|V,2\varepsilon}(\boldsymbol{v})$ such that $\mu_{U|V}(\boldsymbol{u}'|\boldsymbol{v}) \leq 2^{-n[H(U|V)-2\varepsilon]}$. To correct the flaw, we have to revise the statement of [2, Lemma 5] and a part of the proof of [2, Ths. 4, 6, and 7].

First, we revise [2, Lemma 5]. For a given $\varepsilon > 0$, let

$$l_{\mathcal{A}} \equiv \frac{n[H(U|V)-\varepsilon]}{\log|\mathcal{U}|}$$

as defined in [2, p. 2147].

Lemma 5: We define a *maximum-likelihood (ML) coding function* g_A with the constraint $\boldsymbol{u} \in \mathcal{C}_A(\boldsymbol{c})$ as

$$\begin{aligned} g_A(\boldsymbol{c}|\boldsymbol{v}) &\equiv \arg\max_{\boldsymbol{u}\in\mathcal{C}_A(\boldsymbol{c})} \mu_{U|V}(\boldsymbol{u}|\boldsymbol{v}) \\ &= \arg\max_{\boldsymbol{u}\in\mathcal{C}_A(\boldsymbol{c})} \mu_{UV}(\boldsymbol{u},\boldsymbol{v}). \end{aligned}$$

Let $\mathcal{F}_{U|V,\varepsilon}(\boldsymbol{v})$ be defined as

$$\mathcal{F}_{U|V,\varepsilon}(\boldsymbol{v}) \equiv \left\{ \boldsymbol{u} : \begin{array}{r} H(\nu_{\boldsymbol{u}|\boldsymbol{v}}|\nu_{\boldsymbol{v}}) > H(U|V) - \frac{3\varepsilon}{2} \\ \frac{1}{n}\log\frac{1}{\mu_{U|V}(\boldsymbol{u}|\boldsymbol{v})} \leq H(U|V) + \frac{\varepsilon}{2} \end{array} \right\}.$$

Then, we have

$$\mathcal{F}_{U|V,\varepsilon}(\boldsymbol{v}) \subset \mathcal{T}_{U|V,2\varepsilon}(\boldsymbol{v}).$$

Assume that a set $\mathcal{T}(\boldsymbol{v}) \subset \mathcal{F}_{U|V,\varepsilon}(\boldsymbol{v})$ satisfies

1) $\mathcal{T}(\boldsymbol{v})$ is not empty, and
2) if $\boldsymbol{u} \in \mathcal{T}(\boldsymbol{v})$ and $\boldsymbol{u}' \in \mathcal{F}_{U|V,\varepsilon}(\boldsymbol{v})$ satisfy

$$\mu_{U|V}(\boldsymbol{u}|\boldsymbol{v}) \leq \mu_{U|V}(\boldsymbol{u}'|\boldsymbol{v}),$$

then $\boldsymbol{u}' \in \mathcal{T}(\boldsymbol{v})$.

In fact, we can construct such a set $\mathcal{T}(\boldsymbol{v})$ by taking elements from $\mathcal{F}_{U|V,\varepsilon}(\boldsymbol{v})$ in descending order of probability. If an ensemble $(\mathcal{A}, p_A)$ of a set of functions $A : \mathcal{U}^n \to \mathcal{U}^{l_{\mathcal{A}}}$ satisfies [2, eq. (H4)], then

$$\begin{aligned} &p_{AC}\left(\{(A,\boldsymbol{c}) : g_A(\boldsymbol{c}|\boldsymbol{v}) \notin \mathcal{T}(\boldsymbol{v})\}\right) \\ &\leq \alpha_A - 1 + \frac{|\mathrm{Im}\mathcal{A}|\,[\beta_A+1]}{|\mathcal{T}(\boldsymbol{v})|} + \frac{2^{-n[\varepsilon/2-\lambda_{\mathcal{UV}}]}|\mathcal{U}|^{l_{\mathcal{A}}}}{|\mathrm{Im}\mathcal{A}|}, \end{aligned}$$

for any $\boldsymbol{v}$ satisfying $\mathcal{T}(\boldsymbol{v}) \neq \emptyset$.

Proof: First, we prove that $\mathcal{F}_{U|V,\varepsilon}(\boldsymbol{v}) \subset \mathcal{T}_{U|V,2\varepsilon}(\boldsymbol{v})$. Assume that $\boldsymbol{u} \in \mathcal{F}_{U|V,\varepsilon}(\boldsymbol{v})$. Then, we have

$$\begin{aligned} H(\nu_{\boldsymbol{u}|\boldsymbol{v}}|\nu_{\boldsymbol{v}}) &> H(U|V) - \frac{3\varepsilon}{2} \\ \frac{1}{n}\log\frac{1}{\mu_{U|V}(\boldsymbol{u}|\boldsymbol{v})} &\leq H(U|V) + \frac{\varepsilon}{2}. \end{aligned}$$

From [2, Lemma 21], we have

$$\begin{aligned} D(\nu_{\boldsymbol{u}|\boldsymbol{v}}\|\mu_{U|V}|\nu_{\boldsymbol{v}}) &= \frac{1}{n}\log\frac{1}{\mu_{U|V}(\boldsymbol{u}|\boldsymbol{v})} - H(\nu_{\boldsymbol{u}|\boldsymbol{v}}|\nu_{\boldsymbol{v}}) \\ &< H(U|V) + \frac{\varepsilon}{2} - \left[H(U|V) - \frac{3\varepsilon}{2}\right] \\ &\leq 2\varepsilon. \end{aligned} \tag{1}$$

This implies that $\boldsymbol{u} \in \mathcal{T}_{U|V,2\varepsilon}(\boldsymbol{v})$. Therefore, we have the fact that $\mathcal{F}_{U|V,\varepsilon}(\boldsymbol{v}) \subset \mathcal{T}_{U|V,2\varepsilon}(\boldsymbol{v})$.

Next, we prove that $g_A(\boldsymbol{c}|\boldsymbol{v}) \notin \mathcal{T}(\boldsymbol{v})$ implies that $\mathcal{T}(\boldsymbol{v}) \cap \mathcal{C}_A(\boldsymbol{c}) = \emptyset$ or $\mathcal{G}(\boldsymbol{v}) \cap \mathcal{C}_A(\boldsymbol{c}) \neq \emptyset$, where $\mathcal{G}(\boldsymbol{v})$ is defined as

$$\mathcal{G}(\boldsymbol{v}) \equiv \left\{\boldsymbol{u} : H(\nu_{\boldsymbol{u}|\boldsymbol{v}}|\nu_{\boldsymbol{v}}) \leq H(U|V) - \frac{3\varepsilon}{2}\right\}.$$

If $\mathcal{T}(\boldsymbol{v}) \cap \mathcal{C}_A(\boldsymbol{c}) \neq \emptyset$, then there is a $\boldsymbol{u} \in \mathcal{T}(\boldsymbol{v}) \cap \mathcal{C}_A(\boldsymbol{c})$ such that $g_A(\boldsymbol{c}|\boldsymbol{v})$ satisfies

$$\mu_{U|V}(g_A(\boldsymbol{c}|\boldsymbol{v})|\boldsymbol{v}) \geq \mu_{U|V}(\boldsymbol{u}|\boldsymbol{v}).$$

We have $g_A(\boldsymbol{c}|\boldsymbol{v}) \in \mathcal{T}(\boldsymbol{v})$ or $g_A(\boldsymbol{c}|\boldsymbol{v}) \notin \mathcal{F}_{U|V,\varepsilon}(\boldsymbol{v})$ from the second assumption of $\mathcal{T}(\boldsymbol{v})$. On the other hand, we have

$$\begin{aligned} \frac{1}{n}\log\frac{1}{\mu_{U|V}(g_A(\boldsymbol{c}|\boldsymbol{v})|\boldsymbol{v})} &\leq \frac{1}{n}\log\frac{1}{\mu_{U|V}(\boldsymbol{u}|\boldsymbol{v})} \\ &\leq H(U|V) + \frac{\varepsilon}{2}, \end{aligned} \tag{2}$$

where the second inequality comes from the fact that $\boldsymbol{u} \in \mathcal{T}(\boldsymbol{v}) \subset \mathcal{F}_{U|V,\varepsilon}(\boldsymbol{v})$. Then, we have the fact that $g_A(\boldsymbol{c}|\boldsymbol{v}) \notin \mathcal{F}_{U|V,\varepsilon}(\boldsymbol{v})$ implies

$$H(g_A(\boldsymbol{c}|\boldsymbol{v})|\boldsymbol{v}) \leq H(U|V) - \frac{3\varepsilon}{2},$$

which is equivalent to $g_A(\boldsymbol{c}|\boldsymbol{v}) \in \mathcal{G}(\boldsymbol{v})$. Since $g_A(\boldsymbol{c}|\boldsymbol{v}) \in \mathcal{C}_A(\boldsymbol{c})$, we have the fact that $g_A(\boldsymbol{c}|\boldsymbol{v}) \in \mathcal{G}(\boldsymbol{v})$ implies $\mathcal{G}(\boldsymbol{v}) \cap \mathcal{C}_A(\boldsymbol{c}) \neq \emptyset$. Then, we have the fact that $\mathcal{T}(\boldsymbol{v}) \cap \mathcal{C}_A(\boldsymbol{c}) \neq \emptyset$ implies $g_A(\boldsymbol{c}|\boldsymbol{v}) \in \mathcal{T}(\boldsymbol{v})$ or $\mathcal{G}(\boldsymbol{v}) \cap \mathcal{C}_A(\boldsymbol{c}) \neq \emptyset$, which is equivalent to the fact that $g_A(\boldsymbol{c}|\boldsymbol{v}) \notin \mathcal{T}(\boldsymbol{v})$ implies $\mathcal{T}(\boldsymbol{v}) \cap \mathcal{C}_A(\boldsymbol{c}) = \emptyset$ or $\mathcal{G}(\boldsymbol{v}) \cap \mathcal{C}_A(\boldsymbol{c}) \neq \emptyset$.

For a conditional type $\nu_{\cdot|\boldsymbol{v}}$ for given $\boldsymbol{v}$, let $\mathcal{T}_{\nu_{\cdot|\boldsymbol{v}}}(\boldsymbol{v})$ a set of typical sequences defined as

$$\mathcal{T}_{\nu_{\cdot|\boldsymbol{v}}}(\boldsymbol{v}) \equiv \{\boldsymbol{u} : \nu_{\boldsymbol{u}|\boldsymbol{v}} = \nu_{\cdot|\boldsymbol{v}}\}.$$

Manuscript received June 04, 2013; accepted June 05, 2013. Date of publication June 12, 2013; date of current version September 11, 2013.
J. Muramatsu is with the NTT Communication Science Laboratories, NTT Corporation, Kyoto 619-0237, Japan (e-mail: muramatsu.jun@lab.ntt.co.jp).
S. Miyake is with the NTT Network Innovation Laboratories, NTT Corporation, Kanagawa 239-0847, Japan (e-mail: miyake.shigeki@lab.ntt.co.jp).
Communicated by O. Milenkovic, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2013.2268157

Similarly to the proof of [3, Lemma 6], we have

$$\begin{aligned}|\mathcal{G}(\boldsymbol{v})| &= \sum_{\nu_{\cdot|\boldsymbol{v}}:H(\nu_{\cdot|\boldsymbol{v}}|\nu_{\boldsymbol{v}})\leq H(U|V)-\frac{3\varepsilon}{2}} \left|\mathcal{T}_{\nu_{\cdot|\boldsymbol{v}}}(\boldsymbol{v})\right| \\ &\leq \sum_{\nu_{\cdot|\boldsymbol{v}}:H(\nu_{\cdot|\boldsymbol{v}}|\nu_{\boldsymbol{v}})\leq H(U|V)-\frac{3\varepsilon}{2}} 2^{nH(\nu_{\cdot|\boldsymbol{v}}|\nu_{\boldsymbol{v}})} \\ &\leq \sum_{\nu_{\cdot|\boldsymbol{v}}:H(\nu_{\cdot|\boldsymbol{v}}|\nu_{\boldsymbol{v}})\leq H(U|V)-\frac{3\varepsilon}{2}} 2^{n[H(U|V)-\frac{3\varepsilon}{2}]} \\ &\leq 2^{n[H(U|V)-3\varepsilon/2+\lambda_{\mathcal{UV}}]} \\ &= 2^{-n[\varepsilon/2-\lambda_{\mathcal{UV}}]}|\mathcal{U}|^{l_{\mathcal{A}}}, \end{aligned} \tag{3}$$

where the first inequality comes from [1, Lemma 2.5] [3, Lemma 4], and the third inequality comes from [1, Lemma 2.2] [3, Lemma 3]. Then, from [2, Lemma 2 and eq. (27)] and (3), we have

$$\begin{aligned}&p_{AC}\left(\{(A,\boldsymbol{c}) : g_A(\boldsymbol{c}|\boldsymbol{v}) \notin \mathcal{T}(\boldsymbol{v})\}\right) \\ &\leq p_{AC}\left(\{(A,\boldsymbol{c}) : \mathcal{T}(\boldsymbol{v}) \cap \mathcal{C}_A(\boldsymbol{c}) = \emptyset\}\right) \\ &\quad + p_{AC}\left(\{(A,\boldsymbol{c}) : \mathcal{G}(\boldsymbol{v}) \cap \mathcal{C}_A(\boldsymbol{c}) \neq \emptyset\}\right) \\ &\leq \alpha_A - 1 + \frac{|\mathrm{Im}\mathcal{A}|\,[\beta_A+1]}{|\mathcal{T}(\boldsymbol{v})|} + \frac{|\mathcal{G}(\boldsymbol{v})|}{|\mathrm{Im}\mathcal{A}|} \\ &\leq \alpha_A - 1 + \frac{|\mathrm{Im}\mathcal{A}|\,[\beta_A+1]}{|\mathcal{T}(\boldsymbol{v})|} + \frac{2^{-n[\varepsilon/2-\lambda_{\mathcal{UV}}]}|\mathcal{U}|^{l_{\mathcal{A}}}}{|\mathrm{Im}\mathcal{A}|}. \end{aligned} \tag{4}$$

■

Next, we show the fact that

$$\mathcal{T}_{U|V,\gamma}(\boldsymbol{v}) \subset \mathcal{F}_{U|V,\varepsilon}(\boldsymbol{v}) \tag{5}$$

by assuming $\boldsymbol{v} \in \mathcal{T}_{V,\gamma}$ and

$$\zeta_{\mathcal{U}|\mathcal{V}}(\gamma|\gamma) \leq \frac{\varepsilon}{2}. \tag{6}$$

Assume that $\boldsymbol{u} \in \mathcal{T}_{U|V,\gamma}(\boldsymbol{v})$. From [2, Lemma 24], we have

$$\begin{aligned}\frac{1}{n}\log\frac{1}{\mu_{U|V}(\boldsymbol{u}|\boldsymbol{v})} &\leq H(U|V) + \zeta_{\mathcal{U}|\mathcal{V}}(\gamma|\gamma) \\ &\leq H(U|V) + \frac{\varepsilon}{2}. \end{aligned} \tag{7}$$

On the other hand, from [2, Lemma 21] and the fact that $\gamma > D(\nu_{\boldsymbol{u}|\boldsymbol{v}}\|\mu_{U|V}|\nu_{\boldsymbol{v}})$ we have

$$\begin{aligned}H(\nu_{\boldsymbol{u}|\boldsymbol{v}}|\nu_{\boldsymbol{v}}) &= \frac{1}{n}\log\frac{1}{\mu_{U|V}(\boldsymbol{u}|\boldsymbol{v})} - D(\nu_{\boldsymbol{u}|\boldsymbol{v}}\|\mu_{U|V}|\nu_{\boldsymbol{v}}) \\ &> H(U|V) - \zeta_{\mathcal{U}|\mathcal{V}}(\gamma|\gamma) - \gamma \\ &\geq H(U|V) - \frac{3\varepsilon}{2}, \end{aligned} \tag{8}$$

where the last inequality comes from the relation $\zeta_{\mathcal{U}|\mathcal{V}}(\gamma|\gamma) \geq \gamma$ and (6). Then, we have (5).

Next, we revise the proof of [2, Th. 4]. The condition

$$\zeta_{\mathcal{W}|\mathcal{Z}}(\gamma|\gamma) \leq \frac{\varepsilon}{2},$$

which implies [2, eqs. (75) and (76)] for all sufficiently large n, should be assumed. The left-hand side of [2, eq. (77)] should be replaced by $|\mathcal{F}_{W|Z,\varepsilon}(\boldsymbol{z})|$, where the first inequality of [2, eq. (77)] comes from (5). The term

$$\frac{2^{-n\varepsilon}|\mathcal{W}|^{l_{\mathcal{A}}+l_{\mathcal{B}}}}{|\mathrm{Im}\mathcal{A}||\mathrm{Im}\mathcal{B}|},$$

which appears in the derivation of [2, eq. (82)], should be replaced by

$$\frac{2^{-n[\varepsilon/2-\lambda_{\mathcal{WZ}}]}|\mathcal{W}|^{l_{\mathcal{A}}+l_{\mathcal{B}}}}{|\mathrm{Im}\mathcal{A}||\mathrm{Im}\mathcal{B}|},$$

which vanishes as $n \to \infty$.

Similarly, we revise the proof of [2, Th. 6]. The condition

$$\zeta_{\mathcal{Y}|\mathcal{XZ}}(\gamma|\gamma) \leq \frac{\varepsilon_{\mathcal{A}}}{2},$$

which implies [2, eq. (85)] for all sufficiently large n, should be assumed. The left-hand side of [2, eq. (93)] should be replaced by $|\mathcal{F}_{Y|XZ,\varepsilon_{\mathcal{A}}}(\boldsymbol{x},\boldsymbol{z})|$, where the first inequality of [2, eq. (93)] comes from (5). The term

$$\frac{2^{-n\varepsilon_{\mathcal{A}}}|\mathcal{Y}|^{l_{\mathcal{A}}}}{|\mathrm{Im}\mathcal{A}|},$$

which appears in the derivation of [2, eq. (95)], should be replaced by

$$\frac{2^{-n[\varepsilon_{\mathcal{A}}/2-\lambda_{\mathcal{XYZ}}]}|\mathcal{Y}|^{l_{\mathcal{A}}}}{|\mathrm{Im}\mathcal{A}|},$$

which vanishes as $n \to \infty$.

Next, we revise the proof of [2, Th. 7]. The condition

$$\zeta_{\mathcal{Z}|\mathcal{Y}}(\gamma|\gamma) \leq \frac{\varepsilon_{\mathcal{A}}}{2},$$

which implies [2, eq. (99)] for all sufficiently large n, should be assumed.

Finally, we revise some minor points. In the statement of [2, Lemma 6], the word "descending" should be replaced by "ascending." In the statement of [2, Lemma 10], "$(i,u) \in \{1,\ldots,l\} \times \mathrm{GF}(q)$" should be replaced by "$(i,u) \in \{1,\ldots,l\} \times [\mathrm{GF}(q) \setminus \{0\}]$."

ACKNOWLEDGMENT

We thank Dr. J. Honda who pointed out the flaw of the lemma. We also thank him for other valuable comments.

REFERENCES

[1] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[2] J. Muramatsu and S. Miyake, "Hash property and coding theorems for sparse matrices and maximal-likelihood coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2143–2167, May 2010.

[3] J. Muramatsu and S. Miyake, "Hash property and fixed-rate universal coding theorems," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2688–2698, Jun. 2010.