Comments and Corrections

Corrections to "Hash Property and Fixed-Rate Universal Coding Theorems"

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

There are flaws in the proof of [1, Ths. 1 and 3]. More precisely, inequalities

$$E_A[\mathrm{Error}_X(A)] \le \max\left\{\frac{\alpha_A|\mathcal{X}|^{l_{\mathcal{A}}}}{|\mathrm{Im}\mathcal{A}|}, 1\right\} 2^{-n[F_X(R)-2\lambda_{\mathcal{X}}]} + \beta_A$$

$$E_{ABC}[\mathrm{Error}_{Y|X}(A,B,C)] \le \alpha_{AB} - 1 + \frac{\beta_{AB}+1}{\kappa} + 2\kappa\left[\max\{\alpha_A, 1\} 2^{-n[F_{Y|X}(R_{\mathcal{A}})-2\lambda_{\mathcal{XY}}]} + \beta_A\right]$$

which appears in [1, eq. (37)] and [1, p. 2695], respectively, do not imply the existence of desired functions A, B, and a vector $\boldsymbol{c}$. To correct the flaws, we have to revise the statement of [1, Ths. 1 and 3, Corollary 2] as follows. Let $|\theta|^+ \equiv \max\{0, \theta\}$ as defined in [1, eq. (2)] and

$$\alpha'_A \equiv \frac{|\mathcal{X}|^{l_{\mathcal{A}}}\alpha_A}{|\mathrm{Im}\mathcal{A}|}.$$

It should be noted that α_A, β_A, and $\lambda_{\mathcal{U}}$ depend on n, where $\lambda_{\mathcal{U}} \equiv [|\mathcal{U}|/n]\log(n+1)$ as defined in [1, eq. (1)]. Furthermore, we can assume that $\beta_A \ge 0$ without loss of generality because [1, eq. (H4)] still holds when β_A is replaced by $|\beta_A|^+$.

Theorem 1: For a given fixed rate R, assume that $(\mathcal{A}, p_A)$ satisfies [1, eq. (H4)]. Then, for a given $\xi > 0$, there is a function (matrix) $A \in \mathcal{A}$ such that

$$\mathrm{Error}_X(A) \le [1+\xi]\left[2^{-n[F_X(R)-3\lambda_{\mathcal{X}}]}\max\left\{\alpha'_A, 1\right\} + 2^{n\lambda_{\mathcal{X}}}\beta_A\right]$$

for all stationary memoryless sources X, where $1/[1+\xi]$ represents the upper bound of the failure probability of selecting an appropriate function $A \in \mathcal{A}$. Since

$$\inf_{X:H(X)<R} F_X(R) > 0$$

then the error probability goes to zero as $n \to \infty$ for all X satisfying

$$H(X) < R$$

by assuming that ξ is a constant and

$$\lim_{n\to\infty} \frac{\log \alpha_A(n)}{n} = 0 \tag{1}$$

$$\lim_{n\to\infty} 2^{n\lambda_{\mathcal{X}}(n)}\beta_A(n) = 0. \tag{2}$$

Corollary 2: Let $\mathcal{A}$ be a set of linear functions and assume that $(\mathcal{A}, p_A)$ satisfies [1, eq. (H4)] for a fixed rate R. Then for a given $\xi > 0$ there is a (sparse) matrix $A \in \mathcal{A}$ such that

$$\mathrm{Error}_{Y|X}(A) \le [1+\xi]\left[2^{-n[F_Z(R)-3\lambda_{\mathcal{X}}]}\max\left\{\alpha'_A, 1\right\} + 2^{n\lambda_{\mathcal{X}}}\beta_A\right]$$

for all stationary memoryless channels with additive noise Z, where the error probability goes to zero as $n \to \infty$ for all X satisfying

$$\log|\mathcal{X}| - R < I(X;Y) = \log|\mathcal{X}| - H(Z)$$

by assuming (1) and (2) and that ξ is a constant.

Theorem 3: For given $R_{\mathcal{A}}$, $R_{\mathcal{B}} > 0$, assume that $(\mathcal{A}, p_A)$ (respectively, $(\mathcal{A}\times\mathcal{B}, p_{AB})$) satisfies [1, eq. (H4)] with (α_A, β_B) (respectively, $(\alpha_{AB}, \beta_{AB})$). For given input distribution μ_X, $\xi > 0$, and κ satisfying

$$H(X) \ge R_{\mathcal{A}} + R_{\mathcal{B}} + \lambda_{\mathcal{X}} + \frac{\log\kappa}{n}$$

there are functions (matrices) $A \in \mathcal{A}$, $B \in \mathcal{B}$, and a vector $\boldsymbol{c} \in \mathrm{Im}\mathcal{A}$ such that

$$\mathrm{Error}_{Y|X}(A,B,\boldsymbol{c}) \le 2[1+\xi]\left[\alpha_{AB} - 1 + \frac{\beta_{AB}+1}{\kappa} + 2\kappa\left[2^{-n[F_{Y|X}(R_{\mathcal{A}})-3\lambda_{\mathcal{XY}}]}\max\{\alpha_A, 1\} + 2^{2n\lambda_{\mathcal{XY}}}\beta_A\right]\right] \tag{3}$$

for all stationary memoryless channels $\mu_{Y|X}$, where $1/[1+\xi]$ represents the upper bound of failure probability of selecting appropriate functions $A \in \mathcal{A}$, $B \in \mathcal{B}$, and a vector $\boldsymbol{c} \in \mathrm{Im}\mathcal{A}$. Since

$$\inf_{\mu_{Y|X}:H(X|Y)<R_{\mathcal{A}}} F_{Y|X}(R_{\mathcal{A}}) > 0$$

then the right-hand side of (3) goes to zero as $n \to \infty$ for all $\mu_{Y|X}$ satisfying

$$H(X|Y) < R_{\mathcal{A}}$$

by assuming that ξ is a constant and

$$\lim_{n\to\infty}\frac{\log\alpha_A(n)}{n} = 0$$
$$\lim_{n\to\infty}\alpha_{AB}(n) = 1$$
$$\lim_{n\to\infty}\kappa(n)2^{2n\lambda_{\mathcal{XY}}(n)}\beta_A(n) = 0 \tag{4}$$
$$\lim_{n\to\infty}\frac{\beta_{AB}(n)}{\kappa(n)} = 0 \tag{5}$$
$$\lim_{n\to\infty}\kappa(n) = \infty \tag{6}$$
$$\lim_{n\to\infty}\frac{\log\kappa(n)}{n} = 0 \tag{7}$$

Manuscript received April 14, 2011; revised October 10, 2011; accepted December 12, 2011. Date of current version April 17, 2012.

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 T. Uyematsu, Associate Editor for Shannon Theory.

Digital Object Identifier 10.1109/TIT.2011.2181486

where κ denotes $\kappa(n)$.

Remark 1: By tracing the proof of [3, Lemma 18, eqs. (66) and (70)], we can confirm that the ensemble of sparse matrices introduced in [1, Sec. III-B] and [3, Sec. IV] satisfies (2) by defining $\tau \equiv 2\lceil \tau' \log n \rceil$ and letting the constant τ' be sufficiently large depending on $|\mathcal{X}|$.

Remark 2: The existence of a sequence κ satisfying (4)–(7) can be shown similar to [1, eq. (29)] by assuming $\lim_{n\to\infty} 2^{2n\lambda_{\mathcal{X}\mathcal{Y}}(n)}\beta_A(n) = 0$.

Corrections of the proof of theorems are presented in the following. The proof is analogous to [2].

Proof of [1, Th. 1]: Instead of [1, eq. (37)], we use the following inequality:

$$\begin{aligned}
&E_A\left[\sum_{\boldsymbol{x}\in\mathcal{T}_U}\frac{\chi(g_A(A\boldsymbol{x})\neq\boldsymbol{x})}{|\mathcal{T}_U|}\right]\\
&\leq E_A\left[\sum_{\boldsymbol{x}\in\mathcal{T}_U}\frac{\chi([\mathcal{G}_U\setminus\{\boldsymbol{x}\}]\cap\mathcal{C}_A(A\boldsymbol{x})\neq\emptyset)}{|\mathcal{T}_U|}\right]\\
&=\sum_{\boldsymbol{x}\in\mathcal{T}_U}\frac{p_A(\{A:[\mathcal{G}_U\setminus\{\boldsymbol{x}\}]\cap\mathcal{C}_A(A\boldsymbol{x})\neq\emptyset\})}{|\mathcal{T}_U|}\\
&\leq\frac{1}{|\mathcal{T}_U|}\sum_{\boldsymbol{x}\in\mathcal{T}_U}\min\left\{\frac{|\mathcal{G}_U|\alpha_A}{|\mathrm{Im}\mathcal{A}|}+\beta_A,1\right\}\\
&\leq\min\left\{\frac{|\mathcal{X}|^{l_{\mathcal{A}}}2^{-n[R-H(U)-\lambda_{\mathcal{X}}]}\alpha_A}{|\mathrm{Im}\mathcal{A}|}+\beta_A,1\right\}\\
&\leq 2^{-n[|R-H(U)|^+-\lambda_{\mathcal{X}}]}\max\left\{\frac{|\mathcal{X}|^{l_{\mathcal{A}}}\alpha_A}{|\mathrm{Im}\mathcal{A}|},1\right\}+\beta_A.
\end{aligned}\tag{8}$$

Then, by using the Markov inequality, we have the fact that for a given $\xi > 0$, there is a function (matrix) A such that

$$\begin{aligned}
&\sum_{\boldsymbol{x}\in\mathcal{T}_U}\frac{\chi(g_A(A\boldsymbol{x})\neq\boldsymbol{x})}{|\mathcal{T}_U|}\\
&\leq[1+\xi]2^{n\lambda_{\mathcal{X}}}\left[2^{-n[|R-H(U)|^+-\lambda_{\mathcal{X}}]}\max\left\{\alpha'_A,1\right\}+\beta_A\right]
\end{aligned}$$

for any type U. Then, we have

$$\begin{aligned}
&\mathrm{Error}_X(A)\\
&=\sum_{\boldsymbol{x}}\mu_X(\boldsymbol{x})\chi(g_A(A\boldsymbol{x})\neq\boldsymbol{x})\\
&=\sum_U\mu_X(\mathcal{T}_U)\sum_{\boldsymbol{x}\in\mathcal{T}_U}\frac{\chi(g_A(A\boldsymbol{x})\neq\boldsymbol{x})}{|\mathcal{T}_U|}\\
&\leq\sum_U 2^{-nD(\nu_U\|\mu_X)}[1+\xi]2^{-n[|R-H(U)|^+-2\lambda_{\mathcal{X}}]}\max\left\{\alpha'_A,1\right\}\\
&\quad+\sum_U\mu_X(\mathcal{T}_U)[1+\xi]2^{n\lambda_{\mathcal{X}}}\beta_A\\
&\leq[1+\xi]\left[2^{-n[F_X(R)-3\lambda_{\mathcal{X}}]}\max\left\{\alpha'_A,1\right\}+2^{n\lambda_{\mathcal{X}}}\beta_A\right]
\end{aligned}\tag{9}$$

for any μ_X. ■

Proof of [1, Th. 3]: Assume that $\mathcal{T}\subset\mathcal{T}_U$ satisfies [1, eq. (40)]. Similarly to the proof of [1, eq. (42)], we have

$$\begin{aligned}
&E_{ABC}\left[p_M(\{\boldsymbol{m}:g_{AB}(\boldsymbol{c},\boldsymbol{m})\notin\mathcal{T}\})\right]\\
&\leq p_{ABCM}(\{(A,B,\boldsymbol{c},\boldsymbol{m}):\mathcal{T}\cap\mathcal{C}_{AB}(\boldsymbol{c},\boldsymbol{m})=\emptyset\})\\
&\leq\alpha_{AB}-1+\frac{|\mathrm{Im}\mathcal{A}||\mathrm{Im}\mathcal{B}|\left[\beta_{AB}+1\right]}{|\mathcal{T}|}\\
&\leq\alpha_{AB}-1+\frac{\beta_{AB}+1}{\kappa}.
\end{aligned}\tag{10}$$

Next, by using

$$\begin{aligned}
&E_A\left[\chi(g_A(A\boldsymbol{x}|\boldsymbol{y})\neq\boldsymbol{x})\right]\\
&=p_A\left(\left\{A:\begin{array}{l}\exists\boldsymbol{x}'\neq\boldsymbol{x}\text{ s.t. }H(\boldsymbol{x}'|\boldsymbol{y})\leq H(\boldsymbol{x}|\boldsymbol{y})\\ \text{and }A\boldsymbol{x}'=A\boldsymbol{x}\end{array}\right\}\right)\\
&\leq p_A(\{A:[\mathcal{G}(\boldsymbol{y})\setminus\{\boldsymbol{x}\}]\cap\mathcal{C}_A(A\boldsymbol{x})\neq\emptyset\})\\
&\leq\min\left\{\frac{2^{n[H(U|V)+\lambda_{\mathcal{X}\mathcal{Y}}]}\alpha_A}{|\mathrm{Im}\mathcal{A}|}+\beta_A,1\right\}\\
&\leq 2^{-n[|R_{\mathcal{A}}-H(U|V)|^+-\lambda_{\mathcal{X}\mathcal{Y}}]}\max\left\{\alpha_A,1\right\}+\beta_A
\end{aligned}\tag{11}$$

we have

$$\begin{aligned}
&E_{AC}\left[\sum_{\boldsymbol{x}\in\mathcal{T}}\sum_{\boldsymbol{y}\in\mathcal{T}_{V|U}(\boldsymbol{x})}\frac{\chi(g_A(C|\boldsymbol{y})\neq\boldsymbol{x})\chi(A\boldsymbol{x}=C)}{|\mathcal{T}||\mathcal{T}_{V|U}(\boldsymbol{x})|}\right]\\
&=\sum_{\boldsymbol{x}\in\mathcal{T}}\sum_{\boldsymbol{y}\in\mathcal{T}_{V|U}(\boldsymbol{x})}\frac{E_A\left[\chi(g_A(A\boldsymbol{x}|\boldsymbol{y})\neq\boldsymbol{x})E_C[\chi(A\boldsymbol{x}=C)]\right]}{|\mathcal{T}||\mathcal{T}_{V|U}(\boldsymbol{x})|}\\
&\leq\frac{2^{-n[|R_{\mathcal{A}}-H(U|V)|^+-\lambda_{\mathcal{X}\mathcal{Y}}]}\max\left\{\alpha_A,1\right\}+\beta_A}{|\mathrm{Im}\mathcal{A}|}
\end{aligned}\tag{12}$$

which is the replacement of [1, eq. (43)]. Then, by using the Markov inequality, we have the fact that for a given $\xi > 0$ there are functions (matrices) $A\in\mathcal{A}$, $B\in\mathcal{B}$, and a vector $\boldsymbol{c}\in\mathrm{Im}\mathcal{A}$ satisfying

$$p_M(\{\boldsymbol{m}:g_{AB}(\boldsymbol{c},\boldsymbol{m})\notin\mathcal{T}\})\leq 2[1+\xi]\left[\alpha_{AB}-1+\frac{\beta_{AB}+1}{\kappa}\right]$$

$$\begin{aligned}
p_{MY}(\mathcal{S}_1\cap\mathcal{S}_2^c)&=\sum_{\boldsymbol{m}}p_M(\boldsymbol{m})\sum_{\boldsymbol{x}\in\mathcal{T}}\chi(g_{AB}(\boldsymbol{c},\boldsymbol{m})=\boldsymbol{x})\sum_{\boldsymbol{y}}\mu_{Y|X}(\boldsymbol{y}|\boldsymbol{x})\chi(g_A(\boldsymbol{c}|\boldsymbol{y})\neq\boldsymbol{x})\\
&\leq\sum_{\boldsymbol{m}}p_M(\boldsymbol{m})\sum_{\boldsymbol{x}\in\mathcal{T}}\chi(A\boldsymbol{x}=\boldsymbol{c})\chi(B\boldsymbol{x}=\boldsymbol{m})\sum_{\boldsymbol{y}}\mu_{Y|X}(\boldsymbol{y}|\boldsymbol{x})\chi(g_A(\boldsymbol{c}|\boldsymbol{y})\neq\boldsymbol{x})\\
&=\frac{|\mathcal{T}|}{|\mathrm{Im}\mathcal{B}|}\sum_{V|U}\sum_{\boldsymbol{x}\in\mathcal{T}}\mu_{Y|X}(\mathcal{T}_{V|U}(\boldsymbol{x})|\boldsymbol{x})\sum_{\boldsymbol{y}\in\mathcal{T}_{V|U}(\boldsymbol{x})}\frac{\chi(g_A(\boldsymbol{c}|\boldsymbol{y})\neq\boldsymbol{x})\chi(A\boldsymbol{x}=\boldsymbol{c})}{|\mathcal{T}||\mathcal{T}_{V|U}(\boldsymbol{x})|}\\
&\leq\frac{2[1+\xi]2^{n\lambda_{\mathcal{X}\mathcal{Y}}}|\mathcal{T}|}{|\mathrm{Im}\mathcal{A}||\mathrm{Im}\mathcal{B}|}\sum_{V|U}2^{-nD(\nu_{V|U}\|\mu_{Y|X}|\nu_U)}\left[2^{-n[|R_{\mathcal{A}}-H(U|V)|^+-\lambda_{\mathcal{X}\mathcal{Y}}]}\max\left\{\alpha_A,1\right\}+\beta_A\right]\\
&\leq 2[1+\xi]\kappa\left[2^{-n[F_{Y|X}(R_{\mathcal{A}})-3\lambda_{\mathcal{X}\mathcal{Y}}]}\max\left\{\alpha_A,1\right\}+2^{2n\lambda_{\mathcal{X}\mathcal{Y}}}\beta_A\right]
\end{aligned}\tag{13}$$

and

$$\sum_{\boldsymbol{x}\in\mathcal{T}}\sum_{\boldsymbol{y}\in\mathcal{T}_{V|U}(\boldsymbol{x})}\frac{\chi(g_A(\boldsymbol{c}|\boldsymbol{y})\neq\boldsymbol{x})\chi(A\boldsymbol{x}=\boldsymbol{c})}{|\mathcal{T}||\mathcal{T}_{V|U}(\boldsymbol{x})|}$$
$$\leq\frac{2[1+\xi]2^{n\lambda_{\mathcal{X}\mathcal{Y}}}}{|\mathrm{Im}\mathcal{A}|}$$
$$\cdot\left[2^{-n[|R_{\mathcal{A}}-H(U|V)|^{+}-\lambda_{\mathcal{X}\mathcal{Y}}]}\max\{\alpha_A,1\}+\beta_A\right]$$

for every $V|U$. Finally, we define $(\mathrm{UC}i)$ as [1, eqs. (UC1) and (UC2)] and

$$\mathcal{S}_i\equiv\{(\boldsymbol{m},\boldsymbol{y}):(\mathrm{UCi})\}$$

(there is a typo in [1, def. of $\mathcal{S}_i$]. Then, we have

$$p_{MY}(\mathcal{S}_1^c)\leq 2[1+\xi]\left[\alpha_{AB}-1+\frac{\beta_{AB}+1}{\kappa}\right]$$

and (13), shown at the bottom of the previous page, and is the replacement of [1, eq. (44)], for every $\mu_{Y|X}$. Then, we have (3) from the fact that

$$\mathrm{Error}_{Y|X}(A,B,\boldsymbol{c})\leq p_{MY}(\mathcal{S}_1^c)+p_{MY}(\mathcal{S}_1\cap\mathcal{S}_2^c)$$

(there is a typo in [1, eq. (41)]). ■

Acknowledgment

The authors thank anonymous reviewers and the associate editor Prof. Uyematsu for valuable comments.

References

[1] J. Muramatsu and S. Miyake, "Hash property and fixed-rate universal coding theorems," *IEEE Trans. Inf. Theory*, vol. IT-56, no. 6, pp. 2688–2698, Jun. 2010.
[2] I. Csiszár, "Linear codes for sources and source networks: Error exponents, universal coding," *IEEE Trans. Inf. Theory*, vol. IT-28, no. 4, pp. 585–592, Jul. 1982.
[3] J. Muramatsu and S. Miyake, "Hash property and coding theorems for sparse matrices and maximal-likelihood coding," *IEEE Trans. Inf. Theory*, vol. IT-56, no. 9, pp. 4762–4762, Sep. 2010, (Corrections: vol. IT-56, no. 9, p. 4762, Sep. 2010.).