統計数理(2009)
第 57 巻 第 2 号 203–219

特集「ネットワーク情報理論」
[研究詳解]

疎行列アンサンブルのハッシュ性と多端子情報源符号

村松 純[1] ・三宅 茂樹[2]

(受付 2009 年 1 月 6 日；改訂 3 月 3 日；採択 3 月 24 日)

要　　旨

本稿では，多端子情報理論の基本的な問題である Slepian-Wolf の問題，Wyner-Ziv の問題，One-helps-one 問題に焦点をあてて，疎行列を用いた符号の構成を与える．そのためにまず，アンサンブルの持つハッシュ性と呼ばれる性質を導入し，この性質を利用して漸近最良性を持つ符号の構成を与える．疎行列はハッシュ性を持つことから，疎行列を利用した漸近最良性を持つ符号の存在が示される．

キーワード： 情報理論，ハッシュ性，疎行列を用いた符号，Slepian-Wolf の問題，Wyner-Ziv の問題，One-helps-one 問題．

1. はじめに

加法的雑音を伴う通信路に対する漸近最良性を持つ符号として疎行列を用いた LDPC (Low Density Parity Check) 符号がある．これは，確率伝搬法 (Belief Propagation, Aji and McEliece, 2000; Kschischang et al., 2001) や線形計画法 (Linear Code Linear Programing, Feldman et al., 2005) 等の近似アルゴリズムを用いることにより現実的な計算時間で最尤復号を実現出来ることから，近年盛んに研究されている．このアイデアは加法的雑音を伴う通信路に対する符号へ応用できるだけでなく，他のさまざまな符号の構成にも応用出来ることが明らかになってきた．さらに，それらの符号の漸近最良性は疎行列アンサンブルの持つハッシュ性と呼ばれる性質から導かれることが Muramatsu and Miyake (2008a, 2008b, 2009) によって明らかにされた．本稿では，多端子情報理論の基本的な問題である Slepian-Wolf の問題 (図 1, Slepian and Wolf, 1973)，Wyner-Ziv の問題 (図 2, Wyner and Ziv, 1973)，One-helps-one 問題 (図 3, Wyner, 1973; Wyner and Ziv, 1976) に焦点をあてて，ハッシュ性を持つアンサンブルを用いた符号の構成を紹介する．

2. 準備

本稿で使用する記号や記法を説明する．

系列や列ベクトルはボールド体を用いて $\boldsymbol{u}$ のように記す．$\mathcal{U}, \overline{\mathcal{U}}$ を有限集合とし，有限集合 $\mathcal{U}$ の要素の個数を $|\mathcal{U}|$ と記す．$\mathcal{U} \setminus \{\boldsymbol{u}\}$ は差集合を表す．次節以降でハッシュ性を仮定するときは，関数の線形性や $\overline{\mathcal{U}} \equiv \mathcal{U}^l$ であることは本質的ではない．実際，$l \log |\mathcal{U}|$ を $\log |\overline{\mathcal{U}}|$ に置き換

[1] NTT コミュニケーション科学基礎研究所：〒619–0237 京都府相楽郡精華町光台 2–4
[2] NTT 未来ねっと研究所：〒180–8585 東京都武蔵野市緑町 3–9–11

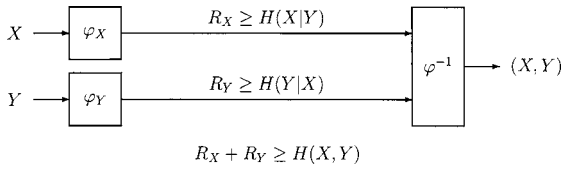

図 1. Slepian-Wolf 問題.

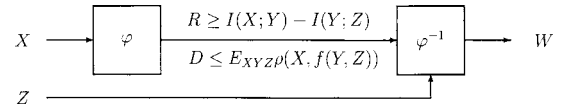

図 2. Wyner-Ziv 問題.

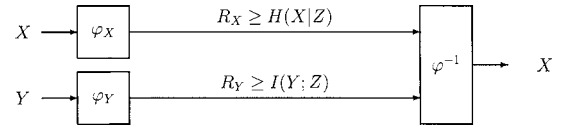

図 3. One-helps-one 問題.

えれば全く同じ議論が出来る.

関数 $A:\mathcal{U}^n \to \overline{\mathcal{U}}$ に対して，A の系列 $\boldsymbol{u} \in \mathcal{U}^n$ での値を関数の線形性のあるなしに関わらず $A\boldsymbol{u}$ と記す．線形性を持つ関数が $l \times n$ 行列で表現されている時は $\overline{\mathcal{U}} \equiv \mathcal{U}^l$ となる.

関数の集合 $\mathcal{A}$ に対して $\mathrm{Im}\mathcal{A}$ を次のように定義する.

$$\mathrm{Im}\mathcal{A} \equiv \bigcup_{A \in \mathcal{A}} \{A\boldsymbol{u} : \boldsymbol{u} \in \mathcal{U}^n\}$$

集合 $\mathcal{C}_A(\boldsymbol{c})$, $\mathcal{C}_{AB}(\boldsymbol{c},\boldsymbol{b})$ を次のように定義する.

$$\mathcal{C}_A(\boldsymbol{c}) \equiv \{\boldsymbol{u} : A\boldsymbol{u} = \boldsymbol{c}\}$$
$$\mathcal{C}_{AB}(\boldsymbol{c},\boldsymbol{b}) \equiv \{\boldsymbol{u} : A\boldsymbol{u} = \boldsymbol{c}, B\boldsymbol{u} = \boldsymbol{b}\}$$

線形符号の理論では，行列 A に対して集合 $\mathcal{C}_A(\boldsymbol{c})$ はシンドローム $\boldsymbol{c}$ で定まるコセットと呼ばれている.

確率分布 p, p' と条件つき確率分布 q, q' に対してエントロピー $H(p)$, 条件つきエントロピー $H(q|p)$, ダイヴァージェンス $D(p\|p')$, 条件つきダイヴァージェンス $D(q\|q'|p)$ を次のように定義する.

$$H(p) \equiv \sum_u p(u) \log \frac{1}{p(u)}$$
$$H(q|p) \equiv \sum_{u,v} q(u|v)p(v) \log \frac{1}{q(u|v)}$$
$$D(p \,\|\, p') \equiv \sum_u p(u) \log \frac{p(u)}{p'(u)}$$

$$D(q\,\|\,q'|p)\equiv\sum_v p(v)\sum_u q(u|v)\log\frac{q(u|v)}{q'(u|v)}$$

ここで，本稿を通して対数の底を 2 とする．

確率変数 U と V の同時確率分布を μ_{UV} と記す．周辺分布をそれぞれ μ_U, μ_V と記し，V を与えた時の U の条件つき確率分布を $\mu_{U|V}$ とする．U のエントロピー，V を与えたときの U の条件つきエントロピー U と V の相互情報量は以下のように定義される．

$$H(U)\equiv H(\mu_U)$$
$$H(U|V)\equiv H(\mu_{U|V}|\mu_V)$$
$$I(U;V)\equiv H(U)-H(U|V)$$

最後に，経験分布 $\nu_{\boldsymbol{u}}$, 条件つき経験分布 $\nu_{\boldsymbol{u}|\boldsymbol{v}}$ を次のように定義する．

$$\nu_{\boldsymbol{u}}(u)\equiv\frac{|\{1\le i\le n:u_i=u\}|}{n}$$
$$\nu_{\boldsymbol{u}|\boldsymbol{v}}(u|v)\equiv\frac{\nu_{\boldsymbol{uv}}(u,v)}{\nu_{\boldsymbol{v}}(v)}$$

3. $(\boldsymbol{\alpha},\boldsymbol{\beta})$-ハッシュ性

本節では，符号の存在定理の十分条件を与える $(\boldsymbol{\alpha},\boldsymbol{\beta})$-ハッシュ性の概念を新たに導入する．これは関数のアンサンブル(関数の集合上の確率分布)によって定義されるものであるが，関数の線形性については特に仮定しない．

定義 1. $\mathcal{A}$ を関数 $A:\mathcal{U}^n\to\overline{\mathcal{U}}_{\mathcal{A}}$ の集合とする．そして

$$\lim_{n\to\infty}\frac{\log\dfrac{|\overline{\mathcal{U}}_{\mathcal{A}}|}{|\mathrm{Im}\mathcal{A}|}}{n}=0 \tag{3.1}$$

を仮定する．p_A を $\mathcal{A}$ 上の確率分布とする．ここで，p_A の添字 A は $\mathcal{A}$ の要素を表すのではなく，$\mathcal{A}$ の要素を値とする確率変数(関数)を表している．関数の集合 $\mathcal{A}$ と確率分布 p_A の組 $(\mathcal{A},p_A)$ をアンサンブルと呼ぶ．通常，アンサンブルは関数の集合を表し，その集合上に一様分布を仮定する．本稿では，関数の集合と必ずしも一様ではない確率分布をアンサンブルと呼んでいる．そしてアンサンブル $(\mathcal{A},p_A)$ に対して

$$\lim_{n\to\infty}\alpha_A(n)=1 \tag{3.2}$$

$$\lim_{n\to\infty}\beta_A(n)=0 \tag{3.3}$$

を満たす数列 $\boldsymbol{\alpha}_A\equiv\{\alpha_A(n)\}_{n=1}^{\infty}$, $\boldsymbol{\beta}_A\equiv\{\beta_A(n)\}_{n=1}^{\infty}$ が存在して

$$\sum_{\substack{\boldsymbol{u}\in\mathcal{T}\\ \boldsymbol{u}'\in\mathcal{T}'}}p_A\left(\left\{A:A\boldsymbol{u}=A\boldsymbol{u}'\right\}\right)\le|\mathcal{T}\cap\mathcal{T}'|+\frac{|\mathcal{T}||\mathcal{T}'|\alpha_A(n)}{|\mathrm{Im}\mathcal{A}|}+\min\{|\mathcal{T}|,|\mathcal{T}'|\}\beta_A(n) \tag{3.4}$$

を任意の $\mathcal{T},\mathcal{T}'\subset\mathcal{U}^n$ に対して満たしているとき，$(\mathcal{A},p_A)$ は $(\boldsymbol{\alpha}_A,\boldsymbol{\beta}_A)$-ハッシュ性を持つという．本稿を通して，系列の長さ n が明らかなときには，n を省略して α_A, β_A と記す．また，α_A, β_A の添字 A は $\mathcal{A}$ の要素に依存していることを意味しているのではなく，$\mathcal{A}$ の要素を値とする確率変数(関数)に依存する可能性を示している．

以後，単に “ハッシュ性” と呼ぶときはある $(\boldsymbol{\alpha}_A,\boldsymbol{\beta}_A)$ が存在して $(\boldsymbol{\alpha}_A,\boldsymbol{\beta}_A)$-ハッシュ性を持っているものとする．式(3.4)右辺の第 1 項は $\boldsymbol{u}\in\mathcal{T}\cap\mathcal{T}'$ に対する $p_A(\{A:A\boldsymbol{u}=A\boldsymbol{u}'\})=1$ の和を表す．第 2 項は確率 $p_A(\{A:A\boldsymbol{u}=A\boldsymbol{u}'\})$ がおおよそ $1/|\mathrm{Im}\mathcal{A}|$ であるような $\boldsymbol{u}\neq\boldsymbol{u}'$ に対する和の上限を与えている．第 3 項は確率 $p_A(\{A:A\boldsymbol{u}=A\boldsymbol{u}'\})$ が $1/|\mathrm{Im}\mathcal{A}|$ をはるかに越えるような $\boldsymbol{u}\neq\boldsymbol{u}'$ に対する和の上限を与えている．

以下で，ハッシュ性を持つアンサンブルの例を挙げる．

例 1. 最初の例として，Carter and Wegman (1979)で導入された汎用ハッシュ関数クラスを紹介する．関数 $A:\mathcal{U}^n\to\overline{\mathcal{U}}_{\mathcal{A}}$ の集合 $\mathcal{A}$ が任意の $\boldsymbol{u}\neq\boldsymbol{u}'$ に対して

$$|\{A:A\boldsymbol{u}=A\boldsymbol{u}'\}|\leq\frac{|\mathcal{A}|}{|\overline{\mathcal{U}}_{\mathcal{A}}|}$$

が成り立っている時，$\mathcal{A}$ は**汎用ハッシュ関数クラス**であるという．例えば，$\mathcal{U}^n$ 上の関数全体，線形写像 $A:\mathcal{U}^n\to\mathcal{U}^{l_{\mathcal{A}}}$ の全体は汎用ハッシュ関数クラスの例である(Carter and Wegman, 1979)．また，有限体 $\mathcal{U}^n\equiv\mathrm{GF}(2^n)$ に対して

$$\mathcal{A}\equiv\left\{A:\begin{array}{l}A\boldsymbol{u}\equiv[\boldsymbol{a}\boldsymbol{u}\text{の最初の }l_{\mathcal{A}}\text{ ビット}]\\ \boldsymbol{a}\in\mathrm{GF}(2^n)\end{array}\right\}$$

もまた汎用ハッシュ関数クラスである．ここで，$\boldsymbol{a}\boldsymbol{u}$ は $\boldsymbol{a},\boldsymbol{u}\in\mathrm{GF}(2^n)$ の積を表す．

上記の全ての例において，$\mathrm{Im}\mathcal{A}=\overline{\mathcal{U}}_{\mathcal{A}}$ を満たしている．汎用ハッシュ関数クラス $\mathcal{A}$ と $\mathcal{A}$ 上の一様分布 p_A に対して

$$\sum_{\substack{\boldsymbol{u}\in\mathcal{T}\\ \boldsymbol{u}'\in\mathcal{T}'}}p_A\left(\left\{A:A\boldsymbol{u}=A\boldsymbol{u}'\right\}\right)\leq|\mathcal{T}\cap\mathcal{T}'|+\frac{|\mathcal{T}||\mathcal{T}'|}{|\mathrm{Im}\mathcal{A}|}$$

が任意の $\mathcal{T},\mathcal{T}'\subset\mathcal{U}^n$ で成り立つことが容易に確認できる．これは，各 n で $\mathbf{1}(n)\equiv1$, $\mathbf{0}(n)\equiv0$ と定めることにより $(\mathcal{A},p_A)$ が $(\mathbf{1},\mathbf{0})$-ハッシュ性を持つことを意味する．

例 2. 次の例では，線形写像(行列) $A:\mathcal{U}^n\to\mathcal{U}^{l_{\mathcal{A}}}$ のアンサンブルを考える．全ての線形写像上に一様分布を仮定すれば，このアンサンブルが $(\mathbf{1},\mathbf{0})$-ハッシュ性を持つことは例 1 の汎用ハッシュ関数クラスの例で紹介した．続いて，行列の要素が $\mathrm{GF}(q)$ であるような疎行列のアンサンブルの例を紹介する．これは，MacKay (1999)で与えられた $\mathrm{GF}(2)$ を行列の要素とする疎行列アンサンブルを $\mathrm{GF}(q)$ に拡張したものである．$\mathcal{U}\equiv\mathrm{GF}(q)$ として，$l_{\mathcal{A}}\times n$ 行列 A を以下の手続きで与える．

(1) 要素が全て 0 の行列を初期値とする．

(2) 列のインデックス $i\in\{1,\ldots,n\}$ に対して以下の(a), (b)の手続きを $O(\log_2 n)$ 回行う：

(a) $(j,a)\in\{1,\ldots,l_{\mathcal{A}}\}\times[\mathrm{GF}(q)\setminus\{0\}]$ を一様分布に従い選択する．

(b) a を行列の (j,i) に加える．

このとき，(3.2), (3.3)を満たす $(\boldsymbol{\alpha}_A,\boldsymbol{\beta}_A)$ が存在して，上記の手続きで与えたアンサンブル $(\mathcal{A},p_A)$ は $(\boldsymbol{\alpha}_A,\boldsymbol{\beta}_A)$-ハッシュ性を持つ(Muramatsu and Miyake, 2008a)．上記の手続きは列重みが定数オーダーではないことから，厳密にはこれを疎行列とは呼ばない場合もあるが，列重みが $O(\log_2 n)$ であることから，非常に大きな n では非零の要素が疎であるとみなすことができる．

ここで，$(\boldsymbol{\alpha}_A,\boldsymbol{\beta}_A)$-ハッシュ性を持つアンサンブルの性質を紹介する．以下では，関数 $A:\mathcal{U}^n\to\overline{\mathcal{U}}_{\mathcal{A}}$ の集合 $\mathcal{A}$ に関して，$(\mathcal{A},p_A)$ は $(\boldsymbol{\alpha}_A,\boldsymbol{\beta}_A)$-ハッシュ性を持っているとする．同様に，

$B:\mathcal{U}^n \to \overline{\mathcal{U}}_{\mathcal{B}}$ の集合 $\mathcal{B}$ に関して，$(\mathcal{B},p_B)$ は $(\boldsymbol{\alpha}_B,\boldsymbol{\beta}_B)$-ハッシュ性を持っているとする．$p_C$ を $\mathrm{Im}\mathcal{A}$ 上の確率分布として，確率変数 A, B, C は互いに独立であると仮定する．すなわち，任意の A, B, $\boldsymbol{c}$ に対して

$$p_C(\boldsymbol{c}) = \begin{cases} \dfrac{1}{|\mathrm{Im}\mathcal{A}|}, & \text{if } \boldsymbol{c} \in \mathrm{Im}\mathcal{A} \\ 0, & \text{if } \boldsymbol{c} \in \overline{\mathcal{U}}_{\mathcal{A}} \setminus \mathrm{Im}\mathcal{A} \end{cases}$$

$$p_{ABC}(A,B,\boldsymbol{c}) = p_A(A)p_B(B)p_C(\boldsymbol{c})$$

が成り立っている．

補題 1.（Muramatsu and Miyake, 2008a）任意の $\boldsymbol{u} \in \mathcal{U}^n$, $\mathcal{G} \subset \mathcal{U}^n$ に対して

$$p_A(\{A : [\mathcal{G} \setminus \{\boldsymbol{u}\}] \cap \mathcal{C}_A(A\boldsymbol{u}) \neq \emptyset\}) \leq \frac{|\mathcal{G}|\alpha_A}{|\mathrm{Im}\mathcal{A}|} + \beta_A.$$

補題 2.（Muramatsu and Miyake, 2008a）$\boldsymbol{u}_{A,\boldsymbol{c}} \in \mathcal{U}^n$ が A, $\boldsymbol{c}$ に依存して定まるとき，任意の $\mathcal{G} \subset \mathcal{U}^n$ に対して

$$p_{ABC}(\{(A,B,\boldsymbol{c}) : [\mathcal{G} \setminus \{\boldsymbol{u}_{A,\boldsymbol{c}}\}] \cap \mathcal{C}_{AB}(\boldsymbol{c},B\boldsymbol{u}_{A,\boldsymbol{c}}) \neq \emptyset\}) \leq \frac{|\mathcal{G}|\alpha_B}{|\mathrm{Im}\mathcal{A}||\mathrm{Im}\mathcal{B}|} + \beta_B.$$

補題 3.（Muramatsu and Miyake, 2008a）$\mathcal{T} \neq \emptyset$ に対して

$$p_{AC}(\{(A,\boldsymbol{c}) : \mathcal{T} \cap \mathcal{C}_A(\boldsymbol{c}) = \emptyset\}) \leq \alpha_A - 1 + \frac{|\mathrm{Im}\mathcal{A}|\,[\beta_A + 1]}{|\mathcal{T}|}.$$

上記の補題 1 は，4.1 節の無歪圧縮のための部品の存在を保証し，補題 3 は 4.2 節の典型系列を見つけるための部品の存在を保証する．補題 2 は，無歪圧縮のための部品が典型系列を見つけるための部品と組み合わせられることを保証するもので，補題 1 から証明される．以上の補題は，アンサンブルのハッシュ性だけから導かれる性質であり，関数の線形性を必要としない．言うまでもなく，例 2 で紹介した疎行列のアンサンブルに対しても上記の補題は成立している．証明は Muramatsu and Miyake (2008a) にある．

以下では(疎)行列のアンサンブルを仮定して符号の構成を与える．ただし，特に線形性に関する断りがなければ，以下で紹介する補題および定理の証明はアンサンブルのハッシュ性があれば十分であることを注意しておく．

4. 基本的な部品

この節では，(疎)行列を用いた符号を構成するための基本的な部品を紹介する．最初に，無歪圧縮のための部品(圧縮器，伸長器)および典型系列を探索する部品を定義する．次節では，これらの部品を組み合わせることで，Slepian-Wolf 問題，Wyner-Ziv 問題，One-helps-one 問題といった多様な問題に対して有効な符号が構成できることが示される．本節の補題および定理は全て，前節のハッシュ性を仮定するだけで証明できるものであり，関数の線形性や疎行列性とは直接関係していない．また本論文では，符号の計算複雑度の問題は考えていない．

4.1 無歪圧縮のための部品

$l_{\mathcal{A}} \times n$ 行列 A を用意し，列ベクトル $\boldsymbol{u} \in \mathcal{U}^n$ に対してシンドロームを $A\boldsymbol{u} \in \mathcal{U}^{l_{\mathcal{A}}}$ で与える．$l_{\mathcal{A}} < n$ とすればこのシンドロームは $\boldsymbol{u}$ を圧縮したものとなる．最尤復号を与える写像 g_A を次のように定義する．

$$g_A(\boldsymbol{c}) \equiv \arg \max_{\boldsymbol{u} \in \mathcal{C}_A(\boldsymbol{c})} \mu_U(\boldsymbol{u})$$

このとき，次の補題が成り立つ．

補題 4. 任意の $\delta>0$ に対して十分大きな n を取り，

$$l_{\mathcal{A}} > \frac{nH(U)}{\log|\mathcal{U}|} \tag{4.1}$$

として良い $l_{\mathcal{A}}\times n$ 行列 A を用いることにより，伸長誤り確率を δ 以下に出来る．すなわち

$$\mu_U\left(\{\boldsymbol{u}:\boldsymbol{u}\neq g_A(A\boldsymbol{u})\}\right)<\delta. \tag{4.2}$$

情報源 U に対する無歪固定長符号は図 4 の圧縮器を符号器，補題 4 の伸長器を復号器とすればよい．ここでは，符号の構成のための部品であることを明確にするために，圧縮器・伸長器という用語を用いた．情報源のエントロピーを越える符号化レートを取れば，系列長とともに誤り確率を十分小さくできるような行列 A を用意できることは補題 4 より明らかである．図 4 の多端子(Slepian-Wolf 問題)への拡張については 5.1 節で解説する．

注意. 行列 A の線形性を利用すれば，二元対称通信路に代表される加法的雑音 U を伴う通信路(入力 X, 出力 Y)

$$Y=X+U$$

に対する符号は，補題 4 の系として与えられる．A を正則行列として符号語の集合 $\mathcal{C}_A(\mathbf{0})=\{\boldsymbol{u}:A\boldsymbol{u}=\mathbf{0}\}$ を考える．$|\mathcal{C}_A(\mathbf{0})|=|\mathcal{U}|^{n-l_{\mathcal{A}}}$ であることから，メッセージの集合 $\mathcal{U}^{n-l_A}$ と $\mathcal{C}_A(\mathbf{0})$ を 1 対 1 に対応させる $n\times[n-l_{\mathcal{A}}]$ 行列(生成行列)G が存在し，メッセージ $\boldsymbol{m}\in\mathcal{U}^{n-l_{\mathcal{A}}}$ に対して $\boldsymbol{x}\equiv G\boldsymbol{m}$ を符号語とすることにより通信路の符号器を構成できる．通信路の出力 $\boldsymbol{y}$ は雑音の実現値 $\boldsymbol{u}$ を用いて $\boldsymbol{y}=\boldsymbol{x}+\boldsymbol{u}$ となる．復号器は受信語のシンドローム $A\boldsymbol{y}$ を求めることにより，

$$A\boldsymbol{y}=A[\boldsymbol{x}+\boldsymbol{u}]=A\boldsymbol{u}$$

によって雑音の圧縮された情報を得る．補題 4 より，(4.1) を満たしていれば，$A\boldsymbol{u}$ から小さい誤り確率で $\boldsymbol{u}$ を復元出来るので，

$$\boldsymbol{x}=\boldsymbol{y}-\boldsymbol{u}$$

より通信路入力と対応するメッセージを再生できる．符号化レートは

$$1-\frac{l_{\mathcal{A}}\log|\mathcal{U}|}{n}<1-H(U)$$

となり，$l_{\mathcal{A}}\log|\mathcal{U}|/n$ を $H(U)$ に近づけることにより通信路容量を達成できる．

続いて，図 5 で示されるような複数の行列を用いた復号方式を紹介する．$l_{\mathcal{A}}\times n$ 行列 A と $l_{\mathcal{B}}\times n$ 行列 B を用意し列ベクトル $\boldsymbol{u}\in\mathcal{U}^n$ に対してシンドローム $(A\boldsymbol{u},B\boldsymbol{u})$ を与える．系列 $\boldsymbol{v}$ を条件として与えたときの最尤復号を与える写像 g_{AB} を次のように定義する．

$$g_{AB}(\boldsymbol{c},\boldsymbol{b}|\boldsymbol{v})\equiv\arg\max_{\boldsymbol{u}\in\mathcal{C}_{AB}(\boldsymbol{c},\boldsymbol{b})}\mu_{U|V}(\boldsymbol{u}|\boldsymbol{v})$$

このとき，次の補題が成り立つ．

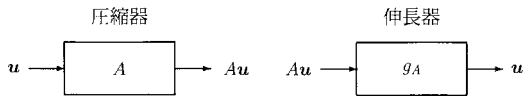

図 4. 無歪み圧縮のための部品(補題 4)．

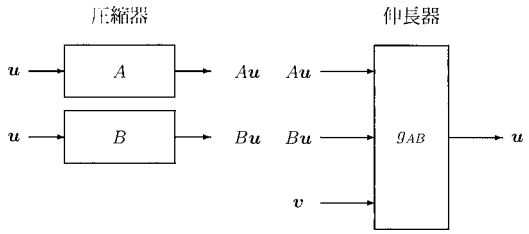

図 5. 無歪み圧縮のための部品 (補題 5).

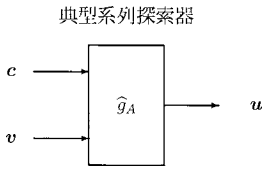

図 6. 典型系列を探索するための部品.

補題 5. 任意の $\delta>0$ に対して十分大きな n を取り,

$$l_{\mathcal{A}}+l_{\mathcal{B}}>\frac{nH(U|V)}{\log|\mathcal{U}|}$$

として良い $l_{\mathcal{A}}\times n$ 行列 A と $l_{\mathcal{B}}\times n$ 行列 B を用いることにより，復号誤り確率を δ 以下に出来る．すなわち

$$\mu_{UV}\left(\{(\boldsymbol{u},\boldsymbol{v}):\boldsymbol{u}\neq g_{AB}(A\boldsymbol{u},B\boldsymbol{u}|\boldsymbol{v})\}\right)<\delta. \tag{4.3}$$

4.2 典型系列を見つけるための部品

ここでは，図 6 で表されるような典型系列を探索する部品を導入する．$l_{\mathcal{A}}\times n$ 行列 A を用意し，系列 $\boldsymbol{v}$ を条件として与えたときの条件つきダイヴァージェンスを最小にする写像 $\widehat{g}_A$ を次のように定義する.

$$\widehat{g}_A(\boldsymbol{c}|\boldsymbol{v})\equiv\arg\min_{\boldsymbol{u}\in\mathcal{C}_A(\boldsymbol{c})}D(\nu_{\boldsymbol{u}|\boldsymbol{v}}\|\mu_{U|V}|\nu_{\boldsymbol{v}})$$

このとき，次の補題が成り立つ.

補題 6. 任意の $\delta,\gamma>0$ に対して十分大きな n を取り,

$$l_{\mathcal{A}}<\frac{nH(U|V)}{\log|\mathcal{U}|}$$

として良い $l_{\mathcal{A}}\times n$ 行列 A とベクトル $\boldsymbol{c}\in\mathrm{Im}\mathcal{A}$ を用いることにより，$\boldsymbol{v}$ を μ_V に従ってランダムに選んだときに $\widehat{g}_A(\boldsymbol{c}|\boldsymbol{v})$ が $\boldsymbol{v}$ の条件つき典型系列にならない確率を δ 以下に出来る．すなわち

$$\mu_V\left(\left\{\boldsymbol{v}:\widehat{g}_A(\boldsymbol{c}|\boldsymbol{v})\notin\mathcal{T}_{U|V,\gamma}(\boldsymbol{v})\right\}\right)<\delta. \tag{4.4}$$

4.3 基本的な部品の組み合わせ

実際の符号の構成では，無歪圧縮のための部品と典型系列を探すための部品を組み合わせて用いる．そのためには行列 A, B とベクトル $\boldsymbol{c}\in \mathrm{Im}\mathcal{A}$ には(4.3)と(4.4)を同時に満たすような性質が要求される．実際，パラメータ $l_{\mathcal{A}}, l_{\mathcal{B}}$ を適切に定めることによりこのような(疎)行列とベクトルを用意できる．

補題 4–6 はアンサンブルのハッシュ性と補題 1, 3 を用いて証明することができる．ただし，後で紹介する符号の存在定理の厳密な証明を行うには，補題 4–6 ではなく補題 1–3 を直接用いなければならない．

4.4 $\boldsymbol{g}, \widehat{\boldsymbol{g}}$ を実現するアルゴリズム

3 節で紹介した疎行列のアンサンブルはハッシュ性を持つので，(4.2)–(4.4)を満たす行列 A, B は疎行列から探すことが出来る．関数 g_A, g_{AB} は最尤復号なので，確率伝搬法や線形計画法などの近似アルゴリズムが利用出来る事が期待される．$\widehat{g}_A$ は一見では最尤復号には見えないが，以下の関係式を用いて最尤復号へ還元できる．

$$\begin{aligned}\arg\min_{\boldsymbol{u}\in\mathcal{C}_A(\boldsymbol{c})} D(\nu_{\boldsymbol{u}|\boldsymbol{v}}\|\mu_{U|V}|\nu_{\boldsymbol{v}}) &= \arg\min_{\boldsymbol{u}\in\mathcal{C}_A(\boldsymbol{c})} D(\nu_{\boldsymbol{u},\boldsymbol{v}}\|\mu_{UV}) \\ &= \arg\max_{\boldsymbol{u}\in\mathcal{C}_A(\boldsymbol{c})} [\log\mu_{UV}(\boldsymbol{u},\boldsymbol{v}) + nH(\nu_{\boldsymbol{u}\boldsymbol{v}})] \\ &= \arg\max_{\nu}\left[nH(\nu) + \max_{\substack{\boldsymbol{u}:\\(\boldsymbol{u},\boldsymbol{v})\in\mathcal{T}_\nu\\ A\boldsymbol{u}=\boldsymbol{c}}} \log\mu_{UV}(\boldsymbol{u},\boldsymbol{v})\right]\end{aligned}$$

ここで，$\mathcal{T}_\nu$ は $\nu_{\boldsymbol{v}}$ が周辺タイプとなる同時タイプ ν を持つ系列の集合であり，最後の等式の右辺の arg は最大値を取る $\boldsymbol{u}$ を与えるものとする．また，タイプ ν の取りうる値は高々 $[n+1]^{|\mathcal{U}||\mathcal{V}|}$ 通りであり，条件 $(\boldsymbol{u},\boldsymbol{v})\in\mathcal{T}_\nu$ は線形制約に過ぎないことに注意．なお，符号の性能が少し劣る可能性があるが，$\widehat{g}_A$ を最尤復号に置き換えても典型系列を見つける事が出来る．

5. 符号の構成

この節では，アンサンブルのハッシュ性を利用した符号の構成を紹介する．この節を通して，φ を符号器，φ^{-1} を復号器とする．系列 $\boldsymbol{x}$, $\boldsymbol{y}$, $\boldsymbol{z}$, $\boldsymbol{w}$ の長さを n とする．

5.1 Slepian-Wolf 問題

ここでは，Slepian-Wolf 問題を考える．Slepian-Wolf 問題とは，図 1 において離れた 2 点にある相関のある情報源 X, Y をそれぞれ φ_X, φ_Y を用いて独立に符号化し，二つの符号器の出力を受信した復号器 φ^{-1} が二つの情報源 (X,Y) を限りなく小さい誤り確率で再生する問題である．レート対 (R_X,R_Y) が以下の不等式を全て満たすことが，誤り確率が 0 に収束する符号が存在する必要十分条件である(Slepian and Wolf, 1973)．

$$\begin{aligned}R_X &\geq H(X|Y)\\ R_Y &\geq H(Y|X)\\ R_X+R_Y &\geq H(X,Y)\end{aligned}$$

なお，Cover (1975)では bin-coding と呼ばれるアンサンブルで符号の存在が証明されており，Csiszár (1982)では行列全体のアンサンブルで符号の存在が証明されている．二元疎行列アンサンブルと最尤復号を用いた符号の存在証明は Muramatsu et al. (2005)にある．

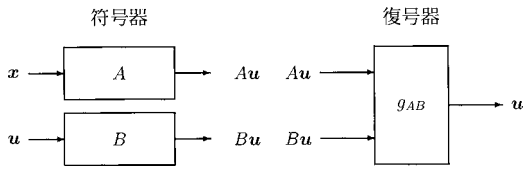

図 7. Slepian-Wolf 符号の構成.

符号器と復号器で共有する(疎)行列

$$A : \mathcal{X}^n \to \mathcal{X}^{l_{\mathcal{A}}}$$
$$B : \mathcal{Y}^n \to \mathcal{Y}^{l_{\mathcal{B}}}$$

を用意し，図 7 で示されるように二つの符号器と復号器

$$\varphi_X : \mathcal{X}^n \to \mathcal{X}^{l_{\mathcal{A}}}$$
$$\varphi_Y : \mathcal{Y}^n \to \mathcal{Y}^{l_{\mathcal{B}}}$$
$$\varphi^{-1} : \mathcal{X}^{l_{\mathcal{A}}} \times \mathcal{Y}^{l_{\mathcal{B}}} \to \mathcal{X}^n \times \mathcal{Y}^n$$

を以下のように定める.

$$\varphi_X(\boldsymbol{x}) \equiv A\boldsymbol{x}$$
$$\varphi_Y(\boldsymbol{y}) \equiv B\boldsymbol{y}$$
$$\varphi^{-1}(\boldsymbol{b}_X, \boldsymbol{b}_Y) \equiv g_{AB}(\boldsymbol{b}_X, \boldsymbol{b}_Y)$$

ここで，g_{AB} は以下の式で与えられる最尤復号器である.

$$g_{AB}(\boldsymbol{b}_X, \boldsymbol{b}_Y) \equiv \arg \max_{(\boldsymbol{x}', \boldsymbol{y}') \in \mathcal{C}_A(\boldsymbol{b}_X) \times \mathcal{C}_B(\boldsymbol{b}_Y)} \mu_{XY}(\boldsymbol{x}', \boldsymbol{y}')$$

符号化レート対 (R_X, R_Y) は以下で与えられる.

$$R_X \equiv \frac{l_{\mathcal{A}} \log |\mathcal{X}|}{n}$$
$$R_Y \equiv \frac{l_{\mathcal{B}} \log |\mathcal{Y}|}{n}$$

誤り確率は $\mathrm{Error}_{XY}(A, B)$ 以下で与えられる.

$$\mathrm{Error}_{XY}(A, B) \equiv \mu_{XY}\left(\left\{(\boldsymbol{x}, \boldsymbol{y}) : \varphi^{-1}(\varphi_X(\boldsymbol{x}), \varphi_Y(\boldsymbol{y})) \neq (\boldsymbol{x}, \boldsymbol{y})\right\}\right)$$

以上の構成に関して以下の定理が成り立つ.

定理 1.（Muramatsu and Miyake, 2008a）定常無記憶情報源 (X, Y) に対してレート対 (R_X, R_Y) が

$$R_X > H(X|Y)$$
$$R_Y > H(Y|X)$$
$$R_X + R_Y > H(X, Y),$$

を満たしていると仮定する．このとき，任意の $\delta>0$ と十分大きな n に対して，

$$\mathrm{Error}_{XY}(A,B)\leq\delta$$

を満たす(疎)行列 $A\in\mathcal{A}$, $B\in\mathcal{B}$ が存在する．

5.2 Wyner-Ziv 問題

ここでは，Wyner-Ziv 問題を考える．Wyner-Ziv 問題とは，図 2 において情報源 X を符号器 φ を用いて符号化し，符号器の出力に加えて X と相関のある補助情報源 Y も受信出来る復号器 φ^{-1} が X と歪み D 以内にある情報 W を再生する問題である．歪み尺度を $\rho:\mathcal{X}\times\mathcal{W}\to[0,\infty)$ として，

$$\rho_{\max}\equiv\max_{x,w}\rho(x,w)<\infty$$

を満たしている事を仮定する．$\boldsymbol{x}\equiv(x_1,\ldots,x_n)$, $\boldsymbol{w}\equiv(w_1,\ldots,w_n)$ に対して $\rho_n(\boldsymbol{x},\boldsymbol{w})$ を

$$\rho_n(\boldsymbol{x},\boldsymbol{w})\equiv\frac{1}{n}\sum_{i=1}^{n}\rho(x_i,w_i)$$

とする．このとき定常無記憶情報源 (X,Y) に対してレート歪み関数 $R_{X|Y}(D)$ は

$$R_{X|Y}(D)=\min_{\substack{\mu_{Y|X},f:\\ E_{XYZ}[\rho(X,f(Y,Z))]\leq D}}[I(X;Z)-I(Y;Z)] \tag{5.1}$$

で与えられる(Wyner and Ziv, 1976)．ここで，上記の最小値は全ての条件付き確率変数 $\mu_{Z|X}$ と関数 $f:\mathcal{Y}\times\mathcal{Z}\to\mathcal{W}$ に渡る最小値であり，(X,Y,Z) の同時確率分布 μ_{XYZ} は

$$\mu_{XYZ}(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z})\equiv\mu_{XY}(\boldsymbol{x},\boldsymbol{y})\mu_{Z|X}(\boldsymbol{z}|\boldsymbol{x}).$$

で与えられる．

最初に条件付き確率分布 $\mu_{Y|X}$ と f を定める．レート歪み関数の最小値を与える $\mu_{Y|X}$ と f をとれば，以下で構成した符号はレート歪み限界を達成する．

$l_{\mathcal{A}}$, $l_{\mathcal{B}}$ を

$$l_{\mathcal{A}}\equiv\frac{n[H(Z|X)-\varepsilon_{\mathcal{A}}]}{\log|\mathcal{Z}|} \tag{5.2}$$

$$\begin{aligned} l_{\mathcal{B}}&\equiv\frac{n[H(Z|Y)-H(Z|X)+\varepsilon_{\mathcal{B}}]}{\log|\mathcal{Z}|}\\ &=\frac{n[I(X;Z)-I(Y;Z)+\varepsilon_{\mathcal{B}}]}{\log|\mathcal{Z}|}. \end{aligned} \tag{5.3}$$

として，符号器と復号器で共有する(疎)行列

$$A:\mathcal{Z}^n\to\mathcal{Z}^{l_{\mathcal{A}}}$$
$$B:\mathcal{Z}^n\to\mathcal{Z}^{l_{\mathcal{B}}}$$

と系列(ベクトル)$\boldsymbol{c}\in\mathcal{Z}^{l_{\mathcal{A}}}$ を用意する．図 8 で示されるように符号器，復号器

$$\varphi:\mathcal{X}^n\to\mathcal{Z}^{l_{\mathcal{B}}}$$
$$\varphi^{-1}:\mathcal{Y}^n\times\mathcal{Z}^{l_{\mathcal{B}}}\to\mathcal{W}^n$$

を次のように定義する．

$$\varphi(\boldsymbol{x})\equiv B\widehat{g}_A(\boldsymbol{c}|\boldsymbol{x})$$

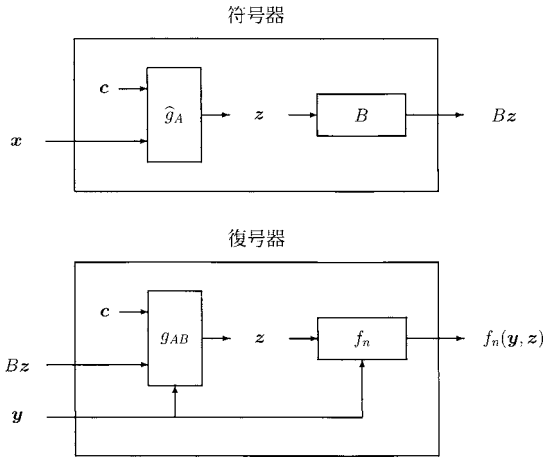

図 8. Wyner-Ziv 符号の構成.

$$\varphi^{-1}(\boldsymbol{b},\boldsymbol{y}) \equiv f_n(g_{AB}(\boldsymbol{c},\boldsymbol{b},\boldsymbol{y}),\boldsymbol{y})$$

ここで,

$$\hat{g}_A(\boldsymbol{c}|\boldsymbol{x}) \equiv \arg \min_{\boldsymbol{z}' \in \mathcal{C}_B(\boldsymbol{c})} D(\nu_{\boldsymbol{x}\boldsymbol{z}'} \| \mu_{Z|X} | \nu_{\boldsymbol{z}})$$

$$g_{AB}(\boldsymbol{c},\boldsymbol{b}|\boldsymbol{y}) \equiv \arg \max_{\boldsymbol{z}' \in \mathcal{C}_{AB}(\boldsymbol{c},\boldsymbol{b})} \mu_{Z|Y}(\boldsymbol{z}'|\boldsymbol{y})$$

であり，$\boldsymbol{y} \equiv (y_1,\ldots,y_n)$, $\boldsymbol{z} \equiv (z_1,\ldots,z_n)$ に対して $f_n(\boldsymbol{y},\boldsymbol{z}) \equiv (w_1,\ldots,w_n)$ を次のように定義する.

$$w_i \equiv f(y_i,z_i)$$

符号化レート R は以下で与えられる.

$$R \equiv \frac{l_{\mathcal{B}} \log |\mathcal{Z}|}{n}.$$

直感的には，符号器にある $\hat{g}_A$ は条件つき典型系列を探す部品であり，行列 B は見つけた条件つき典型系列を無歪圧縮する部品である．そして復号器にある g_{AB} は圧縮した条件つき典型系列を伸長する部品になる．$\boldsymbol{x}$ を与えた時の条件つき典型系列 $\boldsymbol{z}$ が見つかるためには，$\boldsymbol{c}$ のレート [$\boldsymbol{c}$ の長さ]/[$\boldsymbol{x}$ の長さ] は $H(Z|X)$ より小さくなければならない．一方で，$\boldsymbol{c}$, $B\boldsymbol{z}$ と $\boldsymbol{y}$ より $\boldsymbol{z}$ を正しく再生出来るようになるためには，$\boldsymbol{c}$ と $B\boldsymbol{z}$ のレートの和は $H(Z|Y)$ より大きくなければならない．これらを満たすように符号化レートを $H(Z|Y)-H(Z|X)=I(X;Z)-I(Y;Z)$ に近づければ，これは漸近的に最適な符号となる．具体的には以下の定理が成り立つ.

定理 2.（Muramatsu and Miyake, 2008a）(X,Y) を定常無記憶情報源とする．与えられた $\varepsilon_{\mathcal{B}} > \varepsilon_{\mathcal{A}} > 0$ に対して $l_{\mathcal{A}}$, $l_{\mathcal{B}}$ をそれぞれ式(5.2), (5.3)で定めたとき，任意の $\delta > 0$ と十分大きな n に対して

$$R = I(X;Z) - I(Y;Z) + \varepsilon_{\mathcal{B}}$$

$$E_{XY}\left[\rho_n(X^n, \varphi^{-1}(\varphi(X^n),Y^n))\right] \le E_{XYZ}\left[\rho(X,f(Y,Z))\right] + \delta\rho_{\max}$$

を満たす(疎)行列 $A\in\mathcal{A}$, $B\in\mathcal{B}$ とベクトル $\boldsymbol{c}\in\mathrm{Im}A$ が存在する．$\mu_{Z|X}$, f をレート歪み関数の最小値を達成するものにとり，$\varepsilon_{\mathcal{A}},\varepsilon_{\mathcal{B}}\to 0$ とすることにより，提案した符号の性能をレート歪み限界に近づけることができる．

Muramatsu and Miyake (2008a)では $\widehat{g}_A(\boldsymbol{c}|\boldsymbol{x})$ で最尤法を用いているが，証明の方針をほとんど変えずに定理 2 を証明できる．

注意．Martinian and Wainwright (2006b)では，疎行列を用いた Wyner-Ziv 問題の符号が提案されており，Matsunaga and Yamamoto (2003)，Murayama (2004)，Martinian and Wainwright (2006a)，Miyake (2006)で提案された有歪情報源符号を Wyner-Ziv 問題に拡張したものである．ただし，Martinian and Wainwright (2006b)では，一様分布を持つ 2 元情報源 X と加法的な補助情報源 Y を仮定し，歪み尺度にハミング距離を仮定している．Martinian and Wainwright (2006b)では，疎行列を用いた符号器で 'middle layer' と呼ばれる符号語ベクトルを推定する．復号器では符号語ベクトルにもう一つの行列を作用させるだけである．今回提案した方法では，符号語ベクトルを推定するのではなく，再生語ベクトルを行列 A と $\widehat{g}_A$ を用いて推定し，それをもう一つの行列 B を用いて圧縮している(符号語ベクトルと再生語ベクトルの次元が異なることに注意)．そして復号には最尤復号器 g_{AB} が必要である．私達の方法は必ずしも一様とは限らない q 元情報源と必ずしも加法的とは限らない補助情報源，そして一般の歪み尺度に対して漸近的に最適な符号を与えている．

5.3 One-helps-one 問題

ここでは，One-helps-one 問題を考える．One-helps-one 問題とは，図 3 において離れた 2 点にある相関のある情報源 X, Y をそれぞれ φ_X, φ_Y を用いて独立に符号化し，二つの符号器の出力を受信した復号器 φ^{-1} は情報源 X だけを限りなく小さい誤り確率で再生する問題である．ここで，情報源 Y の符号語は X の再生を助ける役割を担っている．定常無記憶情報源 (X,Y) に対して達成可能レート領域は

$$R_X\geq H(X|Z)$$
$$R_Y\geq I(Y;Z),$$

を満たす確率変数 Z が存在するようなレート対 (R_X,R_Y) の集合として与えられる(Wyner, 1973; Wyner and Ziv, 1976)．ここで，μ_{XYZ} の同時分布は

$$\mu_{XYZ}(x,y,z)=\mu_{XY}(x,y)\mu_{Z|Y}(z|y)$$

で与えられる．

条件付き確率分布 $\mu_{Z|Y}$ をあらかじめ定める．$l_{\widetilde{\mathcal{B}}}$, $l_{\mathcal{A}}$, $l_{\mathcal{B}}$ を

$$l_{\widetilde{\mathcal{B}}}\equiv\frac{n[H(X|Z)+\varepsilon_{\widetilde{\mathcal{B}}}]}{\log|\mathcal{X}|} \tag{5.4}$$

$$l_{\mathcal{A}}\equiv\frac{n[H(Z|Y)-\varepsilon_{\mathcal{A}}]}{\log|\mathcal{Z}|} \tag{5.5}$$

$$l_{\mathcal{B}}\equiv\frac{n[I(Y;Z)+\varepsilon_{\mathcal{B}}]}{\log|\mathcal{Z}|}. \tag{5.6}$$

として符号器と復号器で共有する(疎)行列

$$\widetilde{B}:\mathcal{X}^n\to\mathcal{X}^{l_{\widetilde{\mathcal{B}}}}$$
$$A:\mathcal{Z}^n\to\mathcal{Z}^{l_{\mathcal{A}}}$$

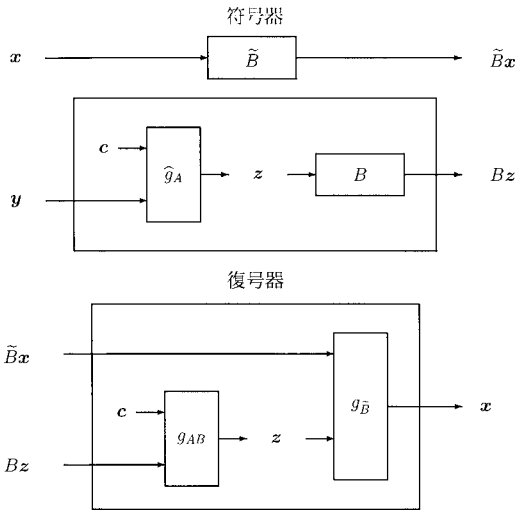

図 9. One-helps-one 問題.

$$B : \mathcal{Z}^n \to \mathcal{Z}^{l_{\mathcal{B}}}$$

と系列(ベクトル)$\boldsymbol{c} \in \mathcal{Z}^{l_{\mathcal{A}}}$ を用意する．図 9 で示されるように二つの符号器と復号器

$$\varphi_X : \mathcal{X}^n \to \mathcal{X}^{l_{\widetilde{\mathcal{B}}}}$$
$$\varphi_Y : \mathcal{Y}^n \to \mathcal{Z}^{l_{\mathcal{B}}}$$
$$\varphi^{-1} : \mathcal{X}^{l_{\widetilde{\mathcal{B}}}} \times \mathcal{Z}^{l_{\mathcal{B}}} \to \mathcal{X}^n$$

を以下のように定める．

$$\varphi_X(\boldsymbol{x}) \equiv \widetilde{B}\boldsymbol{x}$$
$$\varphi_Y(\boldsymbol{y}) \equiv B\widehat{g}_A(\boldsymbol{c}, \boldsymbol{y})$$
$$\varphi^{-1}(\boldsymbol{b}_X, \boldsymbol{b}_Y) \equiv g_{\widetilde{B}}(\boldsymbol{b}_X, g_{AB}(\boldsymbol{c}, \boldsymbol{b}_Y)),$$

ここで，$\widehat{g}_A$, g_{AB}, $g_{\widetilde{B}}$ を以下のように定める．

$$\widehat{g}_A(\boldsymbol{c}|\boldsymbol{y}) \equiv \arg \min_{\boldsymbol{z}' \in \mathcal{C}_A(\boldsymbol{c})} D(\nu_{\boldsymbol{y}\boldsymbol{z}'} \| \mu_{Z|Y} | \nu_{\boldsymbol{y}})$$
$$g_{AB}(\boldsymbol{c}, \boldsymbol{b}_Y) \equiv \arg \max_{\boldsymbol{z}' \in \mathcal{C}_{AB}(\boldsymbol{c}, \boldsymbol{b}_Y)} \mu_Z(\boldsymbol{z}')$$
$$g_{\widetilde{B}}(\boldsymbol{b}_X|\boldsymbol{z}) \equiv \arg \max_{\boldsymbol{x}' \in \mathcal{C}_{\widetilde{B}}(\boldsymbol{b}_X)} \mu_{X|Z}(\boldsymbol{x}'|\boldsymbol{z})$$

符号化レートの対 (R_X, R_Y) は

$$R_X \equiv \frac{l_{\widetilde{\mathcal{B}}} \log |\mathcal{X}|}{n}$$
$$R_Y \equiv \frac{l_{\mathcal{B}} \log |\mathcal{Z}|}{n}$$

で与えられる．復号誤り確率 $\mathrm{Error}_{XY}(A, B, \widetilde{B}, \boldsymbol{c})$ は

$$\mathrm{Error}_{XY}(A, B, \widetilde{B}, \boldsymbol{c}) \equiv \mu_{XY}\left(\left\{(\boldsymbol{x}, \boldsymbol{y}) : \varphi^{-1}(\varphi_X(\boldsymbol{x}), \varphi_Y(\boldsymbol{y})) \neq \boldsymbol{x}\right\}\right)$$

で与えられる.

直感的には, $\boldsymbol{y}$ の符号器にある $\widehat{g}_A$ は条件つき典型系列を探す部品であり, 行列 B は見つけた条件つき典型系列を無歪圧縮する部品である. 一方で, $\boldsymbol{x}$ の符号器にある $\widetilde{B}$ は $\boldsymbol{z}$ との相関を利用して圧縮する部品である. 復号器にある g_{AB} は圧縮した条件つき典型系列を伸長する部品で, これによって $\boldsymbol{y}$ から $\boldsymbol{z}$ を再生する. $g_{\widetilde{B}}$ は再生した $\boldsymbol{z}$ との相関を利用して $\boldsymbol{x}$ を伸長する部品である. $\boldsymbol{y}$ を与えたときの条件つき典型系列 $\boldsymbol{z}$ が見つかるためには, $\boldsymbol{c}$ のレート [$\boldsymbol{c}$ の長さ]/[$\boldsymbol{x}$ の長さ] は $H(Z|Y)$ より小さくなければならない. また, $\boldsymbol{c}$, $B\boldsymbol{z}$ より $\boldsymbol{z}$ を正しく再生出来るようになるためには, $\boldsymbol{c}$ と $B\boldsymbol{z}$ のレートの和は $H(Z)$ より大きくなければならない. これらを満たすように $\boldsymbol{y}$ の符号化レートを $H(Z)-H(Z|Y)=I(Y;Z)$ に近づけることが出来る. 一方で, $\boldsymbol{z}$ を正しく再生できれば $\boldsymbol{x}$ の符号化レート ($\widetilde{B}\boldsymbol{x}$ のレート) を $H(X|Z)$ に近づけることによって $\boldsymbol{x}$ を正しく再生出来る. 具体的には以下の定理が成り立つ.

定理 3. (Muramatsu and Miyake, 2008a) (X,Y) を定常無記憶情報源とする. $\varepsilon_{\mathcal{A}},\varepsilon_{\mathcal{B}},\varepsilon_{\widetilde{\mathcal{B}}}>0$ に対して $l_{\widetilde{\mathcal{B}}}$, $l_{\mathcal{A}}$, $l_{\mathcal{B}}$ をそれぞれ式(5.4), (5.5), (5.6)で定めたとき, 任意の $\delta>0$ と十分大きな n に対して

$$
\begin{aligned}
&R_X = H(X|Z)+\varepsilon_{\widetilde{\mathcal{B}}}\\
&R_Y = I(X;Z)+\varepsilon_{\mathcal{B}}\\
&\mathrm{Error}_{XY}(A,B,\widetilde{B},\boldsymbol{c})\le\delta.
\end{aligned}
$$

を満たす(疎)行列 $A\in\mathcal{A}$, $B\in\mathcal{B}$, $\widetilde{B}\in\widetilde{\mathcal{B}}$ とベクトル $\boldsymbol{c}\in\mathrm{Im}A$ が存在する.

Muramatsu and Miyake (2008a)では $\widehat{g}_A(\boldsymbol{c}|\boldsymbol{x})$ で最尤法を用いているが, 証明の方針をほとんど変えずに定理 3 を証明できる.

6. ランダム符号の統一理論に向けて

本稿では, 疎行列アンサンブルのハッシュ性に注目して, ネットワークを通した情報伝達の基本的な問題である, Slepian-Wolf 問題, Wyner-Ziv 問題, One-helps-one 問題に対する符号の構成を与えた. 提案した符号は理論的には限界性能を達成可能であるが, 疎行列と確率伝搬法や線形計画法等の近似アルゴリズムを用いて実際に動作させたときにどの程度の性能を持つのかを調べることが今後の課題として残されている.

漸近的に最適な符号の存在定理の証明は大きく別けて二つのタイプがある. 一つは Shannon (1948, 1959)にあるランダム符号化論法であり, もう一つは Cover (1975), Csiszár (1982)で代表されるような bin coding と呼ばれるランダム符号化論法である. 漸近的に最適な符号の存在定理は基本的にこれらの二つのランダム符号化論法を組み合わせることによって証明されている.

Shannon の方法は指数的に大きなデータベースのサイズや計算時間が必要のため, 現実的でないと考えられており, 離れた所にある情報源との相関を考慮するような符号化には向いていない. 一方で, bin coding という手法は, 疎行列と確率伝搬法や線形計画法等の近似アルゴリズムが利用でき, 離れた所にある情報源との相関を考慮するような符号化に向いている. ところが, (行列を用いた) bin coding の方法が Shannon のランダム符号化論法へ適用できるかどうかについては Matsunaga and Yamamoto (2003), Martinian and Wainwright (2006a), Martinian and Wainwright (2006b)にあるような特殊な場合を除いて明らかではなく, Gallager (1968)にあるような量子化の方法が必要であった.

本稿で構成する符号は(疎)行列を Shannon の方法へ適応する方法を与えており, 符号の存

在定理はアンサンブルのハッシュ性が本質的であることがわかった．強いハッシュ性に注目した無歪情報源符号に関しては MacKay (2003)，Koga (2007) の結果があるが，疎行列アンサンブルのような弱いハッシュ性に拡張したり，Shannon のランダム符号化論法へ適用できることを明らかにしたのは Muramatsu and Miyake (2008a)，Muramatsu and Miyake (2008b)，Muramatsu and Miyake (2009) の結果が最初である．

我々は，情報理論におけるほとんど全ての漸近的に最適な符号の存在定理がアンサンブルのハッシュ性を仮定するだけで証明できると予想している．これが真実なら，疎行列と近似復号法の組合せでほとんどの符号を実現できることになる．実際，本稿で紹介しなかったいくつかの問題に対する符号の存在定理に関しては Muramatsu and Miyake (2008a, 2008b, 2009) で証明されている．

参 考 文 献

Aji, S. M. and McEliece, R. J. (2000). The generalized distributive law, *IEEE Transactions on Information Theory*, **46**, 325–343.

Carter, J. L. and Wegman, M. N. (1979). Universal classes of hash functions, *Journal of Computer and System Sciences*, **18**, 143–154.

Cover, T. M. (1975). A proof of the data compression theorem of Slepian and Wolf for ergodic sources, *IEEE Transactions on Information Theory*, **21**, 226–228.

Csiszár, I. (1982). Linear codes for sources and source networks: Error exponents, universal coding, *IEEE Transactions on Information Theory*, **28**, 585–592.

Feldman, J., Wainwright, M. J. and Karger, D. R. (2005). Using linear programming to decode binary linear codes, *IEEE Transactions on Information Theory*, **51**, 954–972.

Gallager, R. G. (1968). *Information Theory and Reliable Communication*, John Wiley & Sons, Inc., New York.

Koga, H. (2007). Source coding using families of universal hash functions, *IEEE Transactions on Information Theory*, **53**, 3226–3233.

Kschischang, F. R., Frey, B. J. and Loeliger, H. A. (2001). Factor graphs and the sum-product algorithm, *IEEE Transactions on Information Theory*, **47**, 498–519.

MacKay, D. J. C. (1999). Good error-correcting codes based on very sparse matrices, *IEEE Transactions on Information Theory*, **45**, 399–431.

MacKay, D. J. C. (2003). *Information Theory, Inference, and Learning Algorithms*, Cambridge University Press, Cambridge.

Martinian, E. and Wainwright, M. (2006a). Low density codes achieve the rate-distortion bound, *Proceedings of IEEE Data Compression Coference*, 153–162.

Martinian, E. and Wainwright, M. (2006b). Low-density constructions can achieve the Wyner-Ziv and Gelfand-Pinsker bounds, *Proceedings of 2006 IEEE International Symposium on Information Theory*, 484–488.

Matsunaga, Y. and Yamamoto, H. (2003). A coding theorem for lossy data compression by LDPC codes, *IEEE Transactions on Information Theory*, **49**, 2225–2229.

Miyake, S. (2006). Lossy data compression over Z_q by LDPC code, *Proceedings of 2006 IEEE International Symposium on Information Theory*, 813–816.

Muramatsu, J. and Miyake, S. (2008a). Hash property and coding theorems for sparse matrices and maximal-likelihood coding, submitted to *IEEE Transactions on Information Theory*, available at `arXiv:0801.3878[cs.IT]`, 2007.

Muramatsu, J. and Miyake, S. (2008b). Hash property and fixed-rate universal coding theorems, sub-

mitted to *IEEE Transactions on Information Theory*, available at `arXiv:0804.1183[cs.IT]`, 2008.

Muramatsu, J. and Miyake, S. (2009). Construction of codes for wiretap channel and secret key agreement from correlated source outputs by using sparse matrices, in preparation for submission, available at `arXiv:0903.4014[cs.IT]`, 2009.

Muramatsu, J., Uyematsu, T. and Wadayama, T. (2005). Low density parity check matrices for coding of correlated sources, *IEEE Transactions on Information Theory*, **51**, 3645–3653.

Murayama, T. (2004). Thouless-Anderson-Palmer approach for lossy compression, *Physical Review E*, **69**, 035105 (R).

Shannon, C. E. (1948). A mathematical theory of communication, *Bell System Technical Journal*, **27**, 379–423, 623–656.

Shannon, C. E. (1959). Coding theorems for a discrete source with a fidelity criterion, *IRE National Conventional Record*, **7** (Part 4), 142–163.

Slepian, D. and Wolf, J. K. (1973). Noiseless coding of correlated information sources, *IEEE Transactions on Information Theory*, **19**, 471–480.

Wyner, A. D. (1973). A theorem on the entropy of certain binary sequences and applications II, *IEEE Transactions on Information Theory*, **19**, 772–777.

Wyner, A. D. and Ziv, J. (1973). A theorem on the entropy of certain binary sequences and applications I, *IEEE Transactions on Information Theory*, **19**, 769–771.

Wyner, A. D. and Ziv, J. (1976). The rate-distortion function for source coding with side information at the decoder, *IEEE Transactions on Information Theory*, **22**, 1–10.

Proceedings of the Institute of Statistical Mathematics Vol. 57, No. 2, 203–219 (2009) 219

Hash Property of an Ensemble of Sparse Matrices and Multi-terminal Source Codes

Jun Muramatsu[1] and Shigeki Miyake[2]

[1]NTT Communication Science Laboratories, NTT Corporation
[2]NTT Network Innovation Laboratories, NTT Corporation

The aim of this paper is to construct codes for basic multi-terminal coding problems by using sparse matrices. These problems are the Slepian-Wolf problem, the Wyner-Ziv problem, and the One-helps-one problem. To this end, the notion of a hash property for an ensemble of functions is introduced and asymptotically optimal codes are constructed by using this property. Since an ensemble of q-ary sparse matrices satisfies the hash property, we can construct asymptotically optimal codes by using sparse matrices.

Key words: Information theory, hash property, codes using sparse matrices, Slepian-Wolf problem, Wyner-Ziv problem, one-helps-one problem.