論文の内容の要旨

論文題目　Coding Theorems for Point-to-Point Communication Systems using Sparse Matrix Codes
疎行列を用いた2端子通信系における符号化定理

氏名　Shigeki Miyake　三宅 茂樹

1　まえがき

1990年代の通信路符号におけるターボ符号の発明 [1]，LDPC符号の再発見 [2] 以来シャノン限界に迫る符号化性能と実時間による実行とを両立させる符号を構成することは情報理論の主要なテーマの1つとなっている．

LDPC符号は通信路符号化のみならず無歪みおよび有歪み情報源符号化への適用に関しても研究がなされてきた．情報源を P_U としたとき，無歪み情報源符号化の場合，圧縮レートがブロック長が長くなるにつれてエントロピー限界 $H(U)=\sum_a P_U(a)\log\frac{1}{P_U(a)}$ に近づくときを，また，有歪み情報源符号化の場合，情報源からのメッセージと復号器で復号されたメッセージとの違いの許容度を表す数を D とした際に圧縮レートがブロック長が長くなるにつれてレート・歪み関数 $R(D)=\min_{P_{V|U}:\sum_{a,b}P_{UV}d(a,b)\le D} I(U;V)$ に近づくときを，それぞれの符号は漸近最良性を持つという．一方，通信路符号の場合は通信路を $W_{Y|X}$ としたとき，復号誤り確率がブロック長が長くなるに従って0に近づく際の伝送レートが通信路容量 $C(W_{Y|X})=\max_{P_X} I(X;Y)$ に近づくとき，その符号は漸近最良性を持つという．ただし，$H(U), I(U;V)$ はそれぞれ確率変数 U のエントロピー，確率変数 U および V に関する相互情報量と呼ばれる量である．

Miller と Burshtein [5] はLDPC行列で構成された通信路符号の漸近最良性を，Matsunaga と Yamamoto [4] は有歪み情報源符号の漸近最良性をそれぞれ示した．また，Martinian と Wainwright [3] は多端子系である Wyner-Ziv 系と Gel'fand-Pinsker 系に関して符号を構成し，その漸近最良性を示した．一方で，漸近最良性が示された系は情報源が一様分布であることとか，通信路雑音は付加雑音であることなど，系の統計的な性質に対してある種の対称性が仮定されていた．もし現実的な系に対して漸近最良性を満足する符号を構成する必要が生じた場合，このような仮定は大きな制限となってくる．

本論文は，疎行列を用いて一般の定常無記憶情報源や通信路の符号を構成しその漸近最良性を示す．まず，疎行列の構成法を示し，次いで疎行列で構成されたユニバーサル符号に関して誤り指数を与える．次に有歪み符号を構成し漸近最良性を示し，シミュレーションでその性質を確認する．最後に通信路符号を構成し漸近最良性を示した後で，有歪み情報源符号と組み合わせることで情報源・通信路結合系の符号を構成する．このとき疎行列で構成された符号は，通常のブロック符号で構成された符号よりも少ない最適化の実行回数で実現できることが示される．

分散ビデオ符号化からステガノグラフィまで，多くの応用が見込まれる多端子系は有歪み情報源符号化と通信路符号化との組み合わせで構成されることが多いため，疎行列符号の多端子系への適用も期待される．本論文は，その基礎的部分の検討を行ったものである．

2　疎行列の構成

考察する対象は2端子通信系における符号化，復号化である．符号はアルファベット $[0:q-1]$ 上で行う．ここで，q は素数とする．アルファベットに関しては行列操作が行われるため集合 $[0:q-1]$ には体としての構造が与えられているものと仮定する．従って，以後アルファベットを $[0:q-1]$ と記す代わりに適宜 $GF(q)$ の記法も用いる．また，特に注意しない場合は log の底は q とする．

疎行列とは非ゼロの要素数が0の要素数に比べて小さいものをいう．ここで取り扱う疎行列の構成を次に示す．

[$n\times k$ **疎行列** $\boldsymbol{A}$ **の構成**] t を $O(\log n)$ の偶数の値をとる疎行列パラメータとする．

Step 1: $\boldsymbol{A}$ の全ての要素を0とする．

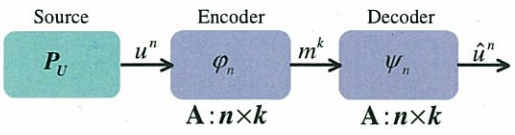

図 1: 無歪み情報源符号化系

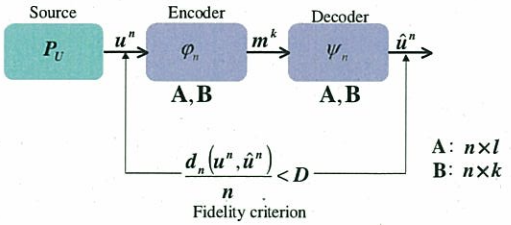

図 2: 有歪み情報源符号化系

各行において次の Step 2 で示す操作を行う.

Step 2: 数 $a \in [1:k]$ および数 $b \in [1:q-1]$ を一様ランダムに取り出す. 次に数 b を a 列にある数字に加える. この際の加法は q を法とする. 以上の操作を t 回繰り返して行い, 次の行に移る.

3 無歪みユニバーサル符号

3.1 問題設定と主定理

図 1 に示す系を考察する. P_U は集合 $GF(q)$ 上の確率分布で, i.i.d. すなわち $P_{U^n}[U^n = u^n] = \prod_{i=1}^n P_U[U_i = u_i]$ が成り立つと仮定する. 符号器 $\varphi_n : GF(q)^n \to GF(q)^k$ は情報源から出力されたメッセージ系列 $u^n \in GF(q)^n$ を符号語 $m^k \in GF(q)^k$ に圧縮する. このとき, 圧縮レート R を $R = k/n$ として定義する. また, 復号器 $\psi_n : GF(q)^k \to GF(q)^n$ は符号語 m^k から元のメッセージ系列を推定し, $\hat{u}^n \in GF(q)^n$ を出力する.

なお, ここで注意すべきことは符号器 φ_n および復号器 ψ_n は情報源の確率分布 P_U の情報を知らないということである. 我々は, この様な条件の下で疎行列を用いて符号器 φ_n, 復号器 ψ_n を構成し, 漸近的に復号誤りが 0 に収束する場合の収束速度を評価する.

まず, 情報源 P_U の属する確率分布族の集合 $\mathcal{P}(\tau)$ を

$$\mathcal{P}(\tau) \stackrel{\text{def}}{=} \left\{ P \in \{GF(q) \text{ 上の i.i.d. 確率分布 }\} \;\middle|\; \min_{a \in [0:q-1]} P(a) > \tau \right\}$$

とする. ただし, τ は正の定数. 次に $n \times k$ 疎行列 $\boldsymbol{A}$ を用いて符号器を $\varphi_n(u^n) \stackrel{\text{def}}{=} u^n \boldsymbol{A}$, 復号器を $\psi_n(m^k) \stackrel{\text{def}}{=} \arg\min_{u^n : u^n \boldsymbol{A} = m^k} H(P_{u^n})$ として構成する. ここで, P_{u^n} は u^n のタイプ (各文字の頻度分布) である. 符号器および復号器は τ を用いていないことに注意する. このとき, 圧縮レート R が予め与えられている際に, 任意の $P \in \mathcal{P}(\tau)$ に対して復号誤り $\sum_{u^n} P(u^n) \mathbf{1}\left[u^n \neq \psi_n(\varphi_n(u^n))\right]$ は次のように評価される.

定理 1 $\mathcal{P}(\tau)$ の部分集合 $\mathcal{P}_\eta(\tau)$ $(0 < \eta < 1)$ を $\mathcal{P}_\eta(\tau) \stackrel{\text{def}}{=} \left\{ P \in \mathcal{P}(\tau) \;\middle|\; H(P) < \eta \right\}$ のように定義する. このとき, 誤り指数

$$\lim_{n\to\infty} \frac{-1}{n} \log \left(\sum_{u^n} P(u^n) \mathbf{1}\left[u^n \neq \psi_n(\varphi_n(u^n))\right] \right) \geq \inf_{\tilde{P} \in \mathcal{P}_{H(P)}(\tau)} \min_{Q} \left[D(Q||\tilde{P}) + |R - H(Q)|^+ \right]$$

が任意の $P \in \mathcal{P}(\tau)$ について成り立つような符号器 φ_n 復号器 ψ_n を構成する疎行列 $\boldsymbol{A}$ は高い確率で存在する. ■

シミュレーション実験の結果については紙面の都合上, 省略する.

4 有歪み情報源符号

4.1 問題設定と主定理

図 2 に示す系を考察する. 情報源 P_U は i.i.d. で, 情報源からの出力を u^n とする. 歪み測度 $d_n : GF(q)^n \times GF(q)^n \to \mathbf{R}^+$ および定数 $D \geq 0$ が与えられた際に, 復号器の出力を $\hat{u}^n$ とすると, $\frac{d_n(u^n,\hat{u}^n)}{n} \leq D$ を満足

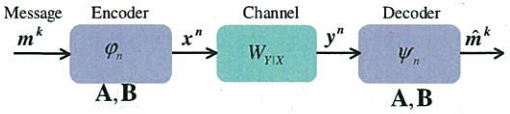

図 3: 通信路符号化系

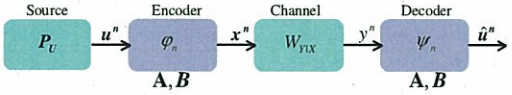

図 4: 情報源・通信路結合符号化系

するような符号器 $\varphi_n : GF(q)^n \to GF(q)^k$ および復号器 $\psi_n : GF(q)^k \to GF(q)^n$ を疎行列を用いて構成したい．このとき次の定理が成り立つ．

定理 2 条件付き確率分布 $P_{V|U}$ を予め与えて固定しておく．十分大きい数 n, l, および k に対して $\frac{l+k}{n} > H(V) + \delta^{1/3}$ および $\frac{l}{n} < H(V|U) - \delta$ を満足する正数 δ が存在するならば，$n \times l$ 疎行列 $\boldsymbol{A}$ および $n \times k$ 疎行列 $\boldsymbol{B}$ を用いて

$$P_{U^n}\left[\frac{d_n\left(U^n, \psi_n\left(\varphi_n(U^n)\right)\right)}{n} > D\right] \to 0 \quad (n \to \infty)$$

を満足する符号器 φ_n および復号器 ψ_n が構成できる． ■

上の定理で存在が示された符号器 φ_n および復号器 ψ_n は次のように構成される．
[符号器の構成] 符号器はベクトル量子化部および圧縮部よりなる．
ベクトル量子化部：情報源からの出力 u^n が与えられたとき，$v^n \stackrel{\text{def}}{=} \arg\max_{\tilde{v}^n : \tilde{v}^n \boldsymbol{A} = c^l} P_{V^n|U^n}(\tilde{v}^n|u^n)$ で定義される v^n を出力する．ここで，$c^l \in GF(q)^l$ は固定された非ゼロの行ベクトルである．
圧縮部：v^n は圧縮部で $m^k \stackrel{\text{def}}{=} v^n \boldsymbol{B}$ のように圧縮・符号化される．
[復号器の構成] 符号語 $m^k \in GF(q)^k$ が与えられたとき，$\hat{u}^n \stackrel{\text{def}}{=} \arg\max_{\substack{\tilde{v}^n : \tilde{v}^n \boldsymbol{A} = c^l \\ \tilde{v}^n \boldsymbol{B} = m^k}} P_{V^n}(\tilde{v}^n)$ で定義されるベクトル量子化 v^n の推定語 $\hat{u}^n$ を出力する．

定理の条件 $\frac{l+k}{n} > H(V) + \delta^{1/3}$ および $\frac{l}{n} < H(V|U) - \delta$ が十分に小さい数 δ に対して成り立っているとする．このとき，$\frac{l+k}{n} = H(V) + 2\delta^{1/3}$ および $\frac{l}{n} = H(V|U) - 2\delta$ とすると，圧縮レート $\frac{k}{n}$ は $I(U;V) + 2(\delta + \delta^{1/3})$ となる．もし，$I(U;V)$ がレート・歪み関数 $R(D)$ に等しいならば，ここで構成した符号は漸近最良性を持つことがいえる．

シミュレーション実験の結果については紙面の都合上，省略する．

5 通信路符号

5.1 問題設定と主定理

図 3 に示す系を考察する．通信路 $W_{Y|X}$ は無記憶定常すなわち，$W_{Y^n|X^n}(y^n|x^n) = \prod_{i=1}^n W_{Y|X}(y_i|x_i)$ と仮定する．このとき，復号誤りを漸近的にいくらでも小さくするような符号器 $\varphi_n : GF(q)^k \to GF(q)^n$ および復号器 $\psi_n : GF(q)^n \to GF(q)^k$ を疎行列を用いて構成したい．このとき次の定理が成り立つ．

定理 3 確率分布 P_X を固定しておく．十分大きい数 n, l, および k に対して $\frac{l+k}{n} < H(X) - \delta$ および $\frac{l}{n} > H(X|Y) + \delta^{1/3}$ を満足する正数 δ が存在するならば，$n \times l$ 疎行列 $\boldsymbol{A}$ および $n \times k$ 疎行列 $\boldsymbol{B}$ を用いて

$$W_{Y^n|X^n}\left(\left(\psi_n^{-1}(m^k)\right)^c | \varphi_n(m^k)\right) \to 0 \ (n \to \infty)$$

を満足する符号器 φ_n および復号器 ψ_n が構成できる． ■

上の定理で存在が示された符号器 φ_n および復号器 ψ_n は次のように構成される．
[符号器の構成] 送りたいメッセージ $m^k \in GF(q)^k$ が与えられたとき，符号語は $\varphi_n(m^k) \stackrel{\text{def}}{=} \arg\max_{\substack{\tilde{x}^n : \tilde{x}^n \boldsymbol{A} = c^l \\ \tilde{x}^n \boldsymbol{B} = m^k}} P_{X^n}(\tilde{x}^n)$ で定義される．
[復号器の構成] 復号器は推定部と復元部よりなる．
推定部：符号語の推定 $\hat{x}^n \stackrel{\text{def}}{=} \arg\max_{\tilde{x}^n : \tilde{x}^n \boldsymbol{A} = c^l} P_{X^n|Y^n}(\tilde{x}^n|y^n)$ を出力する．
復元部：送られたメッセージの推定量 $\hat{m}^k \stackrel{\text{def}}{=} \hat{x}^n \boldsymbol{B}$ を出力する．

定理の条件 $\frac{k-k_0}{n} < H(X)-\delta$ および $\frac{l}{n} > H(X|Y)+\delta^{1/3}$ が十分に小さい数 δ に対して成り立っているとする．このとき，$\frac{k-k_0}{n} = H(X)-2\delta$ および $\frac{l}{n} = H(X|Y)+2\delta^{1/3}$，とすると，伝送レート $\frac{k}{n}$ は $I(X;Y)-2(\delta+\delta^{1/3})$ となる．もし $I(X;Y)$ が通信路容量 $C(W_{Y|X})$ に等しいならば，ここで構成した符号は漸近最良性を持つことがいえる．

5.2 情報源・通信路結合符号化

定理2と定理3とを組み合わせることによって疎行列符号化ならではの興味深い結果が導出される．ここで，図4に示す情報源・通信路結合符号化系を考察する．

系 1 *[情報源・通信路結合線形符号化]* 情報源 P_U，条件付き確率分布 $P_{V|U}$，および通信路 $W_{Y|X}$ が与えられ，$H(V|Y) < H(V|U)$ が成り立つと仮定する．(このとき確率変数 X と V とを同一視した．) 十分大きい数 n および l に対して $H(V|Y)+\delta^{1/3} < \frac{l}{n} < H(V|U)-\delta$ を満足する正数 δ が存在するならば，$n \times l$ 疎行列 $\boldsymbol{A}$ を用いて

$$\sum_{u^n} P_{U^n}(u^n) \sum_{y^n} W_{Y^n|X^n}\left(y^n \mid \varphi_n^{(JL)}(u^n)\right) 1\left[\frac{d_n\left(u^n, \psi_n^{(JL)}(y^n)\right)}{n} > D\right] \to 0 \ (n \to \infty)$$

を満足する符号器 $\varphi_n^{(JL)}$ および復号器 $\psi_n^{(JL)}$ が構成できる．

上記の系で述べていることは，ある条件の下，ベクトル量子化器の出力をそのまま通信路符号とすればよいということである．これによって，与えられた歪み基準と通信路に対して従来に比較して単純な符号が疎行列を用いて構成できることがわかる．

6 まとめ

疎行列を用いて，無歪みユニバーサル符号，有歪み情報源符号および通信路符号を構成し，無歪みユニバーサル符号に関しては復号誤り指数を求め，また，有歪み情報源符号および通信路符号に関しては，構成した符号が漸近最良性を持つことを示した．疎行列を用いて符号を構成することによって，sum-product 法や線形計画法など効率的なアルゴリズムで近似的に実現できることが期待される．

参考文献

[1] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo codes," *Proc. 1993 Int. Conf. Commun.*, pp. 1064-1070, 1993.

[2] D.J.C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, **vol. 45**, no. 2, pp. 399-431, 1999.

[3] E. Martinian and M. J. Wainwright, "Low-density constructions can achieve the Wyner-Ziv and Gelfand-Pinsker bounds," *Proc. 2006 IEEE Int. Symp. Inform. Theory*, pp. 484-488, 2006.

[4] Y. Matsunaga and H. Yamamoto, "A coding theorem for lossy data compression by LDPC codes," *IEEE Trans. Inform. Theory*, **vol. 49**, no. 9, pp. 2225-2229, 2003.

[5] G. Miller and D. Burshtein, "Bounds on the maximum-likelihood decoding error probability of low-density parity-check codes," *IEEE Trans. Information. Theory*, **vol. 47**, no. 7, pp. 2696-2710, 2001.