

Cover の conjecture に関連した結果

山口大・理工, 東南大学 陳 漢武 (Han Wu Chen)

山口大・工 柳 研二郎 (Kenjiro Yanagi)

1 ガウス型通信路

次のようなフィードバックをもつ離散時間ガウス型通信路を考える.

$$Y_n = S_n + Z_n, \quad n = 1, 2, \dots,$$

ただし $Z = \{Z_n; n = 1, 2, \dots\}$ は雑音を表す退化していない平均 0 のガウス過程、 $S = \{S_n; n = 1, 2, \dots\}$ と $Y = \{Y_n; n = 1, 2, \dots\}$ はそれぞれ入力信号と出力信号を表す確率過程である. 通信路は雑音のかからないフィードバックをもつとする. したがって S_n は送信するメッセージと出力信号 $Y_1, \dots, Y_{n-1}$ の関数であるとして表される. レート R , 長さ n の符号語 $x^n(W, Y^{n-1})$, $W \in \{1, \dots, 2^{nR}\}$ と復号関数 $g_n: \mathbb{R}^n \rightarrow \{1, 2, \dots, 2^{nR}\}$ に対して、誤り確率は

$$Pe^{(n)} = Pr\{g_n(Y^n) \neq W; Y^n = x^n(W, Y^{n-1}) + Z^n\},$$

で定義される. ただし W は $\{1, 2, \dots, 2^{nR}\}$ 上の一様分布で雑音 $Z^n = (Z_1, Z_2, \dots, Z_n)$ とは独立である. 入力信号には平均電力制限が課せられる. つまり

$$\frac{1}{n} \sum_{i=1}^n E[S_i^2] \leq P$$

である. またフィードバックは causal である. つまり $S_i (i = 1, 2, \dots, n)$ は $Z_1, \dots, Z_{i-1}$ に従属している. 同様にフィードバックがない場合は $S_i (i = 1, 2, \dots, n)$ は $Z^n = (Z_1, Z_2, \dots, Z_n)$ と独立である.

紙面の都合で途中の経過は省略するが、最終的には有限ブロック長容量は次のように定義される.

$$C_{n,FB}(P) = \max \frac{1}{2n} \log \frac{|R_X^{(n)} + R_Z^{(n)}|}{|R_Z^{(n)}|},$$

ただし $|\cdot|$ は行列式を表し、最大値は

$$Tr[(I + B)R_X^{(n)}(I + B^t) + BR_Z^{(n)}B^t] \leq nP$$

を満たす狭義下三角行列 B と 非負対称行列 $R_X^{(n)}$ についてとる. 同様にフィードバックがないときには容量 $C_n(P)$ は $B = 0$ としたときの最大値である. これらの条件の下で Cover and Pombra [2] は次の結果を得た.

Proposition 1 任意の $\epsilon > 0$ に対して各 $n = 1, 2, \dots$ でブロック長 n で $2^{n(C_{n,FB}(P)-\epsilon)}$ 個の符号語が存在して $n \rightarrow \infty$ のとき $Pe^{(n)} \rightarrow 0$ とできる. 逆に任意の $\epsilon > 0$ とブロック長 n で $2^{n(C_{n,FB}(P)+\epsilon)}$ 個の符号語からなる任意の符号の列に対しても $Pe^{(n)} \rightarrow 0$ ($n \rightarrow \infty$) が成り立たない. これはフィードバックをもたない場合も成り立つ.

ここではブロック長 n を固定したとき $C_{n,FB}(P)$ と $C_n(P)$ との間の関係に興味がある. $C_n(P)$ は Gallager [5] によって正確に求められている.

Proposition 2

$$C_n(P) = \frac{1}{2n} \sum_{i=1}^k \log \frac{nP + r_1 + \dots + r_k}{kr_i},$$

ただし $0 < r_1 \leq r_2 \leq \dots \leq r_n$ は $R_Z^{(n)}$ の固有値、 $k(\leq n)$ は $nP + r_1 + \dots + r_k > kr_k$ を満たす最大整数である.

ところで $C_{n,FB}(P)$ は正確には得られないので、今まで多くの人々によって様々な形の上界が得られている ([4], [7], [2]). 以下簡単のため $R_X^{(n)}, R_Z^{(n)}, \dots$ をそれぞれ $R_X, R_Z, \dots$ のように (n) を省略して用いる.

Theorem 1

$$C_n(P) \leq C_{n,FB}(P) \leq 2C_n(P).$$

Theorem 2

$$C_n(P) \leq C_{n,FB}(P) \leq C_n(P) + \frac{1}{2}.$$

2 Conjecture

最近 Cover [3] により次のような conjecture が出されている.

Theorem 3 (open problem)

$$C_n(P) \leq C_{n,FB}(P) \leq C_n(2P).$$

この conjecture は $n = 2$ のとき成り立つことを示す. つまり

Theorem 4

$$C_2(P) \leq C_{2,FB}(P) \leq C_2(2P).$$

以下その略証を示す.

$n = 2$ のとき $C_{2,FB}(P)$ は次のように与えられる. ただし

$$R_Z = \begin{pmatrix} k & m \\ m & \ell \end{pmatrix}, k, \ell > 0, k\ell > m^2 \neq 0$$

$$R_X = \begin{pmatrix} a & c \\ c & b \end{pmatrix}, a, b \geq 0, ab \geq c^2$$

$$B = \begin{pmatrix} 0 & 0 \\ t & 0 \end{pmatrix}$$

とする. このとき Ihara and Yanagi [6] によってつぎの結果が得られている.

Proposition 3

$$e^{4C_{2,FB}(P)} = \max_{0 \leq a \leq 2P} \frac{(a+k)(b+\ell) - (|m| - \sqrt{ab})^2}{k\ell - m^2},$$

ただし max は

$$b = \frac{(2P-a)(a+k)}{k},$$

$$c = -\sqrt{ab} \ (m > 0),$$

$$c = \sqrt{ab} \ (m < 0),$$

$$t = -\frac{c}{a+k}$$

で与えられる.

a について最大をとる前の式の分子を書き直すと次のようになる.

$$\begin{aligned}
 & (a+k)(b+\ell) - (|m| - \sqrt{ab})^2 \\
 = & \ell a + kb + k\ell - m^2 + 2|m|\sqrt{ab} \\
 = & \ell a + kb + k\ell - m^2 + \frac{2|m|}{\sqrt{k\ell}} \sqrt{\ell a \cdot kb} \\
 \leq & \ell a + kb + k\ell - m^2 + \frac{|m|}{\sqrt{k\ell}} (\ell a + kb) \\
 = & (1 + \frac{|m|}{\sqrt{k\ell}}) (\ell a + kb) + k\ell - m^2 \\
 \leq & 2(\ell a + kb) + k\ell - m^2.
 \end{aligned}$$

ここで

$$\begin{aligned}
 & \ell a + kb \\
 = & \ell a + (2P - a)(a + k) \\
 = & -a^2 + (2P + \ell - k)a + 2Pk \\
 = & -\{a - (P + \frac{\ell - k}{2})\}^2 + (P + \frac{\ell - k}{2})^2 + 2Pk \\
 = & -\{a - (P + \frac{\ell - k}{2})\}^2 \\
 & + P^2 + (k + \ell)P + \frac{(k - \ell)^2}{4}.
 \end{aligned}$$

次の3通りの場合が考えられる.

(1) $0 < P \leq (k - \ell)/2$ のとき, $a = 0, b = 2P$ で最大となり,

$$(1 + \frac{|m|}{\sqrt{k\ell}})2Pk + k\ell - m^2 < 4Pk + k\ell - m^2.$$

(2) $0 < P \leq (\ell - k)/2$ のとき, $a = 2P, b = 0$ で最大となり,

$$(1 + \frac{|m|}{\sqrt{k\ell}})2P\ell + k\ell - m^2 < 4P\ell + k\ell - m^2.$$

(3) $P \geq (k - \ell)/2$ 又は $P \geq (\ell - k)/2$ のとき,

$$\begin{aligned}
 a &= P + \frac{\ell - k}{2}, \\
 b &= (P + \frac{k - \ell}{2})(P + \frac{k + \ell}{2})/k \\
 &= \frac{P^2}{k} + P + \frac{k^2 - \ell^2}{4k}
 \end{aligned}$$

で最大となり,

$$\begin{aligned} & \left(1 + \frac{|m|}{\sqrt{k\ell}}\right) \left\{P^2 + (k + \ell)P + \frac{(k - \ell)^2}{4}\right\} + k\ell - m^2 \\ & < 2P^2 + 2(k + \ell)P + \frac{(k - \ell)^2}{2} + k\ell - m^2. \end{aligned}$$

次に $e^{4C_2(2P)}$ の分子を計算すると

(a) $16P^2 \leq (k - \ell)^2 + 4m^2$ のとき

$$2P\{k + \ell + \sqrt{(k - \ell)^2 + 4m^2}\} + k\ell - m^2.$$

(b) $16P^2 > (k - \ell)^2 + 4m^2$ のとき

$$4P^2 + 2(k + \ell)P + \frac{(k + \ell)^2}{4}.$$

ここで

(1) と (a) の比較

$$\begin{aligned} & k + \ell + \sqrt{(k - \ell)^2 + 4m^2} - 2k \\ & = \ell - k + \sqrt{(k - \ell)^2 + 4m^2} > 0. \end{aligned}$$

(2) と (a) の比較

$$\begin{aligned} & k + \ell + \sqrt{(k - \ell)^2 + 4m^2} - 2\ell \\ & = k - \ell + \sqrt{(k - \ell)^2 + 4m^2} > 0. \end{aligned}$$

(3) と (a) の比較

$$\begin{aligned} & 2P\{k + \ell + \sqrt{(k - \ell)^2 + 4m^2}\} + k\ell - m^2 \\ & \geq 2P\{k + \ell + \sqrt{16P^2}\} + k\ell - m^2 \\ & = 8P^2 + 2(k + \ell)P + k\ell - m^2 \end{aligned}$$

これより

$$\begin{aligned} & 8P^2 + 2(k + \ell)P + k\ell - m^2 \\ & - \left\{2P^2 + 2(k + \ell)P + \frac{(k - \ell)^2}{2} + k\ell - m^2\right\} \\ & = 6P^2 - \frac{(k - \ell)^2}{2} \\ & \geq 6 \cdot \frac{(k - \ell)^2}{4} - \frac{(k - \ell)^2}{2} \\ & = (k - \ell)^2 \geq 0. \end{aligned}$$

(1) と (b) の比較

$$\begin{aligned}
& 4P^2 + 2(k + \ell)P + \frac{(k + \ell)^2}{4} \\
& - 4kP - (k\ell - m^2) \\
= & 4P^2 + 2(\ell - k)P + \frac{(k - \ell)^2}{4} - (k\ell - m^2) \\
= & 4\left(P + \frac{\ell - k}{4}\right)^2 - \frac{(k - \ell)^2}{4} + \frac{(k + \ell)^2}{4} \\
& - k\ell + m^2 \\
= & 4\left(P + \frac{\ell - k}{4}\right)^2 + m^2 > 0.
\end{aligned}$$

(2) と (b) の比較

$$\begin{aligned}
& 4P^2 + 2(k + \ell)P + \frac{(k + \ell)^2}{4} - 4\ell P \\
& - (k\ell - m^2) \\
= & 4P^2 + 2(k - \ell)P + \frac{(k + \ell)^2}{4} - (k\ell - m^2) \\
= & 4\left(P + \frac{k - \ell}{4}\right)^2 - \frac{(k - \ell)^2}{4} + \frac{(k + \ell)^2}{4} \\
& - k\ell + m^2 \\
= & 4\left(P + \frac{k - \ell}{4}\right)^2 + m^2 > 0.
\end{aligned}$$

(3) と (b) の比較

$$\begin{aligned}
& 4P^2 + 2(k + \ell)P + \frac{(k + \ell)^2}{4} \\
& - 2P^2 - 2(k + \ell)P - \frac{(k - \ell)^2}{2} - (k\ell - m^2) \\
= & 2P^2 + \frac{(k + \ell)^2 - 2(k - \ell)^2 - 4k\ell}{4} + m^2 \\
= & 2P^2 - \frac{(k - \ell)^2}{4} + m^2 \\
\geq & 2 \cdot \frac{(k - \ell)^2}{4} - \frac{(k - \ell)^2}{4} + m^2 \\
= & \frac{(k - \ell)^2 + 4m^2}{4} > 0.
\end{aligned}$$

以上より $C_2(P) \leq C_{2,FB}(P) \leq C_2(2P)$.

参考文献

- [1] H. W. Chen and K. Yanagi, "On the Cover's conjecture on capacity of Gaussian channel with feedback", IEICE Trans. Fundamentals, vol E80-A, pp 2272-2275, November 1997.
- [2] T. Cover and S. Pombra, "Gaussian feedback capacity", IEEE Trans. Information Theory, vol IT-35, pp 37-43, January 1989.
- [3] T. Cover and B. Gopinath, Open problems in communication and computation, Springer-Verlag, New York, 1987.
- [4] P. Ebert, "The capacity of the Gaussian channel with feedback", Bell. Syst. Tech. J., vol 49, pp 1705-1712, 1970.
- [5] R. G. Gallager, Information theory and reliable communication, John Wiley and Sons, New York, 1968.
- [6] S. Ihara and K. Yanagi, "Capacity of discrete time Gaussian channel with and without feedback, II", Japan J. Appl. Math., vol 6, pp 245-258, 1989.
- [7] M. Pinsker, talk delivered at the Soviet Information Theory Meeting, (no abstract published), 1969.
- [8] K. Yanagi, "ガウス型通信路の最近の問題について", 京都大学数理解析研究所研究集会「応用函数解析の研究」(1996.6.17-6.18), 講究録, vol 975, pp 1-13, 1996.