# Universal Coding for Correlated Sources with Memory

Tomohiko Uyematsu

*Abstract*— **Universal coding problem for the system of Slepian and Wolf (the SW-system) has first been investigated by Csiszár and Körner. They considered the correlated memoryless sources, and established a universally attainable error exponent as a function of rate pair $(R_1, R_2)$ that is positive whenever $(R_1, R_2)$ is an inner point of the admissible rate region of the SW-system, which is specified depending on what source statistic is given. However, when the sources have their memory, the universal coding problem for the SW-system remains open, in spite of its importance. In this paper we shall deal with such a universal coding problem for the SW-system. Especially, when the sources are ergodic Markov sources, we show that there exists a sequence of universal code such that the probability of decoding error vanishes whenever $(R_1, R_2)$ is an inner point of the admissible rate region.**

*Keywords*— **Slepian-Wolf coding system, universal coding, correlated Markov source, information spectrum**

## I. Introduction

The separate coding problem for correlated sources has first been posed and investigated by Slepian and Wolf[1]. This problem may be regarded as a substantial starting point of multi-user information theory. On the other hand, the problem of *universal* coding for the system is not only interesting in its own right but also very important from the standpoint of practical applications[2]. By universal coding we mean that neither encoding nor decoding depends on particular source statistics, while the coding performance approaches asymptotically the same one as attained when we know the source statistics underlying the system. Universal coding problem for the system of Slepian and Wolf (*the SW-system*) has first been investigated by Csiszár and Körner[3]. They considered the correlated memoryless sources, and established a universally attainable error exponent as a function of rate pair $(R_1, R_2)$ that is positive whenever $(R_1, R_2)$ is an inner point of the admissible rate region of the SW-system (*the SW-region*), which is specified depending on what source statistic is given. However, when the sources have their memory, the universal coding problem for the SW-system remains open except that Csiszár conjectured the existence of the universal code for Markov sources[4, section V].

In this paper we shall deal with a universal coding problem for the SW-system. Especially, when the sources are ergodic Markov sources, we show that there exists a sequence of universal code such that the probability of decoding error vanishes whenever $(R_1, R_2)$ is an inner point of the SW-region. Our result is different from Csiszár's conjecture in the following points. (1) In [4], Csiszár suggested to prove the result by using Markov-type of the sequence[5]. But, we prove the theorem by using the information-spectrum method developed by Han[6]. (2) We also show that such universal code can be constructed algebraically.

This work was supported in part by Japan Society for the Promotion of Science (JSPS) under Grant JSPS-RFTF97P00601.

T. Uyematsu is with the department of Communications and Integrated Systems, Tokyo Institute of Technology, Tokyo 152-8552, Japan. E-mail: uematsu@it.ss.titech.ac.jp

## II. Main Result

Let $\mathcal{X}$ and $\mathcal{Y}$ be arbitrary finite sets. For any positive integer $n$, consider a correlated ergodic Markovian sequences $(X^n, Y^n) = (X_1X_2\cdots X_n, Y_1Y_2\cdots Y_n)$ that takes values in $\mathcal{X}^n \times \mathcal{Y}^n$. Suppose that the joint distribution of the sequence $(X^n, Y^n)$ is described by $Q^n$. The Slepian-Wolf coding system can be stated as follows. The sequences $X^n$ and $Y^n$ emitted from the correlated sources are separately encoded into $f_n(X^n)$ and $g_n(Y^n)$, respectively, and the decoder $\varphi_n$ observes them to reproduce the estimates of $(X^n, Y^n)$, where $f_n$ and $g_n$ are the encoder functions defined by

$$f_n : \mathcal{X}^n \to \mathcal{M}_1 = \{1, 2, \cdots, |\mathcal{M}_1|\},$$
$$g_n : \mathcal{Y}^n \to \mathcal{M}_2 = \{1, 2, \cdots, |\mathcal{M}_2|\},$$

and satisfies the rate constraints

$$\frac{1}{n}\log|\mathcal{M}_1| \le R_1 + \gamma \quad \frac{1}{n}\log|\mathcal{M}_2| \le R_2 + \gamma,$$

for an arbitrary positive number $\gamma$. The decoder function $\varphi_n$ is defined by

$$\varphi_n : \mathcal{M}_1 \times \mathcal{M}_2 \to \mathcal{X}^n \times \mathcal{Y}^n.$$

We call the triples $(f_n, g_n, \varphi_n)$ as a code for the SW-system. The error probability of decoding is

$$\begin{aligned} & P_e^n(f_n, g_n, \varphi_n, Q) \\ &= \Pr(\varphi_n(f_n(X^n), g_n(Y^n)) \neq (X^n, Y^n)) \\ &= \sum_{\substack{(x^n,y^n)\in\mathcal{X}^n\times\mathcal{Y}^n: \\ \varphi_n(f_n(x^n),g_n(y^n))\neq(x^n,y^n)}} Q^n(x^n, y^n). \end{aligned}$$

Then, the next theorem is our main result.

*Theorem 1:* For any ergodic Markov source with a fixed order $k$ and a distribution $Q$, there exists a sequence of universal codes $\{(f_n, g_n, \varphi_n)\}_{n=1}^{\infty}$ with rate $(R_1, R_2)$ such that if $(R_1, R_2)$ is within the SW-region of the source, i.e. $R_1 > H(X|Y)$, $R_2 > H(Y|X)$ and $R_1 + R_2 > H(X,Y)$, then the error probability of decoding satisfies

$$\lim_{n\to\infty} P_e^n(f_n, g_n, \varphi_n, Q) = 0,$$

where $H(X,Y)$ denotes the joint entropy of the sources, while $H(X|Y)$ and $H(Y|X)$ denote the conditional entropies of the sources.

The next corollary is a strong version of Theorem 1.

*Corollary 1:* For any ergodic Markov source with a fixed order $k$ and a distribution $Q$, we can algebraically construct a universal codes $(f_n, g_n, \varphi_n)$ with rate $(R_1, R_2)$. Further, the encoding/decoding complexity of the code is at most $O(n^3)$, and if $(R_1, R_2)$ is within the SW-region of the source, then the error probability of decoding satisfies $\lim_{n\to\infty} P_e^n(f_n, g_n, \varphi_n, Q) = 0$.

## III. Proof

For simplicity, we prove the theorem for ergodic Markov source with order one ($k = 1$). Proof for the higher order can be done similarly.

*Step.1 Approximation of probability distribution*
Let $\Omega(\mathcal{Z})$ be a set of probability distributions of Markov sources over a finite alphabet $\mathcal{Z} = \{1, 2, \cdots, |\mathcal{Z}|\}$. For a given probability distribution $Q \in \Omega(\mathcal{Z})$ and any positive integer $n$, we consider the following approximation of $Q$. Let

$$\begin{aligned} F(i) &\triangleq \left\lfloor \frac{1}{2} + n^2 \sum_{k=1}^{i} Q(k) \right\rfloor \quad i = 1, 2, \cdots, |\mathcal{Z}|, \\ G(i|j) &\triangleq \left\lfloor \frac{1}{2} + n^2 \sum_{k=1}^{i} Q(k|j) \right\rfloor \quad i, j = 1, 2, \cdots, |\mathcal{Z}|, \end{aligned}$$

where $\lfloor x \rfloor$ denotes the maximum integer less than or equal to $x$. It should be noted that both $F(i)$ and $G(i|j)$ take integer values between 0 and $n^2 - 1$. Next, we define the approximation $\hat{Q}$ of $Q$ by

$$\begin{aligned} \hat{Q}(i) &\triangleq \frac{F(i) - F(i-1)}{n^2} \quad i = 1, 2, \cdots, |\mathcal{Z}|, \\ \hat{Q}(i|j) &\triangleq \frac{G(i|j) - G(i-1|j)}{n^2} \quad i, j = 1, 2, \cdots, |\mathcal{Z}|. \end{aligned}$$

Then, we have the following Lemma.

*Lemma 1:* For any positive integer $n$ and $Q \in \Omega(\mathcal{Z})$,

$$\sum_{z^n \in \mathcal{Z}^n} |\hat{Q}^n(z^n) - Q^n(z^n)| \le \frac{|\mathcal{Z}|}{n}. \tag{1}$$

*Proof:* By using the inequality $x - 1 < \lfloor x \rfloor \le x$, we have

$$|\hat{Q}(i) - Q(i)| < \frac{1}{n^2} \quad i = 1, 2, \cdots, |\mathcal{Z}|.$$

Similarly, we also have

$$|\hat{Q}(i|j) - Q(i|j)| < \frac{1}{n^2} \quad i, j = 1, 2, \cdots, |\mathcal{Z}|.$$

Therefore,

$$\begin{aligned} &\sum_{z^n \in \mathcal{Z}^n} |\hat{Q}^n(z^n) - Q^n(z^n)| \\ &\le \sum_{z^{n-1} \in \mathcal{Z}^{n-1}} \sum_{z' \in \mathcal{Z}} \{|\hat{Q}(z'|z^{n-1})\hat{Q}(z^{n-1}) \\ &\quad -Q(z'|z^{n-1})\hat{Q}(z^{n-1})| \\ &\quad +|Q(z'|z^{n-1})\hat{Q}(z^{n-1}) - Q(z'|z^{n-1})Q(z^{n-1})|\} \\ &\le \sum_{z^{n-1} \in \mathcal{Z}^{n-1}} \hat{Q}(z^{n-1}) \sum_{z' \in \mathcal{Z}} |\hat{Q}(z'|z^{n-1}) - Q(z'|z^{n-1})| \\ &\quad + \sum_{z^{n-1} \in \mathcal{Z}^{n-1}} \sum_{z' \in \mathcal{Z}} Q(z'|z^{n-1})|\hat{Q}(z^{n-1}) - Q(z^{n-1})| \\ &\le \frac{|\mathcal{Z}|}{n^2} + \sum_{z^{n-1} \in \mathcal{Z}^{n-1}} |Q(z^{n-1}) - Q(z^{n-1})|. \end{aligned}$$

By repeating this reduction, we have (1). ■

Next lemma is a direct consequence of Lemma 1.

*Lemma 2:* For any positive integer $n$, there exists a subset $D_n(\mathcal{Z})$ of $\Omega(\mathcal{Z})$ satisfying the following two conditions:

(1) $|D_n(\mathcal{Z})| \le (n^2 + 1)^{|\mathcal{Z}| + |\mathcal{Z}|^2}$.

(2) For any $Q \in \Omega(\mathcal{Z})$, there exists a $\hat{Q} \in D_n(\mathcal{Z})$ such that

$$\sum_{z^n \in \mathcal{Z}^n} |\hat{Q}(z^n) - Q(z^n)| < \frac{|\mathcal{Z}|}{n}.$$

*Step.2 Mixture of Markov sources*
Now, we develop an information-spectrum method proposed by Han[6].

For arbitrary fixed number $\delta > 0$, define $\hat{\Omega}(R_1, R_2, \delta)$ as

$$\begin{aligned} \hat{\Omega}(R_1, R_2, \delta) \triangleq \{Q \in \Omega(\mathcal{X} \times \mathcal{Y}) : &H(X|Y) < R_1 - \delta, \\ &H(Y|X) < R_2 - \delta, \text{ and} \\ &H(X,Y) < R_1 + R_2 - \delta\} \end{aligned}$$

Further, we define $\hat{D}_n(R_1, R_2, \delta)$ as

$$\hat{D}_n(R_1, R_2, \delta) \triangleq \hat{\Omega}(R_1, R_2, \delta) \cap D_n(\mathcal{X} \times \mathcal{Y}).$$

Then, consider the mixture $P_{XY}^n$ given by

$$\begin{aligned} P_{XY}^n(x^n, y^n) &\triangleq \frac{1}{M} \sum_{Q \in \hat{D}_n(R_1, R_2, \delta)} Q^n(x^n, y^n), \\ &\quad \forall (x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n, \end{aligned} \tag{2}$$

with $M \triangleq |\hat{D}_n(R_1, R_2)|$. From Lemma 2, we note that

$$M \le (n^2 + 1)^{|\mathcal{X}||\mathcal{Y}| + |\mathcal{X}|^2|\mathcal{Y}|^2}.$$

Next lemma is well-known.

*Lemma 3:* [7] An ergodic Markov source has exponential rates for entropy, i.e. for any $Q \in \Omega(\mathcal{Z})$ with entropy $H$ and for any $\epsilon > 0$

$$\sum_{\substack{z^n \in \mathcal{Z}^n: \\ 2^{-n(H+\epsilon)} \le Q(z^n) \le 2^{-n(H-\epsilon)}}} Q(z^n) \ge 1 - 2^{-nr(n,\epsilon)}$$

where $r(n,\epsilon)$ is bounded away from zero.

From the definition of $\hat{\Omega}(R_1, R_2, \delta)$ and Lemma 3 for any $Q \in \hat{D}_n(R_1, R_2, \delta)$, we have

$$\begin{aligned} & Q^n\left\{\frac{1}{n}\log\frac{1}{P^n_{X|Y}(X^n|Y^n)} \ge R_1 - \delta/2\right\} \\ \le\ & Q^n\left\{\frac{1}{n}\log\frac{1}{Q^n_{X|Y}(X^n|Y^n)} + \frac{1}{n}\log M \ge R_1 - \delta/2\right\} \\ \le\ & 2^{-nr(n,\delta/3)} \end{aligned}$$

for sufficiently large $n$. This implies that

$$\begin{aligned} & P^n_{XY}\left\{\frac{1}{n}\log\frac{1}{P^n_{X|Y}(X^n|Y^n)} \ge R_1 - \delta/2\right\} \\ \le\ & \frac{1}{M}\sum_{Q \in \hat{D}_n(R_1,R_2,\delta)} Q^n\left\{\frac{1}{n}\log\frac{1}{Q^n_{X|Y}(X^n|Y^n)}\right. \\ & \left. + \frac{1}{n}\log M \ge R_1 - \delta/2\right\} \\ \le\ & 2^{-nr(n,\delta/3)}, \end{aligned} \tag{3}$$

for sufficiently large $n$. Similarly, we have

$$P^n_{XY}\left\{\frac{1}{n}\log\frac{1}{P^n_{Y|X}(Y^n|X^n)} \ge R_2 - \delta/2\right\} \le 2^{-nr(n,\delta/3)}, \tag{4}$$

and

$$P^n_{XY}\left\{\frac{1}{n}\log\frac{1}{P^n_{XY}(X^n,Y^n)} \ge R_1 + R_2 - \delta/2\right\} \le 2^{-nr(n,\delta/3)}, \tag{5}$$

for sufficiently large $n$.

*Step.3 Construction of codes*
The mixture $P^n_{XY}$ defined by (2) can be regarded as a general source introduced in [6] (see also [8]). For general source $P^n_{XY}$, we employ the following fundamental lemma.

*Lemma 4* (Miyake-Kanaya[8]) For a general source $P^n_{XY}$, an arbitrary pair of rates $(R_1, R_2)$ and any $n = 1, 2, \cdots$, there exists a sequence of code $(f_n, g_n, \varphi_n)$ such that

$$\begin{aligned} & P^n_e(f_n, g_n, \varphi_n, P^n_{XY}) \\ \le\ & 3 \times 2^{-n\gamma} + \Pr\left\{\frac{1}{n}\log\frac{1}{P^n_{X|Y}(X^n|Y^n)} \ge R_1 - \gamma\right. \\ & \text{or } \frac{1}{n}\log\frac{1}{P^n_{Y|X}(Y^n|X^n)} \ge R_2 - \gamma \\ & \left.\text{or } \frac{1}{n}\log\frac{1}{P^n_{XY}(X^n,Y^n)} \ge R_1 + R_2 - \gamma\right\} \end{aligned} \tag{6}$$

where $\gamma > 0$ is arbitrary.

By choosing $\gamma = \delta/2$ and combining this lemma with (3),(4) and (5), we can show that there exists a code $(f_n, g_n, \varphi_n)$ for the mixture $P^n_{XY}$ such that its probability of decoding error satisfies

$$P^n_e(f_n, g_n, \varphi_n, P^n_{XY}) \le 3 \times 2^{-nr(n,\delta/3)} + 3 \times 2^{-n\delta/2},$$

for sufficiently large $n$.

*Step.4 Proof of universality*
Lastly, we show that the sequence of codes $\{(f_n, g_n, \varphi_n)\}$ obtained in the previous step satisfies the assertion of the theorem. Consider the probability distribution $Q \in \hat{\Omega}(R_1, R_2, \delta)$ Then, there exists a probability distribution $\hat{Q} \in \hat{D}_n(R_1, R_2, \delta)$ such that two conditions in Lemma 2 are satisfied. Hence, for sufficiently large $n$,

$$\begin{aligned} & P^n_e(f_n, g_n, \varphi_n, Q) \\ =\ & \sum_{\substack{(x^n,y^n) \in \mathcal{X}^n \times \mathcal{Y}^n \\ \varphi_n(f_n(x^n), g_n(y^n)) \ne (x^n,y^n)}} Q^n(x^n, y^n) \\ \le\ & \sum_{\substack{(x^n,y^n) \in \mathcal{X}^n \times \mathcal{Y}^n \\ \varphi_n(f_n(x^n), g_n(y^n)) \ne (x^n,y^n)}} \hat{Q}^n(x^n, y^n) \\ & + \sum_{\substack{(x^n,y^n) \in \mathcal{X}^n \times \mathcal{Y}^n \\ \varphi_n(f_n(x^n), g_n(y^n)) \ne (x^n,y^n)}} |\hat{Q}^n(x^n, y^n) - Q^n(x^n, y^n)| \\ \le\ & M P^n_e(f_n, g_n, \varphi_n, P^n_{XY}) \\ & + \sum_{(x^n,y^n) \in \mathcal{X}^n \times \mathcal{Y}^n} |\hat{Q}^n(x^n, y^n) - Q^n(x^n, y^n)| \\ \le\ & 3M2^{-nr(n,\delta/3)} + 3M2^{-n\delta/2} + \frac{|\mathcal{X}||\mathcal{Y}|}{n} \\ \le\ & 3(n^2+1)^{|\mathcal{X}||\mathcal{Y}| + |\mathcal{X}|^2|\mathcal{Y}|^2}(2^{-nr(n,\delta/3)} + 2^{-n\delta/2}) \\ & + \frac{|\mathcal{X}||\mathcal{Y}|}{n}. \end{aligned}$$

Therefore, for any $Q \in \hat{\Omega}(R_1, R_2, \delta)$, the probability of decoding error vanishes.

Lastly, by choosing $\delta > 0$ depending on $n$ such that the following three conditions are satisfied,

(1) $\lim_{n\to\infty} \delta = 0$

(2) $\lim_{n\to\infty} n\,\delta = \infty$

(3) $\lim_{n\to\infty} n\,r(n, \delta/3) = \infty$

then we obtain Theorem 1.

Corollary 1 can be immediately obtained by using the following lemma instead of Lemma 4.

*Lemma 5:* For a general source $P^n_{XY}$, an arbitrary pair of rates $(R_1, R_2)$ and any $n = 1, 2, \cdots$, we can algebraically construct a code $(f_n, g_n, \varphi_n)$ such that the encoding/decoding complexity of the code is at most $O(n^3)$, and that the probability of error satisfies

$$\begin{aligned} & P^n_e(f_n, g_n, \varphi_n, P^n_{XY}) \\ & \le \quad 3\alpha 2^{-n\gamma} + \alpha \Pr\left\{ \frac{1}{n} \log \frac{1}{P^n_{X|Y}(X^n|Y^n)} \ge R_1 - \gamma \right. \\ & \qquad \text{or } \frac{1}{n} \log \frac{1}{P^n_{Y|X}(Y^n|X^n)} \ge R_2 - \gamma \\ & \qquad \left. \text{or } \frac{1}{n} \log \frac{1}{P^n_{XY}(X^n, Y^n)} \ge R_1 + R_2 - \gamma \right\}, \end{aligned} \qquad (7)$$

where $\alpha$ is a constant independent of $P^n_{XY}$ and $\gamma > 0$ is arbitrary.

The construction method of such codes is described in Appendix. The proof of this lemma can be done in a manner similar to [9, Theorem 3].

## Appendix

In what follows, $\mathcal{X}$ and $\mathcal{Y}$ are supposed to be Galois fields, and $|\mathcal{X}|$ and $|\mathcal{Y}|$ are assumed to be powers of two. Otherwise, we add some dummy symbols with zero probability. Further, $\mathcal{X}^m$ and $\mathcal{Y}^m$ are considered as the structure of the extended field of $\mathcal{X}$ and $\mathcal{Y}$, respectively. For any positive integer $n$ and $k_1 (\le n)$, define the decomposition $n = k_1 t_1 + m_1$ with $t_1 = \lceil n/k_1 \rceil - 1$ and $1 \le m_1 \le k_1$. Then, $x \in \mathcal{X}^n$ can be rewritten as $x = (x_0, \cdots, x_{t_1})$, where $x_0 \in \mathcal{X}^{m_1}$ and $x_i \in \mathcal{X}^{k_1}$, $i = 1, \cdots, t_1$. To any choice of elements $\gamma_i \in \mathcal{X}^{k_1}$, $i = 1, \cdots, t_1$, we associate the linear encoder $f : \mathcal{X}^n \to \mathcal{X}^{k_1}$ given by

$$f(x) = \psi(x_0) + \sum_{i=1}^{t_1} \gamma_i x_i,$$

and define $C(n, k_1, \mathcal{X})$ to be the set of all such encoders, where $\psi(z)$ denotes the $k_1$-dimensional vector formed by adding $k_1 - m_1$ zeros after the $m_1$-dimensional components of $z$. In a similar manner, we also define the set $C(n, k_2, \mathcal{Y})$ of encoders $g : \mathcal{Y}^n \to \mathcal{Y}^{k_2}$ with $t_2 = \lceil n/k_2 \rceil - 1$.

*Encoding scheme:* Denote all pairs of mapping in $C(n, k_1, \mathcal{X}) \times C(n, k_2, \mathcal{Y})$ as $(f_i, g_i)$, $i = 1, \cdots, N$ with $N = |\mathcal{X}|^{k_1 t_1} \cdot |\mathcal{Y}|^{k_2 t_2}$. Then, consider the following fixed length code with block length $N_o = nN$, where $n$ is an even integer.

1) A given pair $(x, y) \in \mathcal{X}^{nN} \times \mathcal{Y}^{nN}$ is first represented in the form $x = (x_1, \cdots, x_N)$ with $x_i \in \mathcal{X}^n$, $i = 1, \cdots, N$ and $y = (y_1, \cdots, y_N)$ with $y_i \in \mathcal{Y}^n$, $i = 1, \cdots, N$. Then encode each pairs $(x_i, y_i)$ into $(f_i(x_i), g_i(y_i)) \in \mathcal{X}^{k_1} \times \mathcal{Y}^{k_2}$ for $i = 1, \cdots, N$.
2) Encode $x$ and $y$ into $H_1 x \in \mathcal{X}^{n(N-K_1)}$ and $H_2 y \in \mathcal{Y}^{n(N-K_2)}$, where $H_1$ (resp. $H_2$) denotes the parity check matrices of the algebraic geometry code $C_H(N, K_1, D_1)$ over $\mathcal{X}^n$ (resp. $C_H(N, K_2, D_2)$ over $\mathcal{Y}^n$) constructed from a generalized Hermitian curve [10].

The encoded sequences consist of $N$ pairs of $(f_i(x_i), g_i(y_i))$ and a pair of $(H_1 x, H_2 y)$, and this corresponds to the overall encoders $F : \mathcal{X}^{N_o} \to \mathcal{X}^{k_1 N + n(N-K_1)}$ and $G : \mathcal{Y}^{N_o} \to \mathcal{Y}^{k_2 N + n(N-K_2)}$. □

Further, let us define rates of codes by

$$\begin{aligned} r_1 &\triangleq (k_1/n) \log |\mathcal{X}|, \quad r_2 \triangleq (k_2/n) \log |\mathcal{Y}|, \\ \tilde{r}_1 &\triangleq (1 - K_1/N) \log |\mathcal{X}|, \quad \tilde{r}_2 \triangleq (1 - K_2/N) \log |\mathcal{Y}|, \end{aligned}$$

then the overall rates of the proposed linear encoders $F$ and $G$ are given by $R_1 = r_1 + \tilde{r}_1$ and $R_2 = r_2 + \tilde{r}_2$, respectively.

*Decoding scheme:*

1) For $i = 1, \cdots, N$, decode $(f_i(x_i), g_i(y_i))$ by using the method proposed by Miyake and Kanaya [8, Section 4.1], and obtain the estimate $(\hat{x}_i, \hat{y}_i) \in \mathcal{X}^n \times \mathcal{Y}^n$. Then, the overall estimate $(\hat{x}, \hat{y}) \in \mathcal{X}^{nN} \times \mathcal{Y}^{nN}$ of the encoded sequence can be described as $\hat{x} = (\hat{x}_1, \cdots, \hat{x}_N)$ and $\hat{y} = (\hat{y}_1, \cdots, \hat{y}_N)$.
2) From two syndromes $s_1 \triangleq H_1 x - H_1 \hat{x}$ and $s_2 \triangleq H_2 y - H_2 \hat{y}$, find the vectors $e_1 \in \mathcal{X}^{nN}$ and $e_2 \in \mathcal{Y}^{nN}$ such that $H_1 e_1 = s_1$ and $H_2 e_2 = s_2$. These vectors can be obtained efficiently by using the error correcting procedure of algebraic geometry code. Then, $(\tilde{x}, \tilde{y}) = (\hat{x} - e_1, \hat{y} - e_2)$ is the final estimate of the encoded pair. □

## References


[1] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. on Inform. Theory*, vol.IT-19, pp.471-480, July, 1973.

[2] Y. Oohama, "Universal coding for correlated sources with linked encoders," *IEEE Trans. on Inform. Theory*, vol.42, pp.837-847, May 1996.

[3] I. Csiszár and J. Körner, "Towards a general theory of source networks," *IEEE Trans. on Inform. Theory*, vol.IT-26, pp.155-165, 1980.

[4] I. Csiszár , "Linear codes for source and source networks: error exponents, universal coding," *IEEE Trans. on Inform. Theory*, vol.IT-28, pp.585-592, 1982.

[5] G. Longo and A. Sgarro, "The source coding theorem revisited: A combinatorial approach," *IEEE Trans. on Inform. Theory*, vol.IT-25, pp.544-548, 1979.

[6] T. S. Han, *Information-spectrum methods in information theory*, Baifukan, Tokyo, 1998 (in Japanese).

[7] P. C. Shields, *The ergodic theory of discrete sample paths*, American Math. Society, 1996.

[8] S. Miyake and F. Kanaya, "Coding theorems on correlated general sources," *IEICE Trans. on Fundamentals*, vol.E78-A, No.9, pp.1063-1070, Sep., 1995.

[9] T. Uyematsu, "An Algebraic Construction of Codes for Slepian-Wolf Source Networks," submitted to *IEEE Trans. on Inform. Theory*.

[10] B.-Z. Shen, "A Justesen construction of binary concatenated codes that asymptotically meet the Zyablov bound for low rate," *IEEE Trans. on Inform. Theory*, vol.39, pp.239-242, 1993.