Fifty-third Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
September 29 - October 2, 2015

Linear Code Duality Between Channel Coding and Slepian–Wolf Coding

Lele Wang and Young-Han Kim
Department of Electrical and Computer Engineering
University of California, San Diego
La Jolla, CA 92093, USA
{lew001,yhk}@ucsd.edu

***Abstract*—We study the duality between channel coding and Slepian–Wolf coding in the linear coding framework. We show how a code (both its encoder and decoder) for a *symmetric* channel coding problem can be used to design a code for a general Slepian–Wolf problem. Conversely, we show how a code for a *symmetric* Slepian–Wolf problem can be used to design a code for a general channel coding problem. The exact relations between the rates and the probability of errors of the two codes are established.**

I. Introduction

A. Channel Coding Problem

A binary-input memoryless channel (BMC) $p(y|x)$ consists of an input alphabet $\mathcal{X} = \{0,1\}$, a finite output alphabet $\mathcal{Y}$, and a collection of conditional probability mass functions $p(y|x)$ on $\mathcal{Y}$ for $x \in \{0,1\}$. We say a BMC $p(y|x)$ is *symmetric* if there exists a permutation $\pi\colon \mathcal{Y} \to \mathcal{Y}$ such that $p(y|x) = p(\pi(y)|x \oplus 1)$ for all $y \in \mathcal{Y}$ and $x \in \{0,1\}$.

A (k, n, ϵ) code (f, ϕ) for the BMC $p(y|x)$ consists of

- a codebook $\mathcal{C} \subseteq \{0,1\}^n$ of size $|\mathcal{C}| = 2^k$,
- an encoder $f\colon \mathcal{C} \to \{0,1\}^n$ that maps each codeword c^n to a channel input $x^n = f(c^n)$, and
- a decoder $\phi\colon \mathcal{Y}^n \to \mathcal{C}$ that assigns a codeword estimate $\hat{c}^n = \phi(y^n)$ to each received sequence y^n.

We assume that C^n is uniform over the codebook $\mathcal{C}$. The rate of the code is $R_{\text{ch}} = k/n$. The average probability of error of the code is $\mathsf{P}\{\hat{C}^n \neq C^n\} = \epsilon$.

We say a channel code is *linear* if the codebook $\mathcal{C}$ is such that for any two codewords $c^n, \tilde{c}^n \in \mathcal{C}$, $c^n \oplus \tilde{c}^n \in \mathcal{C}$. Equivalently, a linear code can be defined by its parity check matrix $H_{(n-k)\times n}$. For notational convenience, we introduce the augmented parity check matrix $\bar{H}_{n\times n} = \left[\begin{smallmatrix} 0 \\ H \end{smallmatrix}\right]$ so that all vectors in this paper are of length n. Thus, the codebook of a linear code can be written as $\mathcal{C} = \{c^n\colon \bar{H}c^n = 0^n\}$. When a (k, n, ϵ) code (f, ϕ) is linear with associated augmented parity check matrix $\bar{H}$ and $f(c^n) = c^n$, we say it is a (k, n, ϵ) linear code $(\bar{H}, \phi)$.

B. Slepian–Wolf Problem

A Slepian–Wolf problem $p(x, y)$ consists of two finite alphabets $\mathcal{X} = \{0,1\}, \mathcal{Y}$, and a joint pmf $p(x, y)$ over $\{0,1\} \times \mathcal{Y}$. The binary memoryless source X with side information Y generates a jointly i.i.d. random process $\{(X_i, Y_i)\}$ with $(X_i, Y_i) \sim p_{X,Y}(x_i, y_i)$. We say a Slepian–Wolf problem $p(x, y)$ is *symmetric* if $X \sim \text{Bern}(1/2)$ and the channel $p(y|x)$ is symmetric.

An (l, n, ϵ) code (g, ψ) for the Slepian–Wolf problem $p(x, y)$ consists of

- an index set $\mathcal{I} \subseteq \{0,1\}^n$ of size $|\mathcal{I}| = 2^l$,
- an encoder $g\colon \{0,1\}^n \to \mathcal{I}$ that maps each source sequence x^n to an index $s^n = g(x^n)$, and
- a decoder $\psi\colon \mathcal{I} \times \mathcal{Y}^n \to \{0,1\}^n$ that assigns a source estimate $\hat{x}^n = \psi(s^n, y^n)$ to each index s^n and side information sequence y^n.

The rate of the code is $R_{\text{sw}} = (n - k)/n$. The average probability of error of the code is $\mathsf{P}\{\hat{X}^n \neq X^n\} = \epsilon$.

We say a Slepian–Wolf code is *linear* if for any $x^n, \tilde{x}^n \in \{0,1\}^n$, $g(x^n) \oplus g(\tilde{x}^n) = g(x^n \oplus \tilde{x}^n)$. When an (l, n, ϵ) Slepian–Wolf code (g, ψ) is linear with an encoder defined by matrix multiplication $g(x^n) = \bar{H}x^n$, where $\bar{H}_{n\times n} = \begin{bmatrix} 0 \\ H_{l\times n} \end{bmatrix}$, we say it is an (l, n, ϵ) linear code $(\bar{H}, \psi)$.

C. Background

The connection between the channel coding problem and the Slepian–Wolf problem has long been observed in the literature. In [1], Wyner showed that a linear (k, n, ϵ) code for the binary symmetric channel with crossover probability p (BSC(p)) can be used to construct a linear $(n - k, n, \epsilon)$ code for the symmetric Slepian–Wolf problem $p(x, y)$ where $p(y|x)$ is a BSC(p). Since then, several attempts have been made to generalize this observation [2]–[11]. In [8], Chen, He, Jagmohan, Lastras-Montano, and Yang related a general Slepian–Wolf problem $p(x, y)$ to a dual channel coding problem $p_{V|U}(v|u)$, where $V = (U \oplus X, Y)$ and $(X, Y) \sim p(x, y)$ is independent of U. Under the maximum *a posteriori* decoding, a linear (k, n, ϵ) code for the dual channel $p(v|u)$ can be used to design a linear $(n-k, n, \epsilon)$ code for the Slepian–Wolf problem $p(x, y)$. Miyake [9] studied this duality for sparse matrix codes with minimum-entropy decoding. Such duality were also established for some low-complexity codes, such as LDPC codes with density evolution decoding [10] and polar codes with successive cancellation decoding [11]. In all of these results except [1], the duality was established only for the encoder, i.e., the encoder of one code is treated as a black

978-1-5090-1824-6/15/$31.00 ©2015 IEEE

box in designing another code. However, one has to specify the decoding rule to analyze the probability of error.

D. Contributions

In this paper, we investigate whether the duality result can be established for a given encoder and decoder pair. Given a linear (k, n, ϵ) symmetric channel code $(\bar{H}, \phi)$, how can we construct a general Slepian–Wolf code and what can we say about its performance (in terms of rate and probability of error)? Conversely, given a linear (l, n, ϵ) symmetric Slepian–Wolf code $(\bar{H}, \psi)$, how can we construct a general channel code and what can we say about its performance? The motivation is to translate the performance of commercial off-the-shelf codes that are well studied and simulated in one communication scenario into the performance of codes for another communication scenario. From the theoretical point of view, such a linear code duality will generalize most existing results and will unify the analysis.

The main results of this paper are summarized in Figure 1. We first show how to construct a linear $(n-k, n, \epsilon)$ symmetric Slepian–Wolf code from a linear (k, n, ϵ) symmetric channel code in Section II-A and a general $(n-k, n, \epsilon)$ Slepian–Wolf code from a linear $(n-k, n, \epsilon)$ symmetric Slepian–Wolf code in Section II-B. Next we show how to construct a (k, n, ϵ) symmetric channel code from a linear $(n-k, n, \epsilon)$ symmetric Slepian–Wolf code in Section II-C and a (k, n, ϵ) general channel code from a linear (k, n, ϵ) symmetric channel code in Section II-D. By combining all four results, we establish the duality between the general Slepian–Wolf problem and the general channel coding problem.

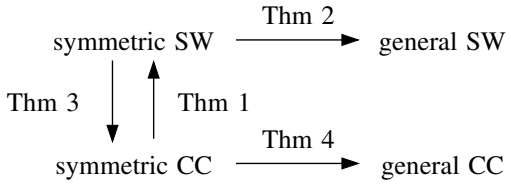

Fig. 1. A summary of the main results. SW is short for Slepian–Wolf coding and CC is short for channel coding.

II. Linear Code Duality

A. A Symmetric Slepian–Wolf Code from a Symmetric Channel Code

Suppose that for the symmetric BMC $p(y|x)$ with permutation π, there is a linear (k, n, ϵ) code $(\bar{H}, \phi)$. Without loss of generality, assume that the augmented parity check matrix is systematic

$$\bar{H} = \begin{bmatrix} 0 & 0 \\ A & I_{n-k} \end{bmatrix},$$

where A is an $(n-k) \times k$ matrix and I_{n-k} is the $(n-k) \times (n-k)$ identity matrix. The block diagram for this problem is shown in Figure 2. We have the average probability of error is given by

$$\mathsf{P}\{\phi(\tilde{R}^n) \neq \tilde{C}^n\} = \epsilon.$$

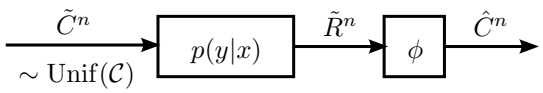

Fig. 2. A channel code for symmetric BMC $p(y|x)$.

To construct a code for the symmetric Slepian–Wolf problem $p(x, y)$ from the above channel code, we first introduce two building blocks.

The first block, termed *codify*, takes two inputs, a binary sequence x^n and the syndrome $\bar{H}x^n$ of it, and outputs the element-wise modulo-two sum of the two inputs $x^n \oplus \bar{H}x^n$, as depicts in the left part of Figure 3. Intuitively, this operation shifts any binary sequence x^n to a codeword, as illustrated in the right part of Figure 3. We prove this in Lemma 1.

Lemma 1. *For any $x^n \in \{0,1\}^n, x^n \oplus \bar{H}x^n \in \mathcal{C}$.*

Proof. For any $x^n \in \{0,1\}^n$, we have

$$\begin{aligned} \bar{H}(x^n \oplus \bar{H}x^n) &= \bar{H}x^n \oplus \begin{bmatrix} 0 & 0 \\ A & I \end{bmatrix} \bar{H}x^n \\ &\overset{(a)}{=} \begin{bmatrix} 0 \\ Hx^n \end{bmatrix} \oplus \begin{bmatrix} 0 & 0 \\ A & I \end{bmatrix} \begin{bmatrix} 0 \\ Hx^n \end{bmatrix} \\ &= \begin{bmatrix} 0 \\ Hx^n \end{bmatrix} \oplus \begin{bmatrix} 0 \\ Hx^n \end{bmatrix} \\ &= 0, \end{aligned}$$

where $H = [A, I]$ in (a). Therefore, $x^n \oplus \bar{H}x^n \in \mathcal{C}$. □

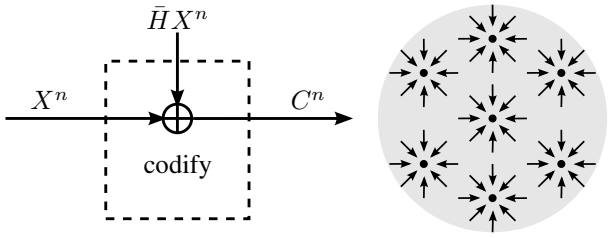

Fig. 3. The codify block. Left: The block diagram. Right: Illustration of a shift by $\bar{H}X^n$ in $\{0,1\}^n$ space.

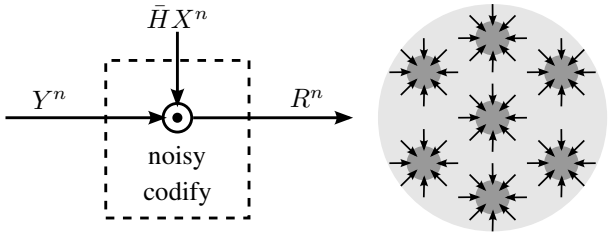

Fig. 4. The noisy codify block. Left: The block diagram. Right: Illustration of a shift by $\bar{H}X^n$ in $\mathcal{Y}^n$ space.

The second block, termed *noisy codify*, takes two inputs, the noisy observation y^n of the binary sequence x^n and the

syndrome $\bar{H}x^n$, and outputs $y^n \odot \bar{H}x^n$, which is defined as follows. For $y \in \mathcal{Y}$ and $s \in \{0,1\}$,

$$y \odot s = \begin{cases} y & \text{if } s = 0 \\ \pi(y) & \text{if } s = 1. \end{cases}$$

Let $y^n \odot s^n$ be the element-wise $\odot$ operation. The left part of Figure 4 depicts the block diagram. Similar to the shift in the codify operation, this block takes a *corresponding shift* in $\mathcal{Y}^n$ space and outputs a *noisy version* of the output sequence in the codify block, as illustrated in the right part of Figure 4. Lemma 2 makes this statement rigorous.

Lemma 2. *Let (X^n, Y^n) be i.i.d. according to $p(x,y)$, where $p(x,y)$ is symmetric under permutation π. Let $C^n = X^n \oplus \bar{H}X^n$ and $R^n = Y^n \odot \bar{H}X^n$. Then,*

$$\mathsf{P}\{C^n = c^n, R^n = r^n\} = \frac{1}{2^k} \prod_{i=1}^{n} p_{Y|X}(r_i|c_i)$$

for every $c^n \in \mathcal{C}$ and $r^n \in \mathcal{Y}^n$.

Proof. Define $\mathcal{S} = \{s^n \in \{0,1\}^n : s^k = 0^k\}$. For any $c^n \in \mathcal{C}$,

$$\begin{aligned}
&\mathsf{P}\{C^n = c^n\} \\
&= \sum_{s^n \in \mathcal{S}} \mathsf{P}\left\{X^n \oplus \bar{H}X^n = c^n, \bar{H}X^n = s^n\right\} \\
&= \sum_{s^n \in \mathcal{S}} \mathsf{P}\left\{X^n = c^n \oplus s^n\right\} \mathsf{P}\left\{\bar{H}X^n = s^n | X^n = c^n \oplus s^n\right\} \\
&\overset{(b)}{=} \sum_{s^n \in \mathcal{S}} \frac{1}{2^n} \\
&= \frac{1}{2^k},
\end{aligned}$$

where (b) follows since X^n is i.i.d. $\mathrm{Bern}(1/2)$ and for any $c^n \in \mathcal{C}$ and $s^n \in \mathcal{S}$, $\bar{H}(c^n \oplus s^n) = 0^n \oplus \begin{bmatrix} 0 & 0 \\ A & I \end{bmatrix} \begin{bmatrix} 0^k \\ s_{k+1}^n \end{bmatrix} = s^n$. Now, for any $r^n \in \mathcal{Y}^n$, consider

$$\begin{aligned}
&\mathsf{P}\{R^n = r^n | C^n = c^n\} \\
&= \sum_{s^n \in \mathcal{S}} \mathsf{P}\left\{\bar{H}X^n = s^n, Y^n \odot \bar{H}X^n = r^n | C^n = c^n\right\} \\
&= \sum_{s^n \in \mathcal{S}} \mathsf{P}\left\{\bar{H}X^n = s^n | C^n = c^n\right\} \\
&\quad \cdot \mathsf{P}\left\{Y^n \odot s^n = r^n | \bar{H}X^n = s^n, X^n = c^n \oplus s^n\right\} \\
&= \sum_{s^n \in \mathcal{S}} \mathsf{P}\left\{\bar{H}X^n = s^n | C^n = c^n\right\} \\
&\quad \cdot \mathsf{P}\{Y^n = r^n \odot s^n | X^n = c^n \oplus s^n\} \\
&= \sum_{s^n \in \mathcal{S}} \mathsf{P}\left\{\bar{H}X^n = s^n | C^n = c^n\right\} \prod_{i=1}^{n} p_{Y|X}(r_i \odot s_i | c_i \oplus s_i) \\
&\overset{(c)}{=} \sum_{s^n \in \mathcal{S}} \mathsf{P}\left\{\bar{H}X^n = s^n | C^n = c^n\right\} \prod_{i=1}^{n} p_{Y|X}(r_i | c_i) \\
&= \prod_{i=1}^{n} p_{Y|X}(r_i | c_i),
\end{aligned}$$

where (c) follows from the symmetry of the channel $p(y|x)$. □

Lemma 2 implies that if Y^n is the output of the channel $p(y|x)$ when the channel input is X^n. Then, the output the noisy codify block, R^n, distributes as if it is the output of the same channel $p(y|x)$ when the channel input is the codified sequence C^n. This is illustrated in Figure 5.

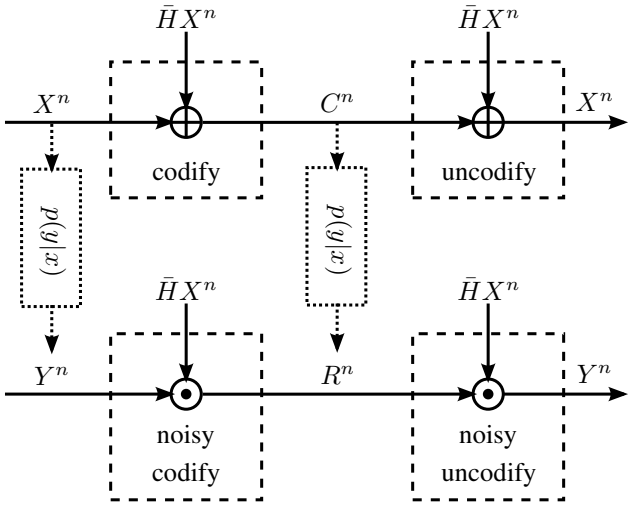

Fig. 5. Relations of the random variables (X^n, Y^n, C^n, R^n). To recover (the top right) X^n from (the bottom left) Y^n, one can go through the path $Y^n \to R^n \to C^n \to X^n$. To get an estimate $\hat{C}^n$ from R^n, one can apply the decoder of the channel code. This explains the three steps—noisy codify, channel decoder, uncodify—in the Slepian–Wolf decoder in Figure 6. Moreover, since the noisy codify and uncodify blocks are invertible, the essential error in recovering X^n from Y^n is the same as the error in recovering C^n from R^n.

Now we are ready to construct a code for the symmetric Slepian–Wolf problem $p(x,y)$. Figure 6 illustrates the block diagram.

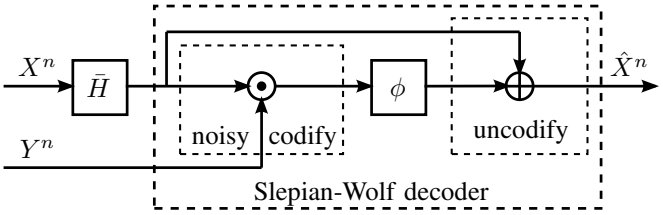

Fig. 6. The construction of a symmetric Slepian–Wolf code from a symmetric channel code.

Encoding. Upon observing the source sequence x^n, the sender transmits $s^n = \bar{H}x^n$.

Decoding. Upon observing y^n sequence and receiving the index s^n, the decoder declares

$$\hat{x}^n = \phi(y^n \odot s^n) \oplus s^n$$

as the source estimate.

Analysis of the probability of error. We have

$$\begin{aligned}
&\mathsf{P}\{\hat{X}^n \neq X^n\} \\
&= \mathsf{P}\{\phi(Y^n \odot \bar{H}X^n) \oplus \bar{H}X^n \neq X^n\} \\
&= \mathsf{P}\{\phi(Y^n \odot \bar{H}X^n) \neq X^n \oplus \bar{H}X^n\} \\
&= \mathsf{P}\{\phi(R^n) \neq C^n\} \\
&\overset{(d)}{=} \mathsf{P}\{\phi(\tilde{R}^n) \neq \tilde{C}^n\} \\
&= \epsilon,
\end{aligned}$$

where (d) follows from Lemma 2.

This code construction leads to the following conclusion.

Theorem 1. *From each linear (k, n, ϵ) code for the symmetric BMC $p(y|x)$, one can construct a linear $(n-k, n, \epsilon)$ code for the symmetric Slepian–Wolf problem $p(x, y)$.*

Remark 1. *By construction, the rate of the Slepian–Wolf code is $R_{sw} = (n-k)/n = 1 - R_{ch}$.*

B. A General Slepian–Wolf Code from a Symmetric Slepian–Wolf Code

Now we consider the general Slepian–Wolf problem $p(x, y)$. We show that by introducing common randomness, every general Slepian–Wolf problem can be *symmetrized* by scrambling.

Lemma 3. *Let $Z \sim \mathrm{Bern}(1/2)$ be independent of (X, Y). Let $\tilde{X} = X \oplus Z$ and $\tilde{Y} = (Y, Z)$. Then, the Slepian–Wolf problem $p(\tilde{x}, \tilde{y})$ is symmetric.*

Proof. First, we note that $\tilde{X} \sim \mathrm{Bern}(1/2)$. Moreover, for every $x, z \in \{0, 1\}$ and $y \in \mathcal{Y}$, we have

$$\begin{aligned}
p_{\tilde{Y}|\tilde{X}}(y, z|x \oplus z) &= \frac{p_{Y,Z,\tilde{X}}(y, z, x \oplus z)}{p_{\tilde{X}}(x \oplus z)} \\
&\overset{(a)}{=} \frac{p_{Y,Z,X}(y, z, x)}{p_{\tilde{X}}(x \oplus z \oplus 1)} \\
&\overset{(b)}{=} \frac{p_{Y,Z,X}(y, z \oplus 1, x)}{p_{\tilde{X}}(x \oplus z \oplus 1)} \\
&= \frac{p_{Y,Z,\tilde{X}}(y, z \oplus 1, x \oplus z \oplus 1)}{p_{\tilde{X}}(x \oplus z \oplus 1)} \\
&= p_{\tilde{Y}|\tilde{X}}(y, z \oplus 1|x \oplus z \oplus 1),
\end{aligned}$$

where (a) follows since $\tilde{X} \sim \mathrm{Bern}(1/2)$ and (b) follows since $Z \sim \mathrm{Bern}(1/2)$ is independent of (X, Y). Thus, the Slepian–Wolf problem $p(\tilde{x}, \tilde{y})$ is symmetric under permutation

$$\pi(\tilde{y}) = \pi(y, z) = (y, z \oplus 1).$$

□

In order to design a code for the general Slepian–Wolf problem (X, Y), we utilize a linear $(n-k, n, \epsilon)$ code $(\bar{H}, \psi)$ for the symmetrized Slepian–Wolf problem $(\tilde{X}, \tilde{Y}) = (X \oplus Z, (Y, Z))$, where $Z \sim \mathrm{Bern}(1/2)$ is independent of (X, Y). The block diagram of this code is shown in Figure 7. The average probability of error of this code is

$$\mathsf{P}\{\psi(\bar{H}\tilde{X}^n, \tilde{Y}^n) \neq \tilde{X}^n\} = \epsilon.$$

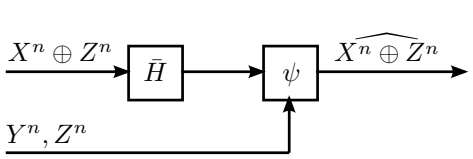

Fig. 7. A code for the symmetrized Slepian–Wolf problem $p(\tilde{x}, \tilde{y})$.

To construct a code for the general Slepian–Wolf problem $p(x, y)$, we share between the encoder and the decoder a common random sequence Z^n, which is i.i.d. $\mathrm{Bern}(1/2)$ and independent of (X^n, Y^n), as shown in Figure 8.

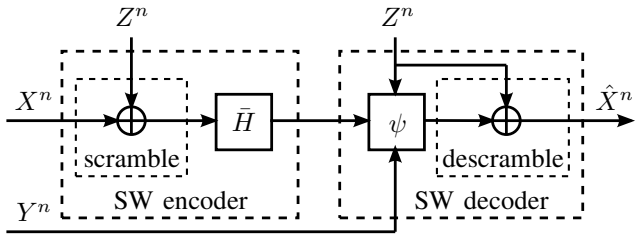

Fig. 8. The construction of a general Slepian–Wolf code from a symmetric Slepian–Wolf code.

Encoding. Upon observing x^n and z^n, the sender transmits

$$s^n = \bar{H}(x^n \oplus z^n).$$

Decoding. Upon receiving s^n and y^n, the decoder declares

$$\hat{x}^n = \psi(s^n, (y^n, z^n)) \oplus z^n$$

as the source estimate.

Analysis of probability of error. The probability of error averaged over Z^n is

$$\begin{aligned}
&\mathsf{P}\{\hat{X}^n \neq X^n\} \\
&= \mathsf{P}\{\psi(\bar{H}(X^n \oplus Z^n), (Y^n, Z^n)) \oplus Z^n \neq X^n\} \\
&= \mathsf{P}\{\psi(\bar{H}\tilde{X}^n, \tilde{Y}^n) \neq \tilde{X}^n\} \\
&= \epsilon.
\end{aligned}$$

This code construction leads to the following conclusion.

Theorem 2. *From each linear $(n-k, n, \epsilon)$ code for the symmetric Slepian–Wolf problem $p(\tilde{x}, \tilde{y})$ as defined above, one can construct an $(n-k, n, \epsilon)$ code for the general Slepian–Wolf problem $p(x, y)$.*

Remark 2. *By construction, the rate of the general Slepian–Wolf code equals that of the associated symmetric Slepian–Wolf code, $R_{gsw} = l/n = R_{sw}$. Moreover, we note that $H(\tilde{X}|\tilde{Y}) = H(X \oplus Z|Y, Z) = H(X|Y, Z) = H(X|Y)$.*

In the next two sections II-C and II-D, we show how to construct a general channel code from a symmetric Slepian–Wolf code. Again, we take two steps. We construct first a symmetric channel code and then a general channel code.

C. A Symmetric Channel Code from a Symmetric Slepian–Wolf Code

Suppose that for the symmetric Slepian–Wolf problem $p(x,y)$, there is a linear $(n-k,n,\epsilon)$ code $(\bar{H},\psi)$, as shown in Figure 9. Let $(\tilde{X}^n,\tilde{Y}^n)$ be i.i.d. according to $p_{X,Y}(\tilde{x},\tilde{y})$. The average probability of error is

$$\mathsf{P}\{\psi(\bar{H}\tilde{X}^n,\tilde{Y}^n)\neq\tilde{X}^n\}=\epsilon.$$

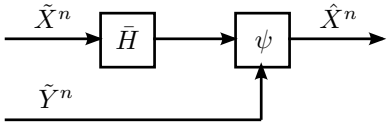

Fig. 9. A code for symmetric Slepian–Wolf problem $p(x,y)$.

To construct a channel code for the symmetric BMC $p(y|x)$, we share a common random sequence Z^n, which is i.i.d. $\mathrm{Bern}(1/2)$ and independent of the message C^n, between the encoder and the decoder. Figure 10 illustrates the block diagram.

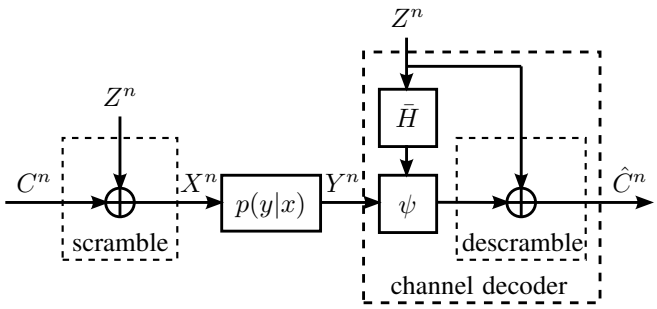

Fig. 10. The construction of a symmetric channel coding from a symmetric Sleplian–Wolf code.

Encoding. To send $c^n\in\mathcal{C}$, the sender transmits

$$x^n=c^n\oplus z^n.$$

Decoding. Upon receiving y^n, the decoder declares

$$\hat{c}^n=\psi(\bar{H}z^n,y^n)\oplus z^n$$

as the codeword estimate.

Analysis of probability of error. The probability of error averaged over Z^n is bounded as

$$\begin{aligned}\mathsf{P}\{\hat{C}^n\neq C^n\}&=\mathsf{P}\{\psi(\bar{H}Z^n,Y^n)\neq C^n\oplus Z^n\}\\&\overset{(a)}{=}\mathsf{P}\{\psi(\bar{H}X^n,Y^n)\neq X^n\}\\&\overset{(b)}{=}\mathsf{P}\{\psi(\bar{H}\tilde{X}^n,\tilde{Y}^n)\neq\tilde{X}^n\}\\&=\epsilon,\end{aligned}$$

where (a) follows since $C^n\in\mathcal{C}$ and thus $\bar{H}X^n=\bar{H}C^n\oplus\bar{H}Z^n=\bar{H}Z^n$ and (b) since after scrambling with i.i.d. uniform Z^n sequence, (X^n,Y^n) are identically distributed as $(\tilde{X}^n,\tilde{Y}^n)$ in the Slepian–Wolf problem. Finally, since the probability of error averaged over Z^n is ϵ, there exists a deterministic z^n sequence such that the probability of error is bounded by ϵ.

This code construction leads to the following conclusion.

Theorem 3. *From each linear $(n-k,n,\epsilon)$ code for the symmetric Slepian–Wolf problem $p(x,y)$, one can construct a (k,n,ϵ) code for the symmetric BMC $p(y|x)$.k*

Remark 3. *By construction, the rate of the channel code $R_{ch}=k/n=1-R_{sw}$.*

Remark 4. *Throughout the construction, we never use the symmetry of the channel $p(y|x)$. Therefore, the same construction works for designing general channel coding from general Slepian–Wolf codes. Due to the uniform dithering, the channel input X is uniform. Thus, the resulting channel code can only achieve up to the symmetric capacity $C_{sym}:=I(\mathrm{Bern}(1/2),p(y|x))$ of the BMC $p(y|x)$.*

D. A General Channel Code from a Symmetric Channel Code

Now we consider the general channel coding problem $p(y|x)$. Similar to the construction from a symmetric Slepian–Wolf code to a general Slepian–Wolf code, the key technique here is to symmetrize a general channel by scrambling.

Lemma 4. *Let $\tilde{Z}\sim\mathrm{Bern}(1/2)$ be independent of (X,Y). Then, the channel*

$$p_{\tilde{Y},\tilde{Z}|\tilde{X}}(\tilde{y},\tilde{z}|\tilde{x}):=\frac{1}{2}p_{Y|X}(\tilde{y}|\tilde{x}\oplus\tilde{z})$$

is symmetric.

Proof. The channel $p_{\tilde{Y},\tilde{Z}|\tilde{X}}(\tilde{y},\tilde{z}|\tilde{x})$ is symmetric under permutation $\pi(\tilde{y},\tilde{z})=(\tilde{y},\tilde{z}\oplus1)$ since

$$\begin{aligned}p_{\tilde{Y},\tilde{Z}|\tilde{X}}(\tilde{y},\tilde{z}|\tilde{x})&=\frac{1}{2}p_{Y|X}(\tilde{y}|\tilde{x}\oplus\tilde{z})\\&=\frac{1}{2}p_{Y|X}(\tilde{y}|\tilde{x}\oplus1\oplus\tilde{z}\oplus1)\\&=p_{\tilde{Y},\tilde{Z}|\tilde{X}}(\tilde{y},\tilde{z}\oplus1|\tilde{x}\oplus1)\end{aligned}$$

for any $\tilde{x},\tilde{z}\in\{0,1\}$ and $\tilde{y}\in\mathcal{Y}$. □

Suppose that we have a linear (k,n,ϵ) code $(\bar{H},\phi)$ for the symmetrized channel $p(\tilde{y},\tilde{z}|\tilde{x})$ as illustrated in Figure 11. The average probability of error satisfies

$$\mathsf{P}\{\tilde{C}^n\neq\phi(\tilde{Y}^n,\tilde{Z}^n)\}=\epsilon.$$

To construct a code for the general channel $p(y|x)$, we share between the encoder and the decoder an i.i.d. $\mathrm{Bern}(1/2)$ sequence Z^n. The encoding and decoding diagram is shown in Figure 12.

Encoding. To send $c^n\in\mathcal{C}$, the sender transmits

$$x^n=c^n\oplus z^n.$$

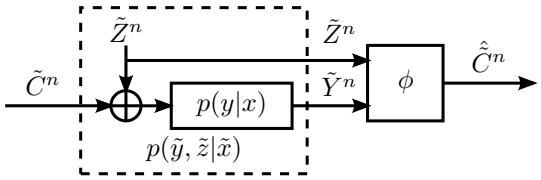

Fig. 11. Channel coding for symmetric BMC $p(\tilde{y},\tilde{z}|\tilde{x})$.

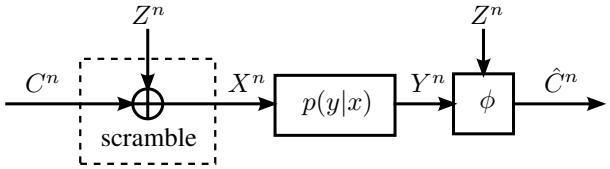

Fig. 12. The construction of a general channel coding from a symmetric channel code.

Decoding. Upon receiving y^n, the decoder declares

$$\hat{c}^n = \phi(y^n, z^n)$$

as the message estimate.

Probability of error analysis. By construction, for all $c^n \in \mathcal{C}$, $y^n \in \mathcal{Y}^n$, and $z^n \in \{0,1\}^n$, we have

$$\begin{aligned}
&\mathsf{P}\{\tilde{Y}^n = y^n, \tilde{Z}^n = z^n | \tilde{C}^n = c^n\} \\
&= \frac{1}{2^n} \prod_{i=1}^{n} p_{Y|X}(y_i | c_i \oplus z_i) \\
&= \mathsf{P}\{Z^n = z^n\}\, \mathsf{P}\{Y^n = y^n | X^n = c^n \oplus z^n\} \\
&\overset{(a)}{=} \mathsf{P}\{Z^n = z^n | C^n = c^n\} \\
&\quad \cdot \mathsf{P}\{Y^n = y^n | X^n = c^n \oplus z^n, C^n = c^n\} \\
&= \mathsf{P}\{Z^n = z^n | C^n = c^n\} \\
&\quad \cdot \mathsf{P}\{Y^n = y^n | Z^n = z^n, C^n = c^n\} \\
&= \mathsf{P}\{Y^n = y^n, Z^n = z^n | C^n = c^n\},
\end{aligned}$$

where (a) follows since Z^n is independent of C^n and $C^n \to X^n \to Y^n$ form a Markov chain. Therefore, the triples (C^n, Y^n, Z^n) and $(\tilde{C}^n, \tilde{Y}^n, \tilde{Z}^n)$ are identically distributed and the probability of error is

$$\mathsf{P}\{C^n \neq \phi(Y^n, Z^n)\} = \mathsf{P}\{\tilde{C}^n \neq \phi(\tilde{Y}^n, \tilde{Z}^n)\} = \epsilon.$$

This code construction leads to the following conclusion.

Theorem 4. *From each linear (k, n, ϵ) code for the symmetric BMC $p(\tilde{y},\tilde{z}|\tilde{x})$ as defined above, one can construct a (k, n, ϵ) code for the general BMC $p(y|x)$.*

Remark 5. *By construction, the rate of the general channel code is $R_{gch} = k/n = R_{ch}$. We note that*

$$\begin{aligned}
I(\tilde{X}; \tilde{Y}, \tilde{Z}) &= I(\tilde{X}; \tilde{Y} | \tilde{Z}) \\
&= H(\tilde{Y} | \tilde{Z}) - H(\tilde{Y} | \tilde{X}, \tilde{Z}) \\
&\overset{(a)}{=} H(\tilde{Y}) - H(\tilde{Y} | \tilde{X} \oplus \tilde{Z}) \\
&= I(\tilde{X} \oplus \tilde{Z}; \tilde{Y}) \\
&= I(\mathrm{Bern}(1/2), p_{Y|X}),
\end{aligned}$$

where (a) follows since $\tilde{X} \sim \mathrm{Bern}(1/2)$ is independent of $\tilde{Z}$ and thus $(\tilde{Y}, \tilde{X} \oplus \tilde{Z})$ is independent of $\tilde{Z}$. Therefore, we can construct a code for general channel $p_{Y|X}(y|x)$ only up to the symmetric capacity $I(\mathrm{Bern}(1/2), p_{Y|X})$.

REFERENCES

[1] A. D. Wyner, "Recent results in the Shannon theory," *IEEE Trans. Inf. Theory*, vol. 20, no. 1, pp. 2–10, 1974.

[2] R. Ahlswede and G. Dueck, "Good codes can be produced by a few permutations," *IEEE Trans. Inf. Theory*, vol. 28, no. 3, pp. 430–443, May 1982.

[3] S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): design and construction," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 626–643, Mar 2003.

[4] J. Garcia-Frias, "Compression of correlated binary sources using turbo codes," *Communications Letters, IEEE*, vol. 5, no. 10, pp. 417–419, Oct 2001.

[5] T. Coleman, A. Lee, M. Medard, and M. Effros, "Low-complexity approaches to Slepian–Wolf near-lossless distributed data compression," *IEEE Trans. Inf. Theory*, vol. 52, no. 8, pp. 3546–3561, Aug 2006.

[6] D. Schonberg, S. Pradhan, and K. Ramchandran, "Distributed code constructions for the entire Slepian–Wolf rate region for arbitrarily correlated sources," in *Signals, Systems and Computers, 2004. Conference Record of the Thirty-Seventh Asilomar Conference on*, vol. 1, Nov 2003, pp. 835–839 Vol.1.

[7] V. Stankovic, A. Liveris, Z. Xiong, and C. Georghiades, "On code design for the slepian-wolf problem and lossless multiterminal networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1495–1507, April 2006.

[8] J. Chen, D. ke He, A. Jagmohan, L. Lastras-Montano, and E. hui Yang, "On the linear codebook-level duality between Slepian–Wolf coding and channel coding," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5575–5590, Dec 2009.

[9] S. Miyake, "Coding theorems for point-to-point communication systems using sparse matrix codes," Ph.D. Thesis, The University of Tokyo, Tokyo, Japan, 2010.

[10] J. Chen, D. ke He, and A. Jagmohan, "The equivalence between Slepian–Wolf coding and channel coding under density evolution," *Communications, IEEE Transactions on*, vol. 57, no. 9, pp. 2534–2540, September 2009.

[11] S. Korada and R. Urbanke, "Polar codes are optimal for lossy source coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1751–1768, Apr. 2010.