ISIT'2013 1569720231

The Ahlswede-Han Conjecture on Channel with Coded Side Information at the Decoder

Wei Kang
School of Information Science and Engineering
Southeast University
Nanjing, China 210096
Email: wkang@seu.edu.cn

Nan Liu
National Mobile Communications Research Laboratory
Southeast University
Nanjing, China 210096
Email: nanliu@seu.edu.cn

***Abstract*—We study the Ahlswede-Han problem of single-user communication with partial state information available at the destination. For a class of channels, we show that the Wyner-Ziv compression of the channel state treating the receiver's channel output as side information is optimal. This result is more general than the modulo-sum channel studied by Aleksic *et. al* in 2009. Thus, for this more general class of channels, we prove the Ahlswede-Han conjecture.**

I. Introduction

In their 1983 paper [1], Ahlswede and Han considered the problem of single-user communication with partial state information available at the destination. More specifically, they considered a point-to-point channel where the channel output depends on the channel input and the channel state, which is i.i.d. across time. There is a third party that observes the channel state and is connected to the destination via an orthogonal link with finite capacity. The problem is determining the optimal coding strategy at the third party such that the communication rate between the source and the destination is maximized, see Fig. 1. Ahlswede and Han proposed a coding strategy, where the third party performs a Wyner-Ziv [2] compression on the channel state treating the channel output at the destination as side information. They conjectured that this coding scheme is optimal [1].

The Ahlswede-Han problem can be seen as a special case of the relay channel. The relay channel, proposed in [3], consists of three nodes: the source, the destination and the relay. It is characterized by the transition distribution of the outputs at the relay and the destination given the inputs by the source and the relay. In the relay channel, if we specify the channel between the relay and the destination to be an orthogonal link with finite capacity, we obtain a special case of the relay channel, called the primitive relay channel [4]. In the primitive relay channel, if we further specify that the output at the relay is independent to the input at the source, then we obtain the Ahlswede-Han problem.

This work is partially supported by the National Basic Research Program of China (973 Program 2012CB316004), the National Natural Science Foundation of China under Grant 61271208, 61201170, the National High Technology Research and Development Program of China (863 Program 2013AA014001), the Research Fund of National Mobile Communications Research Laboratory, Southeast University (No. 2013A02), the Project-sponsored by SRF for ROCS, SEM, and the New Teacher Funds of Southeast University.

In 2008, Kim studied the primitive relay channel [4], and showed that when the channel output at the relay is a deterministic function of the channel output at the destination and the channel input at the source, the optimal strategy of the relay node is to perform a Slepian-Wolf compression [5], a special case of the Wyner-Ziv compression, of the channel output at the relay by treating the output at the destination as side information. Since the Ahlswede-Han problem is a special case of the primitive relay channel, the results in [4] prove that the Ahlswede-Han conjecture is true when the channel state is a deterministic function of the channel output at the destination and the channel input at the source. Indeed, we observe that due to the deterministic nature of the channel, the destination can always compute the channel state with negligible probability of error based on the obtained channel output and decoded channel input of the source. Therefore, the Wyner-Ziv compression performed at the relay is done with zero average distortion, which means that it is in fact a Slepian-Wolf compression.

In 2009, Aleksic *et al.* proved the Ahlwede-Han conjecture for the modulo-sum channel [6]. The modulo-sum channel is a channel where the channel output at the destination is the modulo-sum of the channel input at the source and an i.i.d. sequence, which is correlated to the channel state observed by the relay. Due to the modulo-sum nature of the channel, the optimal input at the source is an i.i.d. distribution uniform on its alphabet, and as a result, the channel output at the destination is independent to the channel state. Thus, for the modulo-sum channel, the optimal strategy at the third party, i.e., Wyner-Ziv compression, reduces to the single-source rate distortion coding [7] of the channel state.

In this paper, we prove the Ahlswede-Han conjecture for a class of channels that is more general than the modulo-sum channel studied in [6]. The converse techniques that we use include the introduction of imaginary channels [8], and the single-letterization technique [7, page 314]. For this class of channels, the optimal Wyner-Ziv compression at the third party is general, in the sense that it does not reduce to the Slepian-Wolf compression, as in the deterministic channel studied in [4], or single-source rate distortion, as in the modulo-sum channel studied in [6].

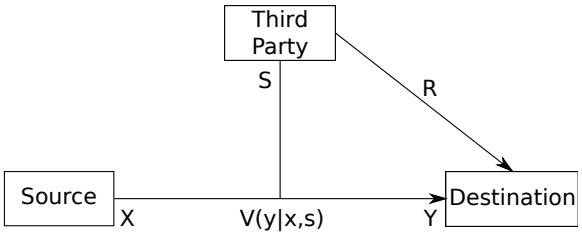

Fig. 1. Channel with coded side information at the decoder

II. System Model

Assume a discrete memoryless channel $V(y|x,s)$ with finite input space $\mathcal{X}$, finite output space $\mathcal{Y}$ and finite channel state space $\mathcal{S}$. Assume that the channel state S^n, which takes values in $\mathcal{S}^n$, is an i.i.d random sequence with distribution $Q(s)$. Let W be a message that is uniform on the set $\{1, 2, \cdots, M\}$. The Ahlswede-Han problem, see Fig. 1, consists of a source node, a destination and a third party. The source node would like to transmit the message W with negligible probability of error to the destination using the channel $V(y|x,s)$. The third party observes the channel state S^n and would like to help with the communication between the source and the destination by describing the source S^n with an index from the set $\{1, 2, \cdots, L\}$. This index is received at the destination with no error and the destination decodes the message W based on the channel output and the index describing the channel state.

An (M, L, n, ϵ_n) code consists of a sequence of encoding function f^n at the source,

$$f^n : \{1, 2, \ldots, M\} \mapsto \mathcal{X}^n$$

a sequence of encoding functions g^n at the third party,

$$g^n : \mathcal{S}^n \mapsto \{1, 2, \ldots, L\}$$

and a decoding function φ^n at the destination,

$$\varphi^n : \mathcal{Y}^n \times \{1, 2, \ldots, L\} \mapsto \{1, 2, \ldots, M\}$$

Define $P_e^n(i)$ as the probability of error when $W = i$, i.e.,

$$P_e^n(i) \stackrel{\triangle}{=} 1 - \sum_{s^n \in \mathcal{S}^n} Q^n(s^n)\, V^n\left(\varphi^{n(-1)}(g^n(s^n), i) | f^n(i), s^n\right)$$

where $\varphi^{n(-1)}(g(s^n), i)$ is the decoding region of message i when the index received from the third party is $g(s^n)$, i.e.,

$$\varphi^{n(-1)}(g(s^n), i) \triangleq \{y^n \in \mathcal{Y}^n : \varphi(y^n, g^n(s^n)) = i\}$$

Then, the average probability of error ϵ_n is defined as

$$\epsilon_n \triangleq \frac{1}{M} \sum_{i=1}^{M} P_e^n(i)$$

A rate pair (R, R_0) is achievable if there exists a sequence of $(2^{nR}, 2^{nR_0}, n, \epsilon_n)$ code such that $\epsilon_n \to 0$ as $n \to \infty$. The capacity region of the Ahlwede-Han problem is the closure of the set of all achievable rate pairs.

We define several special classes of channels below.

Definition 1 *The channel $V(y|x,s)$ is said to be deterministic if S can be written as a deterministic function of (X, Y) , i.e., there exists a deterministic function h such that $S = h(X, Y)$.*

Definition 2 *The channel $V(y|x,s)$ is said to be the modulo-sum channel if $Y = X \oplus Z$, where Z is the output of a discrete memoryless channel $V_z(z|s)$ with the input being the channel state S. The input and output alphabets of the channel V_z are $\mathcal{S}$ and $\mathcal{Z}$, respectively, $\oplus$ represents the modulo sum, and $\mathcal{X} = \mathcal{Y} = \mathcal{Z} = \{0, 1, \cdots, q-1\}$, where q is a positive integer.*

The class of channels $V(y|x,s)$ we consider in this paper satisfies the following two conditions:

1) *Shift-invariant condition*: For any $n = 1, 2, \cdots$, $H(Y^n|X^n = x^n)$, when evaluated with the distribution $\sum_{s^n} p(s^n) V^n(y^n|x^n, s^n)$, is independent of x^n for any $p(s^n)$.
2) *I.i.d.-optimal condition*: For any $n = 1, 2, \cdots$, the optimal distribution that solves the following optimization problem

$$\max_{p(x^n)} \quad H(Y^n) \tag{1}$$

is $p^*(x^n) = \prod_{i=1}^n p^*(x_i)$, i.e., the optimizing distribution is an i.i.d. distribution according to a single-letter distribution $p^*(x)$, irrespective of the distribution $p(s^n)$.

Note that in both conditions, $p(s^n)$ is an arbitrary distribution and is not necessarily equal to the distribution of the i.i.d. channel states, i.e., $Q^n(s^n)$.

The shift-variant condition is exactly the same as Condition 1 in [8]. It specifies that the channel $V(y|x,s)$ is invariant, in terms of conditional output entropy, with respect to the input sequence of source, i.e., x^n. This means that when designing the codebook at the source, the exact locations of the codewords do not affect the performance, rather, it is the relative locations, or "distances", between codewords that matter.

The i.i.d.-optimal condition requires that for any $p(s^n)$, the optimizing distribution in (1) is the same i.i.d. distribution according to $p^*(x)$. This suggests that using an i.i.d. generated codebook with $p^*(x)$ at source is to our advantage, as the larger the output space, i.e., $H(Y^n)$, the more codewords we can pack in the space.

We will show in Section V that the class of channels that satisfy the shift-invariant condition and the i.i.d.-optimal condition is strictly larger than the class of modulo-sum channels.

III. The Ahlswede-Han Conjecture and Existing Results

The following is an achievable region for the Ahlswede-Han problem.

Theorem 1 *[1] The rate pair is achievable if*

$$R_0 \geq I(S;\hat{S}|Y)$$
$$R \leq I(X;Y|\hat{S})$$

for some $p(\hat{s}|s)p(x)$ where the mutual informations are evaluated using the distribution

$$p(x,y,s,\hat{s}) = p(\hat{s}|s)p(x)Q(s)V(y|x,s) \tag{2}$$

The achievable scheme is one where the third party uses Wyner-Ziv compression to compress the channel state treating the channel output at the destination as side information. This compression can be done as long as the rate of compression is no smaller than $I(S;\hat{S}|Y)$, where $\hat{S}$ can be intuitively seen as the distorted version of the channel state and is available at the destination. Upon knowing $\hat{S}$ at the destination, the rate communicated from the source to the destination is $I(X;Y|\hat{S})$, and since the source does not have any knowledge about the channel state, X is independent to $(S,\hat{S})$.

Though no converse results were provided in [1], Ahlswede and Han conjectured that the rate region in Theorem 1 is optimal. Since then, progress has been made on the Ahlswede-Han problem and their conjecture has been proved to be true in two special cases.

The first special case is when the channel is a deterministic channel.

Theorem 2 *[4] When the channel is a deterministic channel, the Ahlswede-Han conjecture is true. In other words, the capacity region of the Ahlswede-Han problem is*

$$R_0 \geq H(S|Y) \tag{3}$$
$$R \leq I(X;Y|S) \tag{4}$$

for some $p(x)$ where the mutual informations are evaluated using the distribution

$$p(x,y,s) = p(x)Q(s)V(y|x,s) \tag{5}$$

Due to the deterministic nature of the channel, since the destination is required to decode the message W with negligible probability of error, it essentially knows X^n, and therefore, the destination knows the channel state S^n by calculating $S_i = h(X_i,Y_i)$, $i = 1,2,\cdots,n$. As a result, the Wyner-Ziv compression performed at the third party reduces to the Slepian-Wolf compression, i.e., Wyner-Ziv compression with distortion zero, and the rate of the Slepian-Wolf compression is $H(S|Y)$ as in (3). The communication rate between the source and the destination, when the source has no knowledge of the channel state and the destination has perfect knowledge of the channel state, is $I(X;Y|S)$ where X and S are independent, as in (4) and (5).

The second special case is when the channel is a modulo-sum channel.

Theorem 3 *[6] When the channel is a modulo-sum channel, the Ahlswede-Han conjecture is true. In other words, the capacity region of the Ahlswede-Han problem is*

$$R_0 \geq I(S;\hat{S}) \tag{6}$$
$$R \leq q - H(Z|\hat{S}) \tag{7}$$

for some $p(\hat{s}|s)$ where the mutual informations are evaluated using the distribution

$$p(z,s,\hat{s}) = p(\hat{s}|s)Q(s)V_z(z|s)$$

Due to the modulo-sum nature of the channel, the input distribution that maximizes the communication rate between the source and the destination is the uniform distribution on $\mathcal{X}$. Once the input takes the uniform distribution, Y and S are independent. As a result, the Wyner-Ziv compression performed at the third party reduces to the single-source compression, i.e., Wyner-Ziv compression with independent side information, and according to rate-distortion theory [7], the minimum compression rate is $I(S;\hat{S})$ as in (6). The communication rate between the source and the destination, when the source has no knowledge of the channel state and the destination knows the compressed version of the channel state $\hat{S}$, is $I(X;Y|\hat{S}) = q - H(Z|\hat{S})$, since X is the uniform distribution on $\{0,1,\cdots,q-1\}$, and is independent to $(S,\hat{S},Z)$. Thus, we have (7).

IV. Main Result

The main result of the paper is the following theorem, which proves the Ahlswede-Han conjecture for the class of channels that satisfy the shift-invariant condition and the i.i.d.-optimal condition.

Theorem 4 *For channels that satisfy the shift-invariant condition and the i.i.d.-optimal condition, the Ahlswede-Han conjecture is true. In other words, the capacity region for the Ahlswede-Han problem under the shift-invariant condition and the i.i.d.-optimal condition is*

$$R_0 \geq I(S;\hat{S}|Y) \tag{8}$$
$$R \leq I(X;Y|\hat{S})$$

for some $p(\hat{s}|s)$ where the mutual informations are evaluated using the distribution

$$p(x,y,s,\hat{s}) = p(\hat{s}|s)p^*(x)Q(s)V(y|x,s)$$

We will show in the next section that the class of channels that satisfy the shift-invariant condition and the i.i.d.-optimal condition is strictly larger than the class of modulo-sum channels. Thus, we prove the Ahlswede-Han conjecture for a more general class of channels than the ones studied in [6]. Note from (8) that third party indeed performs a general Wyner-Ziv compression with rate $I(S;\hat{S}|Y)$, which does not reduce to the Slepian-Wolf compression as in (3), or single-source rate distortion as in (6). Thus, this is the first special case showing that the *general* Wyner-Ziv compression is optimal in the Ahlswede-Han problem.

V. Examples

In this section, we provide examples of the channel $V(y|x,s)$ that satisfies the shift-invariant condition and the i.i.d.-optimal condition.

A. The Modulo-sum Channel

For the modulo-sum channel studied in [6], we have

Lemma 1 *The modulo-sum channel satisfies the shift-invariant condition and the i.i.d.-optimal condition.*

Thus, the class of channels that satisfy the shift-invariant condition and the i.i.d.-optimal condition include the modulo-sum channel studied in [6], and therefore, Theorem 4 is a generalized version of Theorem 3.

B. The Modulo-sum Erasure Channel

Another example of a channel that satisfies the shift-invariant condition and the maximum entropy condition is the following: Let Z is the output of a discrete memoryless channel $V_z(z|s)$ with the input being the channel state S. The input and output alphabets of the channel V_z are $\mathcal{S}$ and $\mathcal{Z}$. Let $\mathcal{X} = \{0,1\}$, $\mathcal{Z} = \mathcal{Y} = \{0,e,1\}$. The channel $V(y|x,s) = \sum_{z\in\mathcal{Z}} V_z(z|s)V_y(y|z,x)$, where $V_y(y|z,x)$ is

$$Y = \begin{cases} X \oplus Z, & \text{if } Z \neq e \\ e, & \text{if } Z = e. \end{cases}$$

where $\oplus$ is the modulo-2 sum. We call this channel *the modulo-sum erasure channel*. However, this channel is not a simple combination of modulo-sum channel [6] and erasure channel (deterministic) [4] due to the channel $V_z(z|s)$.

Lemma 2 *The modulo-sum erasure channel satisfies the shift-invariant condition and the i.i.d.-optimal condition.*

Due to space limitations, the proofs of Lemma 1 and 2 are omitted. The modulo-sum erasure channel is an example to show that the class of channels that satisfy the shift-invariant condition and the i.i.d.-optimal condition is strictly larger than the class of modulo-sum channels studied in [6]. Hence, compared to the results in [6], we prove the the Ahlswede-Han conjecture for this larger class of channels.

VI. Proof of Main Result

In this section, we provide the proof of our main result, i.e., Theorem 4.

A. Converse

For any (R, R_0) rate pair achievable, there exists a sequence of codebooks, denoted as $\mathcal{C}^n$, at the source of rate R and probability of error ϵ_n, where $\epsilon_n \to 0$. Let X^n be uniformly distributed on the codebook $\mathcal{C}^n$. Let Y^n be the output of channel V^n when the input is X^n.

Define the following two imaginary channels: define T^n as the output of channel V^n when the channel input is $\bar{x}^n$, where $\bar{x}^n$ is the sequence of $\bar{x}$ repeated n times, $\bar{x} \in \mathcal{X}$. Further define $\tilde{Y}^n$ as the output of the channel V^n when the channel input is the i.i.d. distribution according to $p^*(x)$.

First, we have

$$\begin{aligned} nR_0 &\geq H(g(S^n)) && (9)\\ &= H(S^n) - H(S^n|g(S^n)) && (10)\end{aligned}$$

where (9) follows because entropy is maximized by the uniform distribution. We also have

$$\begin{aligned} nR &= H(W) \\ &= H(W|g(S^n)) && (11)\\ &= I(W;Y^n|g(S^n)) + \epsilon_n && (12)\\ &= H(Y^n|g(S^n)) - H(Y^n|X^n, g(S^n)) + \epsilon_n \\ &= H(Y^n|g(S^n)) + \epsilon_n \\ &\quad - \sum_{x^n,r^n} p(x^n)p(r^n)H(Y^n|X^n = x^n, g(S^n) = r^n) \\ &= H(Y^n|g(S^n)) + \epsilon_n \\ &\quad - \sum_{x^n,r^n} p(x^n)p(r^n)H(Y^n|X^n = \bar{x}^n, g(S^n) = r^n) && (13)\\ &= H(Y^n|g(S^n)) - H(Y^n|X^n = \bar{x}^n, g(S^n)) + \epsilon_n \\ &= H(Y^n|g(S^n)) - H(T^n|g(S^n)) + \epsilon_n && (14)\\ &\leq H(\tilde{Y}^n|g(S^n)) - H(T^n|g(S^n)) + \epsilon_n && (15)\end{aligned}$$

where (11) follows from the independence of W and S^n, (12) follows from Fano's inequality, (13) follows from the shift-invariant condition, (14) follows from the definition of T^n, and (15) follows because the channel satisfies the i.i.d. optimal condition.

According to [7, page 314, eqn. (3.34)], we have

$$\begin{aligned} &H(\tilde{Y}^n|g(S^n)) - H(T^n|g(S^n)) \\ &= \sum_{i=1}^{n} \Bigg(H\left(\tilde{Y}_i|g(S^n), \tilde{Y}^{i-1}, T^n_{(i+1)}\right) \\ &\qquad - H\left(T_i|g(S^n), \tilde{Y}^{i-1}, T^n_{(i+1)}\right)\Bigg) && (16)\\ &H(S^n|g(S^n)) - H(T^n|g(S^n)) \\ &= \sum_{i=1}^{n} \Bigg(H\left(S_i|g(S^n), S^{i-1}, T^n_{(i+1)}\right) \\ &\qquad - H\left(T_i|g(S^n), S^{i-1}, T^n_{(i+1)}\right)\Bigg) \\ &= \sum_{i=1}^{n} \Bigg(H\left(S_i|g(S^n), S^{i-1}, \tilde{Y}^{i-1}, T^n_{(i+1)}\right) \\ &\qquad - H\left(T_i|g(S^n), S^{i-1}, \tilde{Y}^{i-1}, T^n_{(i+1)}\right)\Bigg) && (17)\end{aligned}$$

where (17) follows from Markov Chain

$$\left(g(S^n), S_i, T^n_{(i+1)}\right) \to S^{i-1} \to \tilde{Y}^{i-1}$$

Define the following auxiliary random variables

$$\hat{S}_i = \left(g(S^n), \tilde{Y}^{i-1}, T^n_{(i+1)}\right), \quad \bar{S}_i = S^{i-1}$$

Further define the time-sharing random variable Q to be uniformly distributed on $\{1, 2, \cdots, n\}$, and define

$$\hat{S} = (\hat{S}_Q, Q), \quad \bar{S} = \bar{S}_Q, \quad T = T_Q, \quad S = S_Q, \quad \tilde{Y} = \tilde{Y}_Q$$

According to (16), similar to [7, page 315], there exists a real number t such that

$$\frac{1}{n} H(\tilde{Y}^n | g(S^n)) = H(\tilde{Y}|\hat{S}) + t \tag{18}$$

$$\frac{1}{n} H(T^n | g(S^n)) = H(T|\hat{S}) + t \tag{19}$$

$$0 \le t \le I(\hat{S}; \tilde{Y}) \tag{20}$$

From (17), we have

$$\begin{aligned}
&\frac{1}{n} H(S^n | g(S^n)) \\
&= H(S|\hat{S}, \bar{S}) - H(T|\hat{S}, \bar{S}) + \frac{1}{n} H(T^n | g(S^n)) \\
&= H(S|\hat{S}, \bar{S}) - H(T|\hat{S}, \bar{S}) + H(T|\hat{S}) + t \qquad (21) \\
&= H(S|\hat{S}, \bar{S}) + I(\bar{S}; T|\hat{S}) + t \\
&\le H(S|\hat{S}, \bar{S}) + I(\bar{S}; S|\hat{S}) + t \qquad (22) \\
&= H(S|\hat{S}) + t \qquad (23)
\end{aligned}$$

where (21) follows from (19), (22) follows from Markov Chain $\bar{S} \to (\hat{S}, S) \to T$. Thus, from (10), (20), (23), (15), (18) and (19), and letting $n \to \infty$, we have

$$\begin{aligned}
R_0 &\ge H(S) - H(S|\hat{S}) - I(\hat{S}; \tilde{Y}) \\
&= I(S; \hat{S}|\tilde{Y}) \qquad (24) \\
R &\le H(\tilde{Y}|\hat{S}) - H(T|\hat{S}) \qquad (25)
\end{aligned}$$

where (24) follows from the Markov Chain $\hat{S} \to S \to \tilde{Y}$, and the joint distribution of the random variables satisfy

$$p(s, \hat{s}, \tilde{y}, t) = Q(s) p(\hat{s}|s) p(\tilde{y}|s) p(t|s)$$

where $p(t|s) = V(t|\bar{x}, s)$ and $p(\tilde{y}|s) = \sum_x p^*(x) V(\tilde{y}|x, s)$.

B. Achievability

For channels that satisfy the i.i.d.-optimal condition, rather than the arbitrary $p(x)$ in the distribution (2), we take $p(x) = p^*(x)$, and obtain the following achievable region from Theorem 1 as

$$R_0 \ge I(S; \hat{S}|\tilde{Y}) \tag{26}$$

$$R \le I(\tilde{X}; \tilde{Y}|\hat{S}) \tag{27}$$

for some $p(\hat{s}|s)$ where the mutual informations are evaluated using the distribution

$$p(\tilde{x}, \tilde{y}, s, v) = Q(s) p(\hat{s}|s) p^*(\tilde{x}) V(\tilde{y}|\tilde{x}, s)$$

C. Capacity

We prove that the achievable region in (26)-(27) and the converse region in (24)-(25) are the same.

For the same $p(\hat{s}|s)$, $I(\hat{S}; S|\tilde{Y})$ in (26) and that in (24) is the same, and $H(\tilde{Y}|\hat{S})$ in (27) and that in (25) are the same. Hence, we only need to prove that $H(\tilde{Y}|\tilde{X}, \hat{S})$ in (27) is equal to $H(T|\hat{S})$ in (25) for the same $p(\hat{s}|s)$.

The term $H(\tilde{Y}|\tilde{X}, \hat{S})$ in (27) satisfy

$$\begin{aligned}
H(\tilde{Y}|\tilde{X}, \hat{S}) &= \sum_{\tilde{x}, \hat{s}} p^*(\tilde{x}) p(\hat{s}) H(\tilde{Y}|\tilde{X} = \tilde{x}, \hat{S} = \hat{s}) \\
&= \sum_{\tilde{x}, v} p^*(\tilde{x}) p(\hat{s}) H(\tilde{Y}|\tilde{X} = \bar{x}, \hat{S} = \hat{s}) \qquad (28) \\
&= \sum_{\hat{s}} p(\hat{s}) H(\tilde{Y}|\tilde{X} = \bar{x}, \hat{S} = \hat{s}) \qquad (29)
\end{aligned}$$

where (28) follows because of the shift-invariant condition. The term $H(T|\hat{S})$ in (25) satisfy

$$H(T|\hat{S}) = \sum_{\hat{s}} p(\hat{s}) H(T|\hat{S} = \hat{s}) \tag{30}$$

Both $H(\tilde{Y}|\tilde{X} = \bar{x}, \hat{S} = \hat{s})$ in (29) and $H(T|\hat{S} = \hat{s})$ in (30) are the entropy of the distribution $\sum_s p(s|\hat{s}) W(\cdot|\bar{x}, s)$. Therefore, they are equal. This means that the achievable region described in (26)- (27) and the converse region described in (24)-(25) are the same and both represent the capacity region.

VII. Conclusion

We study the Ahlswede-Han problem of single-user communication with partial state information available at the destination. For channels that satisfy the shift-invariant condition and the i.i.d.-optimal condition, we show that the Wyner-Ziv compression of the channel state treating the channel output at the destination as side information is optimal. This result is more general than the modulo-sum channel studied by Aleksic *et. al* in 2009. Thus, for this more general class of channels, we prove the Ahlswede-Han conjecture.

Compared to previous special cases where Slepian-Wolf compression of the channel state is optimal for the deterministic channel, and single-source rate distortion compression of the channel state is optimal for the modulo-sum channel, our results constitute the first special case where the general Wyner-Ziv compression of the channel state is optimal.

References

[1] R. Ahlswede and T. S. Han. On source coding with side information via a multiple-access channel and related problems in multi-user information theory. *IEEE Trans. Inform. Theory*, 29(3):396–412, 1983.

[2] A. D. Wyner and J. Ziv. The rate-distortion function for source coding with side information at the decoder. *IEEE Trans. Inform. Theory*, 22(1):1–10, 1976.

[3] T. M. Cover and A. El Gamal. Capacity theorems for the relay channel. *IEEE Trans. Inform. Theory*, 25:572–584, Sep. 1979.

[4] Y. H. Kim. Capacity of a class of deterministic relay channels. *IEEE Trans. Inform. Theory*, 53(3):1328–1329, 2008.

[5] D. Slepian and J. K. Wolf. Noiseless coding of correlated information sources. *IEEE Trans. Inform. Theory*, 19:471–480, 1973.

[6] Marko Aleksic, Peyman Razaghi, and Wei Yu. Capacity of a class of modulo-sum relay channels. *IEEE Transactions on Information Theory*, 55(3):921–930, March 2009.

[7] I. Csiszar and J. Korner. *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Academic Press, 1981.

[8] N. Liu and A. Goldsmith. Capacity regions and bounds for a class of Z-interference channels. *IEEE Trans. on Information Theory*, 55(11):4986–4994, November 2009.