On Existence of Optimal Linear Encoders over Non-field Rings for Data Compression

Sheng Huang, Mikael Skoglund, *Senior Member, IEEE*

Abstract

This note proves that, for any set of finite correlated discrete memoryless sources, there exists a sequence of linear encoders over some finite non-field rings which achieves the data compression limit, the Slepian–Wolf region.

Index Terms

Finite Ring, Linear Source Coding, Data Compression

I. Introduction

Let t_i ($i \in \mathcal{S} = \{1, 2, \cdots, s\}$) be a discrete memoryless source generating i.i.d. random data

$$X_i^{(1)}, X_i^{(2)}, \cdots, X_i^{(n)}, \cdots,$$

where $X_i^{(n)} \in \mathscr{X}_i$ and $\left[X_1^{(n)}, X_2^{(n)}, \cdots, X_s^{(n)}\right] \sim p$ for all $i \in \mathcal{S}$ and $n \in \mathbb{N}^+$. It is well known that the limit for compressing data generated by $t_1, t_2, \cdots, t_s$ with independent encoders is illustrated by the Slepian–Wolf region [1]. Even thought it is guaranteed by [1] that there always exist encoders achieving the data compression limit. The structures of the encoders are unclear, which confines the scope of their applications. Fortunately, [2], [3] proves that linear encoders over finite fields achieve the same limit, i.e. the Slepian–Wolf region. In addition, the linear structure of the linear encoder (over field) offers strict benefit to other problems, e.g. encoding functions of correlated sources (also known as source coding for computing) [4], [5], [6], [7]. However, special constraints are casted upon the algebraic structures of finite fields, for instance, the size of a finite field must be a power of a prime, the characteristic of a finite field has to be a prime and a field contains no zero divisor. They limit the performance of linear encoders over fields. As a consequence, linear encoders over finite rings are proposed [8].

Demonstrated in [8], linear encoders over non-field rings achieve the data compression limit, i.e. the Slepian–Wolf region, in many circumstances as well. The ring versions are also recommended because the arithmetic of lots of non-field rings (e.g. modulo integer rings) is substantially easier to implement than the one for fields. Most importantly, it is shown that the ring version strictly outperforms its field counterpart in the source coding for

S. Huang and M. Skoglund are with the Communication Theory Lab, School of Electrical Engineering, KTH Royal Institute of Technology, Stockholm, 10044, Sweden e-mail: (sheng.huang@ee.kth.se; skoglund@ee.kth.se).

This work was funded in part by the Swedish Research Council.

computing problem [8, Problem 1]. It is proved that linear encoders over non-field rings achieve strictly larger achievable region with strictly smaller alphabet size in some computing problem [9].

Although verified in various scenarios, it has not been proved (neither denied) that linear encoders over non-field rings are always optimal in the Slepian–Wolf problem, namely achieving the Slepian–Wolf region. This article is to prove that there always exist linear encoders over non-field rings that achieve the data compression limit, the Slepian–Wolf region, in any scenario. In other words, the achievable region (2) [8, (8)] is indeed the Slepian–Wolf region. Therefore, the optimality issue is closed on this regard.

II. Linear Source Coding over Finite Rings

Generally speaking, the data generated by a source is not necessarily associated with any specific algebraic structure. In order to apply the linear encoders (over ring), we assume that there exists a set $\Phi = \{\Phi_1, \Phi_2, \cdots, \Phi_s\}$ of injections $\Phi_i : \mathscr{X}_i \to \mathfrak{R}_i$ mapping $\mathscr{X}_i$ to a finite ring $\mathfrak{R}_i$ of order $|\mathfrak{R}_i| \geq |\mathscr{X}_i|$ for all $i \in \mathcal{S} = \{1, 2, \cdots, s\}$. Thus, $\mathscr{X}_i$ can be seen as a subset of $\mathfrak{R}_i$ for a fixed Φ. To facilitate our discussion, we define $\Phi(x_T) = \{\Phi_i(x_i)\}_{i\in T}$, where $x_T = \prod_{i\in T} x_i \in \prod_{i\in T} \mathscr{X}_i$, for any $\emptyset \neq T \subseteq \mathcal{S}$. Let $\mathfrak{R}_T$ be the ring $\prod_{i\in T} \mathfrak{R}_i$ (direct product) for $\emptyset \neq T \subseteq \mathcal{S}$. It is well known that $\mathfrak{I}$ is a left ideal of $\mathfrak{R}_T$ if and only if $\mathfrak{I} = \prod_{i\in T} \mathfrak{I}_i$ and $\mathfrak{I}_i$ is a left ideal of $\mathfrak{R}_i$ [8, Proposition II.4]. Similarly, we often write $\mathfrak{I}_T$ for the left ideal $\prod_{i\in T} \mathfrak{I}_i$. Meanwhile, $\mathfrak{I} \leq_l \mathfrak{R}$ is used to indicate that the subset $\mathfrak{I}$ is a left ideal of the ring $\mathfrak{R}$, $\mathfrak{R}/\mathfrak{I}$ for the quotient group $\mathfrak{R} \mod \mathfrak{I}$. Let $[X_1, X_2, \cdots, X_s] \sim p$ and

$$\mathcal{R}_\Phi = \left\{ [R_1, R_2, \cdots, R_s] \in \mathbb{R}^s \middle| \sum_{i\in T} \frac{R_i \log|\mathfrak{I}_i|}{\log|\mathfrak{R}_i|} > H(X_T|X_{T^c}) - H(Y_{\mathfrak{R}_T/\mathfrak{I}_T}|X_{T^c}), \right.$$
$$\left. \forall\, \emptyset \neq T \subseteq \mathcal{S}, \forall\, 0 \neq \mathfrak{I}_i \leq_l \mathfrak{R}_i \right\}, \tag{1}$$

where $T^c = \mathcal{S} \setminus T$, X_T is the random variable array $\prod_{i\in T} X_i$ and $Y_{\mathfrak{R}_T/\mathfrak{I}_T} = \Phi(X_T) + \mathfrak{I}_T$ is a random variable with sample space $\mathfrak{R}_T/\mathfrak{I}_T$. It is proved in [8, Theorem IV.1] that $\mathcal{R}_\Phi$ is achievable with linear encoders over $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$ (or achievable for simplicity). In exact terms, $\forall\, \epsilon > 0$, there exists $N_0 \in \mathbb{N}^+$, for all $n > N_0$, there exist linear encoders (left linear mappings [8, Definition II.5] to be more precise) $\phi_i : \Phi(\mathscr{X}_i)^n \to \mathfrak{R}_i^{k_i}$ $(i \in \mathcal{S})$ and a decoder ψ, such that

$$\Pr\left\{ \psi\left(\prod_{i\in S} \phi_i(\mathbf{X}_i) \right) \neq \prod_{i\in S} \mathbf{X}_i \right\} < \epsilon,$$

where $\mathbf{X}_i = \left[\Phi\left(X_i^{(1)}\right), \Phi\left(X_i^{(2)}\right), \cdots, \Phi\left(X_i^{(n)}\right) \right]^t$, as long as $\left[\frac{k_1 \log|\mathfrak{R}_1|}{n}, \frac{k_2 \log|\mathfrak{R}_2|}{n}, \cdots, \frac{k_s \log|\mathfrak{R}_s|}{n} \right] \in \mathcal{R}_\Phi$. By simple time sharing argument, it is noticeable that

$$\mathcal{R}_l = \mathrm{cov}\left(\bigcup_{\Phi\in\mathscr{M}} \mathcal{R}_\Phi \right), \tag{2}$$

where $\mathscr{M}$ is the family of all possible Φ's and $\mathrm{cov}(A)$ is the convex hull of a set $A \subseteq \mathbb{R}^s$, is also achievable. For convenience, a coding rate $\mathbf{R} \in \mathbb{R}^s$ is said to be *achievable* with linear encoders over $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$ if $\mathbf{R} \in \mathcal{R}_l$.

However, $\mathbf{R}$ is said to be *directly achievable* with linear encoders over $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$ if $\mathbf{R} \in \mathcal{R}_\Phi$ for some fixed $\Phi \in \mathscr{M}$.

It is not difficult to see that (1), as well as (2), coincides with the Slepian–Wolf region, if $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$ are fields [8]. We claim existence of optimal linear encoders over non-field rings for any data compression scenario of Slepian–Wolf, i.e. $\mathcal{R}_l$ is indeed the Slepian–Wolf region

$$\mathcal{R}[X_1, X_2, \cdots, X_s] = \left\{ [R_1, R_2, \cdots, R_s] \in \mathbb{R}^s \middle| \sum_{j \in T} R_j > H(X_T | X_{T^c}), \forall\, \emptyset \neq T \subseteq \mathcal{S} \right\}.$$

Proofs of this are presented in the Section III and Section IV.

III. Existence Theorem I: Single Source

For any single source scenario, the assertion that there always exists a finite ring $\mathfrak{R}_1$, such that $\mathcal{R}_l$ is in fact the Slepian–Wolf region

$$\mathcal{R}[X_1] = \{R_1 \in \mathbb{R} | R_1 > H(X_1)\},$$

is equivalent to there always exists a finite ring $\mathfrak{R}_1$ and an injection $\Phi_1 : \mathscr{X}_1 \to \mathfrak{R}_1$, such that

$$\max_{0 \neq \mathfrak{I}_1 \leq_l \mathfrak{R}_1} \frac{\log |\mathfrak{R}_1|}{\log |\mathfrak{I}_1|} \left[H(X_1) - H(Y_{\mathfrak{R}_1/\mathfrak{I}_1}) \right] = H(X_1), \tag{3}$$

where $Y_{\mathfrak{R}_1/\mathfrak{I}_1} = \Phi_1(X_1) + \mathfrak{I}_1$.

Theorem III.1. *Let $\mathfrak{R}_1$ be a finite ring of order $|\mathfrak{R}_1| \geq |\mathscr{X}_1|$. If $\mathfrak{R}_1$ contains one and only one proper non-trivial left ideal $\mathfrak{I}_0$ and $|\mathfrak{I}_0| = \sqrt{|\mathfrak{R}_1|}$, then region* (2) *coincides with the Slepian–Wolf region, i.e. there exists an injection $\Phi_1 : \mathscr{X}_1 \to \mathfrak{R}_1$, such that* (3) *holds.*

Remark 1. Examples of such a ring $\mathfrak{R}_1$ in the above theorem include $\mathbb{M}_{L,p} = \left\{ \begin{bmatrix} x & 0 \\ y & x \end{bmatrix} \middle| x, y \in \mathbb{Z}_p \right\}$ and $\mathbb{Z}_{p^2}$, where p is any prime. For any single source scenario, one can always choose $\mathfrak{R}_1$ to be either $\mathbb{M}_{L,p}$ or $\mathbb{Z}_{p^2}$. Consequently, optimality is attained.

Proof of Theorem III.1: Notice that the random variable $Y_{\mathfrak{R}_1/\mathfrak{I}_0}$ depends on the injection Φ_1, so does its entropy $H(Y_{\mathfrak{R}_1/\mathfrak{I}_0})$. Obviously $H(Y_{\mathfrak{R}_1/\mathfrak{R}_1}) = 0$, since the sample space of the random variable $Y_{\mathfrak{R}_1/\mathfrak{R}_1}$ contains only one element. Therefore,

$$\frac{\log |\mathfrak{R}_1|}{\log |\mathfrak{R}_1|} \left[H(X_1) - H(Y_{\mathfrak{R}_1/\mathfrak{R}_1}) \right] = H(X_1).$$

Henceforth, (3) is equivalent to

$$\begin{aligned} &\frac{\log |\mathfrak{R}_1|}{\log |\mathfrak{I}_0|} \left[H(X_1) - H(Y_{\mathfrak{R}_1/\mathfrak{I}_0}) \right] \leq H(X_1) \\ \Leftrightarrow &H(X_1) \leq 2H(Y_{\mathfrak{R}_1/\mathfrak{I}_0}), \end{aligned} \tag{4}$$

since $|\mathfrak{I}_0| = \sqrt{|\mathfrak{R}_1|}$. By Lemma A.1, there exists injection $\tilde{\Phi}_1 : \mathscr{X}_1 \to \mathfrak{R}_1$ such that (4) holds if $\Phi_1 = \tilde{\Phi}_1$. The statement follows. ∎

Up to isomorphism, there are exactly 4 distinct rings of order p^2 for a given prime p. They include 3 non-field rings, $\mathbb{Z}_p \times \mathbb{Z}_p$, $\mathbb{M}_{L,p}$ and $\mathbb{Z}_{p^2}$, in addition to the field[1] $\mathbb{F}_{p^2}$. It has been proved that, using linear encoders over the last three, optimality can always be achieved in the single source scenario. Actually, the same holds true for all multiple sources scenarios.

IV. Existence Theorem II: Multiple Sources

Theorem IV.1. *Let $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$ be s finite rings with $|\mathfrak{R}_i| \geq |\mathscr{X}_i|$. If $\mathfrak{R}_i$ is isomorphic to either*

1) *a field, i.e. $\mathfrak{R}_i$ contains no proper non-trivial left (right) ideal; or*
2) *a ring containing one and only one proper non-trivial left ideal $\mathfrak{I}_{0i}$ and $|\mathfrak{I}_{0i}| = \sqrt{|\mathfrak{R}_i|}$,*

for all feasible i, then (2) *coincides with the Slepian–Wolf region $\mathcal{R}[X_1, X_2, \cdots, X_s]$.*

Remark 2. Obvious that Theorem IV.1 includes Theorem III.1 as a special case. In fact, its proof resembles the one of Theorem III.1. Examples of $\mathfrak{R}_i$'s include all finite fields, $\mathbb{M}_{L,p}$ and $\mathbb{Z}_{p^2}$, where p is a prime. However, Theorem IV.1 does not guarantee that all rates, except the *vertexes*, in the *polytope* of the Slepian–Wolf region are directly achievable for the multiple sources case. A time sharing scheme is required in our current proof. Nevertheless, all rates are directly achievable if $\mathfrak{R}_i$'s are fields or if $s = 1$. This is partially the reason that the two theorems are stated separately.

Proof of Theorem IV.1: It suffices to prove that, for any $\mathbf{R} = [R_1, R_2, \cdots, R_s] \in \mathbb{R}^s$ satisfies

$$R_i > H(X_i|X_{i-1}, X_{i-2}, \cdots, X_1), \forall\, 1 \leq i \leq s,$$

$\mathbf{R} \in \mathcal{R}_\Phi$ for some set of injections $\Phi = \{\Phi_1, \Phi_2, \cdots, \Phi_s\}$, where $\Phi_i : \mathscr{X}_i \to \mathfrak{R}_i$. Let $\tilde{\Phi} = \{\tilde{\Phi}_1, \tilde{\Phi}_2, \cdots, \tilde{\Phi}_s\}$ be the set of injections, where, if

(i) $\mathfrak{R}_i$ is a field, $\tilde{\Phi}_i$ is any injection;
(ii) $\mathfrak{R}_i$ satisfies 2), $\tilde{\Phi}_i$ is the injection such that

$$H(X_i|X_{i-1}, X_{i-2}, \cdots, X_1) \leq 2H(Y_{\mathfrak{R}_i/\mathfrak{I}_{0i}}|X_{i-1}, X_{i-2}, \cdots, X_1),$$

when $\Phi_i = \tilde{\Phi}_i$. The existence of $\tilde{\Phi}_i$ is guaranteed by Lemma A.1.

If $\Phi = \tilde{\Phi}$, then

$$\begin{aligned}
&\frac{\log|\mathfrak{I}_i|}{\log|\mathfrak{R}_i|} H(X_i|X_{i-1}, X_{i-2}, \cdots, X_1) \\
\geq& H(X_i|X_{i-1}, X_{i-2}, \cdots, X_1) - H(Y_{\mathfrak{R}_i/\mathfrak{I}_i}|X_{i-1}, X_{i-2}, \cdots, X_1) \\
=& H(X_i|Y_{\mathfrak{R}_i/\mathfrak{I}_i}, X_{i-1}, X_{i-2}, \cdots, X_1),
\end{aligned}$$

[1]The finite field of order q is often denoted by $\mathbb{F}_q$ in this paper.

for all $1 \leq i \leq s$ and $0 \neq \mathfrak{I}_i \leq_l \mathfrak{R}_i$. As a consequence,

$$\begin{aligned}\sum_{i\in T}\frac{R_i\log|\mathfrak{I}_i|}{\log|\mathfrak{R}_i|} >& \sum_{i\in T}\frac{\log|\mathfrak{I}_i|}{\log|\mathfrak{R}_i|}H(X_i|X_{i-1},X_{i-2},\cdots,X_1)\\ \geq& \sum_{i\in T}\left[H(X_i|Y_{\mathfrak{R}_i/\mathfrak{I}_i},X_{i-1},X_{i-2},\cdots,X_1)\right]\\ \geq& \sum_{i\in T}\left[H(X_i|Y_{\mathfrak{R}_T/\mathfrak{I}_T},X_{T^c},X_{i-1},X_{i-2},\cdots,X_1)\right]\\ \geq& H\left(X_T\left|Y_{\mathfrak{R}_T/\mathfrak{I}_T},X_{T^c}\right.\right)\\ =& H\left(X_T|X_{T^c}\right)-H\left(Y_{\mathfrak{R}_T/\mathfrak{I}_T}|X_{T^c}\right),\end{aligned}$$

for all $\emptyset \neq T \subseteq \{1,2,\cdots,s\}$. Thus, $\mathbf{R} \in \mathcal{R}_{\tilde{\Phi}}$. ■

By Theorem III.1 and Theorem IV.1, we draw the conclusion that

Corollary IV.2. *For any scenario of SW, there always exists a sequence of linear encoders over rings (fields, non-field rings) which achieves the data compression limit, the SW region.*

In fact, linear encoder over ring can be optimal for even scenarios beyond those stated in the above theorems. We classify some of these scenarios in the rest of this section.

Theorem IV.3. *Let $\mathfrak{R}_{l1},\mathfrak{R}_{l2},\cdots,\mathfrak{R}_{ls}$ ($l=1,2$) be a set of finite rings of equal size, and $\mathfrak{R}_i=\mathfrak{R}_{1i}\times\mathfrak{R}_{2i}$ for all feasible i. If the coding rate $\mathbf{R}\in\mathbb{R}^s$ is achievable with linear encoders over $\mathfrak{R}_{l1},\mathfrak{R}_{l2},\cdots,\mathfrak{R}_{ls}$ ($l=1,2$), then $\mathbf{R}$ is achievable with linear encoders over $\mathfrak{R}_1,\mathfrak{R}_2,\cdots,\mathfrak{R}_s$.*

Proof: By definition, $\mathbf{R}$ is a convex combination of coding rates which are directly achieved by different linear encoding schemes over $\mathfrak{R}_{l1},\mathfrak{R}_{l2},\cdots,\mathfrak{R}_{ls}$ ($l=1,2$), respectively. To be more precise, there exist $\mathbf{R}_1,\mathbf{R}_2,\cdots,\mathbf{R}_m\in\mathbb{R}^s$ and positive numbers $w_1,w_2,\cdots,w_m$ with $\sum_{j=1}^m w_j=1$, such that $\mathbf{R}=\sum_{j=1}^m w_j\mathbf{R}_j$. Moreover, there exist injections $\Phi_l=\{\Phi_{l1},\Phi_{l2},\cdots,\Phi_{ls}\}$ ($l=1,2$), where $\Phi_{li}:\mathscr{X}_i\to\mathfrak{R}_{li}$, such that

$$\begin{aligned}\mathbf{R}_j\in\mathcal{R}_{\Phi_l}=\Bigg\{[R_1,R_2,\cdots,R_s]\in\mathbb{R}^s\Bigg|&\sum_{i\in T}\frac{R_i\log|\mathfrak{I}_{li}|}{\log|\mathfrak{R}_{li}|}>H(X_T|X_{T^c})-H(Y_{\mathfrak{R}_{lT}/\mathfrak{I}_{lT}}|X_{T^c}),\\ &\forall\,\emptyset\neq T\subseteq\mathcal{S},\forall\,0\neq\mathfrak{I}_{li}\leq_l\mathfrak{R}_{li}\Bigg\},\end{aligned}\tag{5}$$

where $\mathfrak{R}_{lT}=\prod_{i\in T}\mathfrak{R}_{li}$, $\mathfrak{I}_{lT}=\prod_{i\in T}\mathfrak{I}_{li}$ and $Y_{\mathfrak{R}_{lT}/\mathfrak{I}_{lT}}=\Phi_l(X_T)+\mathfrak{I}_{lT}$ is a random variable with sample space $\mathfrak{R}_{lT}/\mathfrak{I}_{lT}$. To show that $\mathbf{R}$ is achievable with linear encoders over $\mathfrak{R}_1,\mathfrak{R}_2,\cdots,\mathfrak{R}_s$, it suffices to prove that $\mathbf{R}_j$ is achievable with linear encoders over $\mathfrak{R}_1,\mathfrak{R}_2,\cdots,\mathfrak{R}_s$ for all feasible j. Let $\mathbf{R}_j=[R_{j1},R_{j2},\cdots,R_{js}]$. For all $\emptyset\neq T\subseteq\mathcal{S}$ and $0\neq\mathfrak{I}_i=\mathfrak{I}_{1i}\times\mathfrak{I}_{2i}\leq_l\mathfrak{R}_i$ with $0\neq\mathfrak{I}_{li}\leq_l\mathfrak{R}_{li}$ ($l=1,2$), we have

$$\sum_{i\in T}\frac{R_{ji}\log|\mathfrak{I}_i|}{\log|\mathfrak{R}_i|}=\sum_{i\in T}\frac{R_{ji}\log|\mathfrak{I}_{1i}|}{\log|\mathfrak{R}_{1i}|}\frac{c_1}{c_1+c_2}+\sum_{i\in T}\frac{R_{ji}\log|\mathfrak{I}_{2i}|}{\log|\mathfrak{R}_{2i}|}\frac{c_2}{c_1+c_2},$$

where $c_l = \log|\mathfrak{R}_{l1}|$. By (5), it can be easily seen that

$$\sum_{i\in T}\frac{R_{ji}\log|\mathfrak{I}_i|}{\log|\mathfrak{R}_i|} > H(X_T|X_{T^c}) - \frac{1}{c_1+c_2}\sum_{l=1}^{2} c_l H(Y_{\mathfrak{R}_{lT}/\mathfrak{I}_{lT}}|X_{T^c}).$$

Meanwhile, let $\mathfrak{R}_T = \prod_{i\in T}\mathfrak{R}_i$, $\mathfrak{I}_T = \prod_{i\in T}\mathfrak{I}_i$, $\Phi = \{\Phi_{11}\times\Phi_{21}, \Phi_{12}\times\Phi_{22}, \cdots, \Phi_{1s}\times\Phi_{2s}\}$ (Note:

$$\Phi_{1,i}\times\Phi_{2,i} : x_i \mapsto (\Phi_{1,i}(x_i), \Phi_{2,i}(x_i)) \in \mathfrak{R}_i$$

for all $x_i \in \mathscr{X}_i$.) and $Y_{\mathfrak{R}_T/\mathfrak{I}_T} = \Phi(X_T) + \mathfrak{I}_T$. It can be verified that $Y_{\mathfrak{R}_{lT}/\mathfrak{I}_{lT}}$ $(l = 1, 2)$ is a function of $Y_{\mathfrak{R}_T/\mathfrak{I}_T}$, hence, $H(Y_{\mathfrak{R}_T/\mathfrak{I}_T}|X_{T^c}) \geq H(Y_{\mathfrak{R}_{lT}/\mathfrak{I}_{lT}}|X_{T^c})$. Consequently,

$$\sum_{i\in T}\frac{R_{ji}\log|\mathfrak{I}_i|}{\log|\mathfrak{R}_i|} > H(X_T|X_{T^c}) - H(Y_{\mathfrak{R}_T/\mathfrak{I}_T}|X_{T^c}),$$

which implies that $\mathbf{R}_j \in \mathcal{R}_{\Phi,\text{prod}}$ by Theorem B.1. We therefore conclude that $\mathbf{R}_j$ is achievable with linear encoder over $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$ for all feasible j, so is $\mathbf{R}$. ■

Obviously, $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$ in Theorem IV.3 are of the same size. Inductively, one can verify the following without any difficulty.

Theorem IV.4. *Let $\mathscr{L}$ be any finite index set, $\mathfrak{R}_{l1}, \mathfrak{R}_{l2}, \cdots, \mathfrak{R}_{ls}$ $(l \in \mathscr{L})$ be a set of finite rings of equal size, and $\mathfrak{R}_i = \prod_{l\in\mathscr{L}} \mathfrak{R}_{li}$ for all feasible i. If the coding rate $\mathbf{R} \in \mathbb{R}^s$ is achievable with linear encoders over $\mathfrak{R}_{l1}, \mathfrak{R}_{l2}, \cdots, \mathfrak{R}_{ls}$ $(l \in \mathscr{L})$, then $\mathbf{R}$ is achievable with linear encoders over $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$.*

Remark 3. The situation Theorem IV.4 (Theorem IV.3) illustrates is delicate. Let $\mathscr{X}_i$ $(1 \leq i \leq s)$ be the set of all symbols generated by the ith source. The hypothesis of Theorem IV.4 (Theorem IV.3) implicitly implies the constraint $|\mathscr{X}_i| \leq |\mathfrak{R}_{li}|$ for all feasible i and l. As a consequence, Theorem IV.4 (Theorem IV.3) does not imply that linear encoders over $\mathbb{M}_{L,p}\times\mathbb{Z}_{p^2}$ (p is a prime) always achieve the Slepian–Wolf region (since linear encoders over $\mathbb{M}_{L,p}$ and $\mathbb{Z}_{p^2}$ always achieve the Slepian–Wolf region by Theorem IV.1). The correct statement is that linear encoders over $\mathbb{M}_{L,p}\times\mathbb{Z}_{p^2}$ always achieve the Slepian–Wolf region if $|\mathscr{X}_i| \leq p^2$ for all feasible i.

Remark 4. Let $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$ be a set of finite rings each of which is isomorphic to either

1) a ring $\mathfrak{R}$ containing one and only one proper non-trivial left ideal whose order is $\sqrt{|\mathfrak{R}|}$, e.g. $\mathbb{M}_{L,p}$ and $\mathbb{Z}_{p^2}$ (p is a prime); or
2) a ring of a finite product of finite field(s) and/or ring(s) satisfying 1), e.g. $\mathbb{M}_{L,p}\times\prod_{j=1}^{m}\mathbb{Z}_{p_j}$ (p and p_j's are prime) and $\prod_{i=1}^{m'}\mathbb{M}_{L,p_i}\times\prod_{j=1}^{m''}\mathbb{F}_{q_j}$ (m' and m'' are non-negative, p_i's are prime and q_j's are power of primes).

Theorem IV.1 and Theorem IV.4 ensure that linear encoders over ring $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$ are always optimal in any applicable (subjected to the condition presented in related theorem) Slepian–Wolf coding scenario. As a very special case, $\mathbb{Z}_p\times\mathbb{Z}_p$, where p is a prime, is always optimal in any (single source or multiple sources) scenario with alphabet size less than or equal to p. However, using product of rings or a field is not mandatory. As shown in Theorem III.1,

neither $\mathbb{M}_{L,p}$ nor $\mathbb{Z}_{p^2}$ is (isomorphic to) a product of rings nor a field. It is also not required to have a restriction on the alphabet size (see Theorem IV.1), even for product rings (see Example IV.5 for a case of $\mathbb{Z}_2 \times \mathbb{Z}_3$).

Example IV.5. Consider the single source scenario, where $X_1 \sim p$ and $\mathscr{X}_1 = \mathbb{Z}_6$, satisfying the follows.

X_1	0	1	2	3	4	5
$p(X_1)$	0.05	0.1	0.15	0.2	0.2	0.3

By [8, Theorem IV.1],

$$\begin{aligned}\mathcal{R} &= \{R_1 \in \mathbb{R} | R_1 > \max\{2.40869, 2.34486, 2.24686\}\} \\ &= \{R_1 \in \mathbb{R} | R_1 > 2.40869 = H(X_1)\}\end{aligned}$$

is achievable with linear coding over ring $\mathbb{Z}_6$. Obviously, $\mathcal{R}$ is just the SW region $\mathcal{R}[X_1]$. Optimality is claimed.

V. Conclusion

For any data compression problem of Slepian–Wolf, one can always select finite rings which can be (isomorphic to) either $\mathbb{M}_{L,p}$, $\mathbb{Z}_{p^2}$ (p is a prime), a field or a product ring of several previous rings. It is guaranteed that linear encoders over these rings are optimal, respectively. Therefore, the optimality issue considered is closed on the regard of existence. However, the ultimate target is to verify (or deny) that (2) is the Slepian–Wolf region for all possible choices of rings. From this viewpoint, the problem remains open.

Acknowledgment

The authors would like to wish the Communication Theory Lab of KTH a very merry Christmas!

Appendix A
A Supporting Lemma

Lemma A.1. *Let $\mathfrak{R}$ be a finite ring, X and Y be two correlated discrete random variables, and $\mathscr{X}$ be the sample space of X with $|\mathscr{X}| \leq |\mathfrak{R}|$. If $\mathfrak{R}$ contains one and only one proper non-trivial left ideal $\mathfrak{I}$ and $|\mathfrak{I}| = \sqrt{|\mathfrak{R}|}$, then there exists injection $\tilde{\Phi} : \mathscr{X} \to \mathfrak{R}$ such that*

$$H(X|Y) \leq 2H(\tilde{\Phi}(X) + \mathfrak{I}|Y). \tag{A.1}$$

Proof: Let

$$\tilde{\Phi} \in \arg\max_{\Phi \in \mathscr{M}} H(\Phi(X) + \mathfrak{I}|Y),$$

where $\mathscr{M}$ is the set of all possible Φ's (maximum can always be reached because $|\mathscr{M}| = \dfrac{|\mathfrak{R}|!}{(|\mathfrak{R}| - |\mathscr{X}|)!}$ is finite, but it is not uniquely attained by $\tilde{\Phi}$ in general). Assume that $\mathscr{Y}$ is the sample space (not necessarily finite) of Y.

Let $q = |\mathfrak{I}|$, $\mathfrak{I} = \{r_1, r_2, \cdots, r_q\}$ and $\mathfrak{R}/\mathfrak{I} = \{a_1 + \mathfrak{I}, a_2 + \mathfrak{I}, \cdots, a_q + \mathfrak{I}\}$. We have that

$$H(X|Y) = -\sum_{y\in\mathscr{Y}}\sum_{i,j=1}^{q} p_{i,j,y}\log\frac{p_{i,j,y}}{p_y} \text{ and}$$
$$H(\tilde{\Phi}(X) + \mathfrak{I}|Y) = -\sum_{y\in\mathscr{Y}}\sum_{i=1}^{q} p_{i,y}\log\frac{p_{i,y}}{p_y},$$

where

$$p_{i,j,y} = \Pr\left\{\tilde{\Phi}(X) = a_i + r_j, Y = y\right\},$$
$$p_y = \sum_{i,j=1}^{q} p_{i,j,y},$$
$$p_{i,y} = \sum_{j=1}^{q} p_{i,j,y}.$$

(Note: $\Pr\left\{\tilde{\Phi}(X) = r\right\} = 0$ if $r \in \mathfrak{R} \setminus \tilde{\Phi}(\mathscr{X})$. In addition, every element in $\mathfrak{R}$ can be uniquely expressed as $a_i + r_j$.) Therefore, (A.1) is equivalent to

$$-\sum_{y\in\mathscr{Y}}\sum_{i,j=1}^{q} p_{i,j,y}\log\frac{p_{i,j,y}}{p_y} \leq -2\sum_{y\in\mathscr{Y}}\sum_{i=1}^{q} p_{i,y}\log\frac{p_{i,y}}{p_y}$$
$$\Leftrightarrow \sum_{y\in\mathscr{Y}} p_y \sum_{i=1}^{q}\frac{p_{i,y}}{p_y} H\left(\frac{p_{i,1,y}}{p_{i,y}}, \frac{p_{i,2,y}}{p_{i,y}}, \cdots, \frac{p_{i,q,y}}{p_{i,y}}\right) \leq \sum_{y\in\mathscr{Y}} p_y H\left(\frac{p_{1,y}}{p_y}, \frac{p_{2,y}}{p_y}, \cdots, \frac{p_{q,y}}{p_y}\right), \tag{A.2}$$

where $H(v_1, v_2, \cdots, v_q) = -\sum_{j=1}^{q} v_j \log v_j$. Let

$$A = \sum_{y\in\mathscr{Y}} p_y H\left(\sum_{i=1}^{q}\frac{p_{i,1,y}}{p_y}, \sum_{i=1}^{q}\frac{p_{i,2,y}}{p_y}, \cdots, \sum_{i=1}^{q}\frac{p_{i,q,y}}{p_y}\right).$$

The concavity of the function H implies that

$$\sum_{y\in\mathscr{Y}} p_y \sum_{i=1}^{q}\frac{p_{i,y}}{p_y} H\left(\frac{p_{i,1,y}}{p_{i,y}}, \frac{p_{i,2,y}}{p_{i,y}}, \cdots, \frac{p_{i,q,y}}{p_{i,y}}\right) \leq A. \tag{A.3}$$

At the same time,

$$\sum_{y\in\mathscr{Y}} p_y H\left(\frac{p_{1,y}}{p_y}, \frac{p_{2,y}}{p_y}, \cdots, \frac{p_{q,y}}{p_y}\right) = \max_{\Phi\in\mathscr{M}} H(\Phi(X) + \mathfrak{I}|Y)$$

by the definition of $\tilde{\Phi}$. We now claim that

$$A \leq \max_{\Phi\in\mathscr{M}} H(\Phi(X) + \mathfrak{I}|Y). \tag{A.4}$$

Suppose otherwise, i.e. $A > \sum_{y\in\mathscr{Y}} p_y H\left(\frac{p_{1,y}}{p_y}, \frac{p_{2,y}}{p_y}, \cdots, \frac{p_{q,y}}{p_y}\right)$. Let $\Phi' : \mathscr{X} \to \mathfrak{R}$ be defined as

$$\Phi' : x \mapsto a_j + r_i \Leftrightarrow \tilde{\Phi}(x) = a_i + r_j.$$

We have that

$$H(\Phi'(X)+\mathfrak{I}|Y) = \sum_{y\in\mathscr{Y}} p_y H\left(\sum_{i=1}^{q}\frac{p_{i,1,y}}{p_y}, \sum_{i=1}^{q}\frac{p_{i,2,y}}{p_y}, \cdots, \sum_{i=1}^{q}\frac{p_{i,q,y}}{p_y}\right) = A$$
$$> \sum_{y\in\mathscr{Y}} p_y H\left(\frac{p_{1,y}}{p_y}, \frac{p_{2,y}}{p_y}, \cdots, \frac{p_{q,y}}{p_y}\right) = \max_{\Phi\in\mathscr{M}} H(\Phi(X)+\mathfrak{I}|Y).$$

It is absurd that $H(\Phi'(X)+\mathfrak{I}|Y) > \max_{\Phi\in\mathscr{M}} H(\Phi(X)+\mathfrak{I}|Y)$! Therefore, (A.2) is valid by (A.3) and (A.4), so is (A.1). ∎

APPENDIX B
ACHIEVABILITY THEOREM OF PRODUCT RINGS

Theorem B.1. *Suppose $\mathfrak{R}_i$ ($1\le i\le s$) is a (finite) product ring $\prod_{l=1}^{k_i}\mathfrak{R}_{l,i}$ of finite rings $\mathfrak{R}_{l,i}$'s, and the sample space $\mathscr{X}_i$ satisfies $|\mathscr{X}_i|\le|\mathfrak{R}_{l,i}|$ for all feasible i and l. Given injections $\Phi_{l,i}:\mathscr{X}_i\to\mathfrak{R}_{l,i}$ and let*

$$\Phi = \{\Phi_1, \Phi_2, \cdots, \Phi_s\},$$

where $\Phi_i = \prod_{l=1}^{k_i}\Phi_{l,i}$ is defined as

$$\Phi_i : x_i \mapsto (\Phi_{1,i}(x_i), \Phi_{2,i}(x_i), \cdots, \Phi_{k_i,i}(x_i)) \in \mathfrak{R}_i, \forall\, x_i\in\mathscr{X}_i.$$

We have that

$$\mathcal{R}_{\Phi,\text{prod}} = \Bigg\{ [R_1, R_2, \cdots, R_s]\in\mathbb{R}^s \Bigg| \sum_{i\in T}\frac{R_i\log|\mathfrak{I}_i|}{\log|\mathfrak{R}_i|} > H(X_T|X_{T_c}) - H(Y_{\mathfrak{R}_T/\mathfrak{I}_T}|X_{T^c}),$$
$$\forall\,\emptyset\ne T\subseteq\mathcal{S}, \forall\,\mathfrak{I}_i = \prod_{l=1}^{k_i}\mathfrak{I}_{l,i} \text{ with } 0\ne\mathfrak{I}_{l,i}\le_l\mathfrak{R}_{l,i}\Bigg\} \tag{B.1}$$

is directly achievable with linear coding over ring $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$. Moreover, $\mathcal{R}_\Phi\subseteq\mathcal{R}_{\Phi,\text{prod}}$.

Proof: The proof follows almost the same as the one proving [8, Theorem IV.1], except that the analysis of the performances (of the encoders and decoder) only focuses on sequences $(a_{i,1}, a_{i,2}, \cdots, a_{i,n})\in\mathfrak{R}_i^n$ ($1\le i\le s$) such that

$$a_{i,j} = \left(\Phi_{1,i}\left(x_i^{(j)}\right), \Phi_{2,i}\left(x_i^{(j)}\right), \cdots, \Phi_{k_i,i}\left(x_i^{(j)}\right)\right) \in \prod_{l=1}^{k_i}\mathfrak{R}_{l,i}$$

for some $x_i^{(j)}\in\mathscr{X}_i$. Let $\mathbf{X}_i, \mathbf{Y}_i$ be any two such sequences satisfying $\mathbf{X}_i-\mathbf{Y}_i\in\mathfrak{I}_i^n$ for some $\mathfrak{I}_i\le_l\mathfrak{R}_i$. Based on the special structure of $\mathbf{X}_i$ and $\mathbf{Y}_i$, it is easy to verify that $\mathfrak{I}_i\ne 0 \Leftrightarrow \mathfrak{I}_i = \prod_{l=1}^{k_i}\mathfrak{I}_{l,i}$ and $0\ne\mathfrak{I}_{l,i}\le_l\mathfrak{R}_{l,i}$, for all $1\le l\le k_i$. (This causes the difference between (1) and (B.1).) In addition, it is obvious that $\mathcal{R}_\Phi\subseteq\mathcal{R}_{\Phi,\text{prod}}$ by their definitions. ∎

Remark 5. The differences between (1) and (B.1) are in the restrictions of $\mathfrak{I}_i$'s, respectively. The reason causing the differences is highlighted in the proof.

REFERENCES

[1] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Transactions on Information Theory*, vol. 19, no. 4, pp. 471–480, Jul. 1973.

[2] P. Elias, "Coding for noisy channels," *IRE Conv. Rec.*, pp. 37–46, Mar. 1955.

[3] I. Csiszár, "Linear codes for sources and source networks: Error exponents, universal coding," *IEEE Transactions on Information Theory*, vol. 28, no. 4, pp. 585–592, Jul. 1982.

[4] J. Körner and K. Marton, "How to encode the modulo-two sum of binary sources," *IEEE Transactions on Information Theory*, vol. 25, no. 2, pp. 219–221, Mar. 1979.

[5] 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 Transactions on Information Theory*, vol. 29, no. 3, pp. 396–411, May 1983.

[6] S. Huang and M. Skoglund, "Polynomials and computing functions of correlated sources," in *IEEE International Symposium on Information Theory*, Jul. 2012, pp. 771–775.

[7] ——, "Computing polynomial functions of correlated sources: Inner bounds," in *International Symposium on Information Theory and its Applications*, Oct. 2012, pp. 160–164.

[8] ——, "On achievability of linear source coding over finite rings," in *IEEE International Symposium on Information Theory*, July 2013.

[9] ——, "On linear coding over finite rings and applications to computing," *IEEE Transactions on Information Theory*, Submitted (1st version). [Online]. Available: http://www.ee.kth.se/∼sheng11