On Existence of Optimal Linear Encoders over Non-field Rings for Data Compression with Application to Computing

Sheng Huang, Mikael Skoglund
Communication Theory Lab, School of Electrical Engineering
KTH Royal Institute of Technology
Stockholm, Sweden
Email: sheng.huang@ee.kth.se, skoglund@ee.kth.se

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

Based on this, we address a variation of the data compression problem which considers recovering some discrete function of the data. It is demonstrated that linear encoder over non-field ring strictly outperforms its field counterpart for encoding some function in terms of achieving strictly larger achievable region with strictly smaller alphabet size.

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 characterized by the Slepian–Wolf region [1]. Although [1] guarantees that there always exist encoders achieving the data compression limit, the structures of the encoders are unclear. This confines the scope of their applications. Fortunately, [2] and [3] prove that linear encoder over finite *field* achieves 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 (see Problem 1) [4], [5], [6], [7], [8]. However, special constraints are casted upon the algebraic structures of finite fields. For instance, the *characteristic* of a finite field has to be a prime; the size of a finite field must be a power of a prime; up to *isomorphism*, there is only one finite field of a fixed size and etc. These restrictions limit the performance of linear encoders over fields (see Example V.3 or [9]). As a consequence, linear encoder over finite *ring* is proposed [9], [10], [11].

Demonstrated in [9], [11], 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. Nevertheless, 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 achieves the Slepian–Wolf region. This article will prove that there always exist linear encoders over non-field rings that achieve the data compression limit, the Slepian–Wolf region, in any scenarios. In other words, the achievable region [11, region (8)] (see (2)) is indeed the Slepian–Wolf region. Therefore, the optimality issue is closed on this regard.

Additionally, this paper also addresses the problem of source coding for computing (see Problem 1). We propose applying linear encoder over ring to the "polynomial approach" introduced in [7], [8] which originally uses linear encoder over field. We will demonstrate that linear encoder over non-field ring dominates the field version in terms of achieving larger achievable regions for encoding many functions (see Example V.3). In fact, there exist infinitely many such functions. Thus, it is worthwhile to further investigate this new encoding technique.

II. Linear Source Coding over Finite Rings

Generally speaking, the datum generated by a source is not necessarily associated with any specific algebraic structure. In order to apply the linear encoders (over rings), 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*[1] $|\mathfrak{R}_i| \geq |\mathscr{X}_i|$ 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 $\mathfrak{R}_i$ (see [11, Proposition II.4]). Similarly, we often write $\mathfrak{I}_T$ for the left ideal $\prod_{i\in T} \mathfrak{I}_i$. Meanwhile, we usually write 0 for the *trivial ideal* $\{0\}$, use $\mathfrak{I} \leq_l \mathfrak{R}$ to indicate that the subset $\mathfrak{I}$ is a left ideal of the ring $\mathfrak{R}$ and designate $\mathfrak{R}/\mathfrak{I}$ as the *quotient group* $\mathfrak{R}$ mod $\mathfrak{I}$. Let $[X_1, X_2, \cdots, X_s] \sim p$ and

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

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 $\mathfrak{R}_T/\mathfrak{I}_T$. [11, Theorem IV.1] proves that $\mathcal{R}_\Phi$ is *achievable* with linear encoders over $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$. 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* [11, Definition II.5] to be more precise) $\phi_i : \mathfrak{R}_i^n \to \mathfrak{R}_i^{k_i}$ ($i \in \mathcal{S}$) and a decoder ψ, such that

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

where $\mathbf{X}_i = \left[\Phi_i\left(X_i^{(1)}\right), \Phi_i\left(X_i^{(2)}\right), \cdots, \Phi_i\left(X_i^{(n)}\right)\right]^t$, 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

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

[1] The number of elements of a finite group / field / ring / left (right) ideal.

sharing argument, it is noticeable that

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

where $\mathscr{M}$ is the family of all possible Φ's and $\operatorname{cov}(A)$ 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 $\Phi \in \mathscr{M}$.

Clearly, for every $\Phi \in \mathscr{M}$, $\mathcal{R}_\Phi$ is the Slepian–Wolf region

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

if all $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$ are all fields [9], [11]. We claim, in this paper, the 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. 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 the Slepian–Wolf region

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

is equivalent to claiming that 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. Let $\mathbb{Z}_q$ be the *modulo integer ring* of order q. 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 $\mathbb{Z}_{p^2}$ with a big enough p. 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 $H(Y_{\mathfrak{R}_1/\mathfrak{I}_0})$. Let $\tilde{\Phi}_1 \in \arg\max_{\Phi_1\in\mathscr{M}} H(Y_{\mathfrak{R}_1/\mathfrak{I}_0})$, where $\mathscr{M}$ is the set of all possible Φ_1's (maximum can always be reached because $|\mathscr{M}| = \frac{|\mathfrak{R}_1|!}{(|\mathfrak{R}_1| - |\mathscr{X}_1|)!}$ is finite, but it is not uniquely attained by $\tilde{\Phi}_1$ in general). We claim that (3) is valid, i.e. (2) is the Slepian–Wolf region, if $\Phi_1 = \tilde{\Phi}_1$. 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,

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

Hence, (3) is equivalent to

$$\frac{\log|\mathfrak{R}_1|}{\log|\mathfrak{I}_0|}\left[H(X_1) - H(Y_{\mathfrak{R}_1/\mathfrak{I}_0})\right] \leq H(X_1) \tag{4}$$

$$\Leftrightarrow H(X_1) \leq 2H(Y_{\mathfrak{R}_1/\mathfrak{I}_0}), \tag{5}$$

since $|\mathfrak{I}_0| = \sqrt{|\mathfrak{R}_1|}$. Let $q = |\mathfrak{I}_0|$, $\mathfrak{I}_0 = \{r_1, r_2, \cdots, r_q\}$ and $\mathfrak{R}_1/\mathfrak{I}_0 = \{a_1 + \mathfrak{I}_0, a_2 + \mathfrak{I}_0, \cdots, a_q + \mathfrak{I}_0\}$. We have that

$$H(X_1) = -\sum_{i,j=1}^{q} p_{i,j} \log p_{i,j} \text{ and}$$

$$H(Y_{\mathfrak{R}_1/\mathfrak{I}_0}) = -\sum_{i=1}^{q} p_i \log p_i,$$

where $p_{i,j} = \Pr\left\{\tilde{\Phi}_1(X_1) = a_i + r_j\right\}$ and $p_i = \sum_{j=1}^{q} p_{i,j}$. (Note: $\Pr\left\{\tilde{\Phi}_1(X_1) = r\right\} = 0$ if $r \in \mathfrak{R}_1 \setminus \tilde{\Phi}_1(\mathscr{X}_1)$; every element in $\mathfrak{R}_1$ can be uniquely expressed as $a_i + r_j$.) Therefore, (5) is equivalent to

$$-\sum_{i,j=1}^{q} p_{i,j} \log p_{i,j} \leq -2\sum_{i=1}^{q} p_i \log p_i \Leftrightarrow$$

$$\sum_{i=1}^{q} p_i H\left(\frac{p_{i,1}}{p_i}, \frac{p_{i,2}}{p_i}, \cdots, \frac{p_{i,q}}{p_i}\right) \leq H\left(p_1, p_2, \cdots, p_q\right), \tag{6}$$

where $H\left(v_1, v_2, \cdots, v_q\right) = -\sum_{j=1}^{q} v_j \log v_j$. Let $A = H\left(\sum_{i=1}^{q} p_{i,1}, \sum_{i=1}^{q} p_{i,2}, \cdots, \sum_{i=1}^{q} p_{i,q}\right)$. The concavity of the function H implies that

$$\sum_{i=1}^{q} p_i H\left(\frac{p_{i,1}}{p_i}, \frac{p_{i,2}}{p_i}, \cdots, \frac{p_{i,q}}{p_i}\right) \leq A. \tag{7}$$

At the same time, $H\left(p_1, p_2, \cdots, p_q\right) = \max_{\Phi_1\in\mathscr{M}} H(Y_{\mathfrak{R}_1/\mathfrak{I}_0})$ by the definition of $\tilde{\Phi}_1$ and $Y_{\mathfrak{R}_1/\mathfrak{I}_0}$. We now claim that

$$A \leq H\left(p_1, p_2, \cdots, p_q\right). \tag{8}$$

Suppose otherwise, i.e. $A > H\left(p_1, p_2, \cdots, p_q\right)$. Let $\Phi_1' : \mathscr{X}_1 \to \mathfrak{R}_1$ be defined as

$$\Phi_1' : x \mapsto a_j + r_i \text{ if and only if } \tilde{\Phi}_1(x) = a_i + r_j.$$

When $\Phi_1 = \Phi_1'$,

$$\begin{aligned} H(Y_{\mathfrak{R}_1/\mathfrak{I}_0}) =& H\left(\sum_{i=1}^{q} p_{i,1}, \sum_{i=1}^{q} p_{i,2}, \cdots, \sum_{i=1}^{q} p_{i,q}\right) = A \\ >& H\left(p_1, p_2, \cdots, p_q\right) = \max_{\Phi_1\in\mathscr{M}} H(Y_{\mathfrak{R}_1/\mathfrak{I}_0}). \end{aligned}$$

$H(Y_{\mathfrak{R}_1/\mathfrak{I}_0}) > \max_{\Phi_1\in\mathscr{M}} H(Y_{\mathfrak{R}_1/\mathfrak{I}_0})$ is absurd! Therefore, (6) is valid by (7) and (8), so are (5) and (4). ■

Up to isomorphism, there are exactly 4 distinct rings of order p^2 for any 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 unique field $\mathbb{F}_{p^2}$ ($\mathbb{F}_q$ is defined to be a field of order q). It has been proved that, with linear encoders over the last three, optimality can always be achieved in the single source scenario. In next section, we will see that linear encoders over any of this three are also optimal for any multiple sources scenario (see Theorem IV.1). In addition, we prove that the same holds true for $\mathbb{Z}_p \times \mathbb{Z}_p$ in appropriate situation (detailed in Remark 3). In fact, this follows as a special case of a much stronger result, Theorem IV.2. It includes but is not limited to the assertion that linear encoders over $\prod_{j=1}^{m} \mathbb{Z}_p$ ($m \in \mathbb{N}^+$) are optimal for any suitable (detailed in Remark 3) data compression circumstance of Slepian–Wolf.

IV. Existence Theorem II: Multiple Sources

We present the existence results of the multiple sources scenario in this section.

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 a field; or 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 also include $\mathbb{M}_{L,p}$ 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 (see [12]). Nevertheless, all rates are directly achievable if $\mathfrak{R}_i$'s are fields or if $s = 1$ (see Theorem III.1).

Theorem IV.2. *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 directly achievable with linear encoders over $\mathfrak{R}_{l1}, \mathfrak{R}_{l2}, \cdots, \mathfrak{R}_{ls}$ for all $l \in \mathscr{L}$, then $\mathbf{R}$ is directly achievable with linear encoders over $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$.*

Proof: Let $\mathbf{R} = [R_1, R_2, \cdots, R_s]$. By definition, there exist injections $\Phi_l = \{\Phi_{l1}, \Phi_{l2}, \cdots, \Phi_{ls}\}$ ($l \in \mathscr{L}$), where $\Phi_{li} : \mathscr{X}_i \rightarrow \mathfrak{R}_{li}$, such that, $\forall\, \emptyset \neq T \subseteq \mathcal{S}$, $\forall\, 0 \neq \mathfrak{I}_{li} \leq_l \mathfrak{R}_{li}$,

$$\sum_{i \in T} \frac{R_i \log |\mathfrak{I}_{li}|}{\log |\mathfrak{R}_{li}|} > H(X_T | X_{T^c}) - H(Y_{\mathfrak{R}_{lT}/\mathfrak{I}_{lT}} | X_{T^c}),$$

where $\mathfrak{R}_{lT} = \prod_{i \in T} \mathfrak{R}_{li}$, $\mathfrak{I}_{lT} = \prod_{i \in T} \mathfrak{I}_{li}$ and $Y_{\mathfrak{R}_{lT}/\mathfrak{I}_{lT}} = \Phi_l(X_T) + \mathfrak{I}_{lT}$. Let $\Phi = \{\Phi'_1, \Phi'_2, \cdots, \Phi'_s\}$, where

$$\Phi'_i : x_i \mapsto \prod_{l \in \mathscr{L}} \Phi_{li}(x_i); \forall\, x_i \in \mathscr{X}_i \;(1 \leq i \leq s).$$

For any $0 \neq \mathfrak{I}_i \leq_l \mathfrak{R}_i$, we have that $\mathfrak{I}_i = \prod_{l \in \mathscr{L}} \mathfrak{I}_{li}$ for some $\mathfrak{I}_{li} \leq_l \mathfrak{R}_{li}$ by [11, Proposition II.4]. Consequently, for any $\emptyset \neq T \subseteq \mathcal{S}$,

$$\begin{aligned}\sum_{i \in T} \frac{R_i \log |\mathfrak{I}_i|}{\log |\mathfrak{R}_i|} &= \sum_{l \in \mathscr{L}} \sum_{i \in T} \frac{R_i \log |\mathfrak{I}_{li}|}{\log |\mathfrak{R}_{li}|} \frac{c_l}{\sum_{l \in \mathscr{L}} c_l}\\
&> H(X_T | X_{T^c}) - \frac{1}{\sum_{l \in \mathscr{L}} c_l} \sum_{l \in \mathscr{L}} c_l H(Y_{\mathfrak{R}_{lT}/\mathfrak{I}_{lT}} | X_{T^c})\\
&> H(X_T | X_{T^c}) - H(Y_{\mathfrak{R}_T/\mathfrak{I}_T} | X_{T^c})\end{aligned}$$

where $c_l = \log |\mathfrak{R}_{l1}|$ and the last inequality follows from the fact that $Y_{\mathfrak{R}_{lT}/\mathfrak{I}_{lT}}$ is a function of $Y_{\mathfrak{R}_T/\mathfrak{I}_T}$. Therefore, $\mathbf{R}$ is contained in the region (1), namely $\mathbf{R}$ is directly achievable with linear encoders over $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$. ■

Remark 3. The situation Theorem IV.2 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.2 implicitly implies the constraint $|\mathscr{X}_i| \leq |\mathfrak{R}_{li}|$ for all feasible i and l. As a consequence, Theorem IV.2 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 $\mathfrak{I}_0$ and $|\mathfrak{I}_0| = \sqrt{|\mathfrak{R}|}$, e.g. $\mathbb{M}_{L,p}$ and $\mathbb{Z}_{p^2}$; or
2) a ring of a finite product of finite field(s) and 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).

Theorem IV.1 and Theorem IV.2 ensure that linear encoders over ring $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$ are always optimal in any applicable Slepian–Wolf coding scenario. Moreover, it is clear that $\mathfrak{R}_i$ ($1 \leq i \leq s$), e.g. $\mathbb{M}_{L,p}$ and $\mathbb{Z}_{p^2}$, is not necessary a field or a product of rings.

So far, we have only shown that there exist linear encoders over non-field rings that are equally good as their field counterparts. In next section, a variation of the Slepian–Wolf coding problem is considered. It will be demonstrated that the non-field ring version can *strictly outperform the field version* in (infinitely) many circumstances.

V. Application: Source Coding for Computing

This section considers the problem of *source coding for computing* defined as follows:

Problem 1 (Source Coding for Computing)**.** Given $\mathcal{S} = \{1, 2, \cdots, s\}$ and $(X_1, X_2, \cdots, X_s) \sim p$. Let t_i ($i \in \mathcal{S}$) be a discrete memoryless source that randomly generates i.i.d. discrete data $X_i^{(1)}, X_i^{(2)}, \cdots, X_i^{(n)}, \cdots$, where $X_i^{(n)}$ has a finite sample space $\mathscr{X}_i$ and $\left[X_1^{(n)}, X_2^{(n)}, \cdots, X_s^{(n)}\right] \sim p$, $\forall\, n \in \mathbb{N}^+$. For a *discrete function* $g : \prod_{i \in \mathcal{S}} \mathscr{X}_i \rightarrow \Omega$, what is the largest region $\mathcal{R}[g] \subset \mathbb{R}^s$, such that, $\forall\, (R_1, R_2, \cdots, R_s) \in \mathcal{R}[g]$ and $\forall\, \epsilon > 0$, there exists an $N_0 \in \mathbb{N}^+$, such that, for all $n > N_0$, there exist s encoders $\phi_i : \mathscr{X}_i^n \rightarrow \left[1, 2^{nR_i}\right], i \in \mathcal{S}$, and one decoder $\psi : \prod_{i \in \mathcal{S}} \left[1, 2^{nR_i}\right] \rightarrow \Omega^n$ with

$$\Pr\left\{\vec{g}\left(X_1^n, \cdots, X_s^n\right) \neq \psi\left[\phi_1\left(X_1^n\right), \cdots, \phi_s\left(X_s^n\right)\right]\right\} < \epsilon,$$

where $X_i^n = \left[X_i^{(1)}, X_i^{(2)}, \cdots, X_i^{(n)}\right]$ and

$$\vec{g}\left(X_1^n, \cdots, X_s^n\right) = \begin{bmatrix} g\left(X_1^{(1)}, \cdots, X_s^{(1)}\right) \\ \vdots \\ g\left(X_1^{(n)}, \cdots, X_s^{(n)}\right) \end{bmatrix} \in \Omega^n?$$

The region $\mathcal{R}[g]$ is called the *achievable coding rate region* for computing g. A region $\mathcal{R} \subset \mathbb{R}^s$ is said to be *achievable* for computing g (or simply achievable) if and only if $\mathcal{R} \subseteq \mathcal{R}[g]$.

Obviously, $\mathcal{R}[g]$ always contains the Slepian–Wolf region, and it coincides with the Slepian–Wolf region if g is an identity function. Unfortunately, $\mathcal{R}[g]$ is unknown for an arbitrary g in general. One of the difficulties of tackling the general problem is that g is often with an unclear structure, e.g. the g given by (13). Fortunately, [7, Lemma A.2] points out that any discrete function with a finite domain is essentially a *polynomial function* over some finite ring (including field). Moreover, such a polynomial function always admits a *presentation* as $\hat{g}$ in (9) (a concrete example is given in Example V.3). Therefore, we can shrink the domain of consideration of Problem 1 to polynomial functions with presentation (9).

Let $\mathfrak{R}[s]$ be the set of all polynomial functions of s variables over ring $\mathfrak{R}$.

Theorem V.1. *If $\hat{g} \in \mathfrak{R}[s]$ admits*

$$\hat{g} = h \circ k, \text{ where } k(x_1, x_2, \cdots, x_s) = \sum_{i=1}^{s} k_i(x_i), \tag{9}$$

and $h, k_i \in \mathfrak{R}[1]$ for all feasible i, then

$$\begin{aligned}\mathcal{R}_{\hat{g}} = \Big\{ &(r, r, \cdots, r) \in \mathbb{R}^s \Big| r > \\ &\max_{0 \neq \mathfrak{I} \leq_l \mathfrak{R}} \frac{\log |\mathfrak{R}|}{\log |\mathfrak{I}|} \left[H(X) - H(Y_{\mathfrak{R}/\mathfrak{I}})\right] \Big\} \subseteq \mathcal{R}[\hat{g}],\end{aligned} \tag{10}$$

where $X = k(X_1, X_2, \cdots, X_s)$ and $Y_{\mathfrak{R}/\mathfrak{I}} = X + \mathfrak{I}$ is a random variable with sample space $\mathfrak{R}/\mathfrak{I}$.

Proof: By [11, Theorem IV.1], $\forall\, \epsilon > 0$, there exists a large enough n, an $m \times n$ matrix (linear encoder) $\mathbf{A} \in \mathfrak{R}^{m \times n}$ and a decoder ψ, such that $\Pr\left\{X^n \neq \psi\left(\mathbf{A}X^n\right)\right\} < \epsilon$, if $m >$

$\max_{0 \neq \mathfrak{I} \leq_l \mathfrak{R}} \dfrac{n\left[H(X) - H(Y_{\mathfrak{R}/\mathfrak{I}})\right]}{\log|\mathfrak{I}|}$. Let $\phi_i = \mathbf{A} \circ \vec{k}_i$ $(1 \leq i \leq s)$ be the encoder of the ith source. Upon receiving $\phi_i(X_i^n)$ from the ith source, the decoder claims that $\vec{h}(\hat{X}^n)$, where $\hat{X}^n = \psi\left[\sum_{i=1}^{s} \phi_i\left(X_i^n\right)\right]$, is the function, namely $\hat{g}$, subject to computation. The probability of decoding error is

$$\begin{aligned}
&\Pr\left\{\vec{h}\left[\vec{k}\left(X_1^n, X_2^n, \cdots, X_s^n\right)\right] \neq \vec{h}(\hat{X}^n)\right\}\\
\leq &\Pr\left\{X^n \neq \hat{X}^n\right\}\\
= &\Pr\left\{X^n \neq \psi\left[\sum_{i=1}^{s} \phi_i\left(X_i^n\right)\right]\right\}\\
= &\Pr\left\{X^n \neq \psi\left[\sum_{i=1}^{s} \mathbf{A}\vec{k}_i\left(X_i^n\right)\right]\right\}\\
= &\Pr\left\{X^n \neq \psi\left[\mathbf{A}\sum_{i=1}^{s} \vec{k}_i\left(X_i^n\right)\right]\right\}\\
= &\Pr\left\{X^n \neq \psi\left[\mathbf{A}\vec{k}\left(X_1^n, X_2^n, \cdots, X_s^n\right)\right]\right\}\\
= &\Pr\left\{X^n \neq \psi\left(\mathbf{A}X^n\right)\right\} < \epsilon.
\end{aligned}$$

From this we conclude that $(r, r, \cdots, r) \in \mathbb{R}^s$ with $r = \dfrac{m \log|\mathfrak{R}|}{n} > \max_{0 \neq \mathfrak{I} \leq_l \mathfrak{R}} \dfrac{\log|\mathfrak{R}|}{\log|\mathfrak{I}|}\left[H(X) - H(Y_{\mathfrak{R}/\mathfrak{I}})\right]$ is achievable, i.e. $\mathcal{R}_{\hat{g}} \subseteq \mathcal{R}[\hat{g}]$. ■

Remark 5. In fact, $\mathcal{R}_{\hat{g}}$ in Theorem V.1 is not the largest achievable region we can achieve. One can reprove all results in [8] by simply replacing the linear encoder over field used in that work by linear encoder over ring. This leads to solutions applied to polynomial functions presented in other formats, e.g.

$$h\left[k_0(x_1, x_2, \cdots, x_{s_0}), \sum_{j=s_0+1}^{s} k_j(x_j)\right], 0 \leq s_0 < s, \tag{11}$$

where h, k_0, k_j's $(s_0 < j \leq s)$ are polynomial functions over the same ring. The new achievable region always includes $\mathcal{R}_{\hat{g}}$ and the Slepian–Wolf region. Due to space limitation, we can only prove Theorem V.1 with the purpose of showing the mechanism while include one modified theorem from [8] without proof in the following. Notice that [7, Lemma A.2] guarantees that every discrete function with a finite domain admits a polynomial presentation of format (9), a special case of (11) and other formats in [8]. Hence, the "polynomial approach" always offers a universal solution to Problem 1.

Theorem V.2. *Let $\mathcal{S}_0 = \{1, 2, \cdots, s_0\} \subseteq \mathcal{S} = \{1, 2, \cdots, s\}$. If $\hat{g} \in \mathfrak{R}[s]$ is given by* (11)*, then $\mathcal{R}[\hat{g}]$ is inner bounded by the region given by,*

$$\begin{aligned}
\sum_{j \in T} R_j \geq |T \setminus \mathcal{S}_0| \max_{0 \neq \mathfrak{I} \leq_l \mathfrak{R}} \frac{\log|\mathfrak{R}|}{\log|\mathfrak{I}|}\left[H(X|V_{\mathcal{S}}) - H(Y_{\mathfrak{R}/\mathfrak{I}}|V_{\mathcal{S}})\right]&\\
+ I(Y_T; V_T|V_{T^c}), \forall\, \emptyset \neq T \subseteq \mathcal{S},& \qquad (12)
\end{aligned}$$

where $\forall\ j \in \mathcal{S}_0$, $V_j = Y_j = X_j$; $\forall\ j \in \mathcal{S} \setminus \mathcal{S}_0$, $Y_j = k_j(X_j)$, V_j's are discrete random variables such that

$$\begin{aligned}
&p(y_1, y_2, \cdots, y_s, v_1, v_2, \cdots, v_s)\\
=&p(y_1, y_2, \cdots, y_s)\prod_{j=s_0+1}^{s} p(v_j|y_j),
\end{aligned}$$

and $X = \sum_{j=s_0+1}^{s} Y_j$, $Y_{\mathfrak{R}/\mathfrak{I}} = X + \mathfrak{I}$.

Remark 6. The achievable region given by (12) always contains the Slepian–Wolf region and is in general larger than the $\mathcal{R}_{\hat{g}}$ from (10).

We conclude our discussion with the following example and some related propositions. This example draws a comparison between fields and non-field rings in the setting of a computing problem. It shows that linear encoder over non-field ring is strictly better than over field (any field). To be more precise, the first achieves strictly larger achievable region with strictly smaller alphabet size.

Example V.3. Let $g : \{\alpha_0, \alpha_1\}^3 \to \{\beta_0, \beta_1, \beta_2, \beta_3\}$ (Fig 1) be a function such that

$$\begin{aligned}
g &: (\alpha_0, \alpha_0, \alpha_0) \mapsto \beta_0; & g &: (\alpha_0, \alpha_0, \alpha_1) \mapsto \beta_3;\\
g &: (\alpha_0, \alpha_1, \alpha_0) \mapsto \beta_2; & g &: (\alpha_0, \alpha_1, \alpha_1) \mapsto \beta_1;\\
g &: (\alpha_1, \alpha_0, \alpha_0) \mapsto \beta_1; & g &: (\alpha_1, \alpha_0, \alpha_1) \mapsto \beta_0;\\
g &: (\alpha_1, \alpha_1, \alpha_0) \mapsto \beta_3; & g &: (\alpha_1, \alpha_1, \alpha_1) \mapsto \beta_2.
\end{aligned} \tag{13}$$

Define $\mu : \{\alpha_0, \alpha_1\} \to \mathbb{Z}_4$ and $\nu : \{\beta_0, \beta_1, \beta_2, \beta_3\} \to \mathbb{Z}_4$ by

$$\begin{aligned}
\mu &: \alpha_j \mapsto j, \quad \forall\ j \in \{0, 1\}, \text{ and}\\
\nu &: \beta_j \mapsto j, \quad \forall\ j \in \{0, 1, 2, 3\},
\end{aligned} \tag{14}$$

respectively. Obviously, g is *equivalent* ([9, Definition VI.3]) to $x + 2y + 3z \in \mathbb{Z}_4[3]$ (Fig 2) via $\mu_1 = \mu_2 = \mu_3 = \mu$ and ν. However, there exists no $\hat{g} \in \mathbb{F}_4[3]$ of format (9) so that g is equivalent to any restriction of $\hat{g}$ by Proposition V.4. Although, by [7, Lemma A.2], there always exists a bigger field $\mathbb{F}_q$ such that g admits a presentation for some $\hat{g} \in \mathbb{F}_q[3]$ of format (9), the size q must be strictly bigger than 4. For instance, let $\hat{h}(x) = \sum_{a \in \mathbb{Z}_5} a\left[1 - (x-a)^4\right] - \left[1 - (x-4)^4\right] \in \mathbb{Z}_5[1]$. Then, g has presentation $\hat{h}(x + 2y + 4z) \in \mathbb{Z}_5[3]$ (Fig 3) via $\mu_1 = \mu_2 = \mu_3 = \mu : \{\alpha_0, \alpha_1\} \to \mathbb{Z}_5$ and $\nu : \{\beta_0, \beta_1, \beta_2, \beta_3\} \to \mathbb{Z}_5$ defined (symbolic-wise) by (14).

Proposition V.4 ([10]). *There exists no polynomial function $\hat{g} \in \mathbb{F}_4[3]$ of format* (9)*, such that a restriction of $\hat{g}$ is equivalent to the function g defined by* (13)*.*

As a consequence of Proposition V.4, in order to use linear encoder over field to compute function g, the alphabet sizes of the three encoders need to be at least 5. However, ring version offers a solution in which the alphabet sizes are 4, strictly smaller than using its field counterpart. Most importantly, the region achieved with linear encoders over a finite field $\mathbb{F}_q$, is always a subset of the one achieved with linear encoders over $\mathbb{Z}_4$. This is proved in the following proposition.

Proposition V.5. *Let g be the function defined by* (13)*, $\{\alpha_0, \alpha_1\}^3$ be the sample space of $(X_1, X_2, X_3) \sim p$ and p_X be the distribution of $X = g(X_1, X_2, X_3)$. If*

$$\begin{cases}
0 \leq \max\{p_X(\beta_1), p_X(\beta_3)\} \nless \min\{p_X(\beta_0), p_X(\beta_2)\} \leq 1\\
0 \leq \max\{p_X(\beta_0), p_X(\beta_2)\} \nless \min\{p_X(\beta_1), p_X(\beta_3)\} \leq 1
\end{cases}$$

then the region $\mathcal{R}_1$ achieved with linear encoders over $\mathbb{Z}_4$ contains the one, that is $\mathcal{R}_2$, obtained with linear encoders over any finite field $\mathbb{F}_q$ for computing g. Moreover, if p is strictly positive, then $\mathcal{R}_1 \supsetneq \mathcal{R}_2$.

Proof: Proof can be found in [9, Proposition VI.7]. ■

Regarding Proposition V.5, a more intuitive comparison can be identified from the presentations of g given in Fig 2 and Fig 3. According to Theorem V.1, linear encoders over field $\mathbb{Z}_5$ achieves the region

$$\mathcal{R}_{\mathbb{Z}_5} = \left\{ (R_1, R_2, R_3) \in \mathbb{R}^3 \middle|\, R_i > H(X_1 + 2X_2 + 4X_3) \right\}.$$

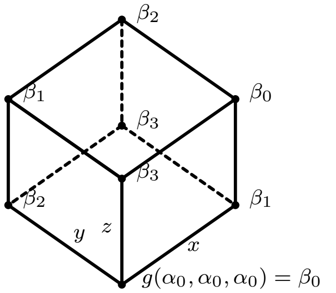

Fig 1: $g : \{\alpha_0, \alpha_1\}^3 \to \{\beta_0, \beta_1, \beta_2, \beta_3\}$

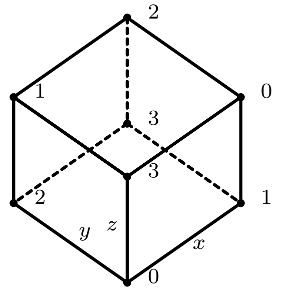

Fig 2: $x + 2y + 3z \in \mathbb{Z}_4[3]$

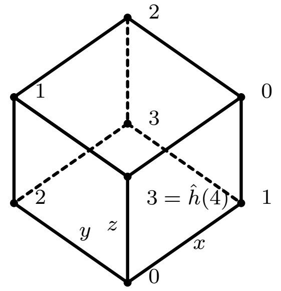

Fig 3: $\hat{h}(x + 2y + 4z) \in \mathbb{Z}_5[3]$

(X_1, X_2, X_3)	p
$(\alpha_0, \alpha_0, \alpha_0)$	$1/90$
$(\alpha_1, \alpha_0, \alpha_1)$	$1/90$
$(\alpha_1, \alpha_0, \alpha_0)$	$42/90$
$(\alpha_0, \alpha_1, \alpha_1)$	$42/90$
$(\alpha_0, \alpha_1, \alpha_0)$	$1/90$
$(\alpha_1, \alpha_1, \alpha_1)$	$1/90$
$(\alpha_0, \alpha_0, \alpha_1)$	$1/90$
$(\alpha_1, \alpha_1, \alpha_0)$	$1/90$

Table 1

The one achieved by linear encoders over ring $\mathbb{Z}_4$ is

$$\mathcal{R}_{\mathbb{Z}_4} = \left\{ (R_1, R_2, R_3) \in \mathbb{R}^3 \middle| R_i > H(X_1 + 2X_2 + 3X_3) \right\}.$$

Clearly, $H(X_1 + 2X_2 + 3X_3) \leq H(X_1 + 2X_2 + 4X_3)$, thus, $\mathcal{R}_{\mathbb{Z}_4} \supseteq \mathcal{R}_{\mathbb{Z}_5}$. Furthermore, $\mathcal{R}_{\mathbb{Z}_4}$ is strictly larger than $\mathcal{R}_{\mathbb{Z}_5}$ as long as

$$0 < \Pr\{\alpha_0, \alpha_0, \alpha_1\}, \Pr\{\alpha_1, \alpha_1, \alpha_0\} < 1,$$

(which implies $H(X_1 + 2X_2 + 3X_3) < H(X_1 + 2X_2 + 4X_3)$). To be specific, assume that $(X_1, X_2, X_3) \sim p$ satisfies Table 1. Then

$$\begin{aligned} \mathcal{R}_{\mathbb{Z}_5} &= \left\{ (R_1, R_2, R_3) \in \mathbb{R}^3 \middle| R_i > 0.4812 \right\} \\ \subsetneq \mathcal{R}_{\mathbb{Z}_4} &= \left\{ (R_1, R_2, R_3) \in \mathbb{R}^3 \middle| R_i > 0.4590 \right\}. \end{aligned}$$

Based on Proposition V.4 and Proposition V.5, we conclude that linear encoder over non-field ring dominates its field counterpart, in terms of achieving better coding rates with smaller alphabet sizes used in the encoders for computing g.

Remark 7. As mentioned in Remark 5, it is possible to obtain larger achievable region in computing g in Example V.3 by applying the linear encoder over ring to the "polynomial approach" introduced in [8]. In this sense, one can still prove that Proposition V.5 holds true. Interested reader can verify this with Theorem V.2.

Remark 8. In the sense of Theorem V.1 or Theorem V.2, there are infinitely many discrete functions for which using linear encoder over field always leads to suboptimal achievable region compared to linear encoder over some non-field ring. Examples include $\sum_{i=1}^{s} x_i \in \mathbb{Z}_{2p}[s]$ for any prime $p > 2$. One can always find an explicit example in which linear encoder over $\mathbb{Z}_{2p}$ dominates. We omit the details because of space limitation.

Remark 9. It is not correct to draw the conclusion that *the linear coding technique considered in this paper, [9] and [11] is included as a subclass of the group coding technique introduced in [13] since "a ring is a group"*. The difference can be seen via the example presented in [13, Section VIII.A]. [13, row 2 of TABLE III] says that group code over group $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ can leads to strictly worse rate compared to group code over group $\mathbb{Z}_4$. On the contrary, we claim that linear encoder over ring $\mathbb{Z}_4 \times \mathbb{Z}_4$ is always at least as good as the one over ring $\mathbb{Z}_4$ by Theorem IV.2. The essential reason for this is that *a ring is not a group*. An algebraic structure needs to be considered with the associated operations. This is why one can define at least 3 non-isomorphic rings on the group $\mathbb{Z}_q \oplus \mathbb{Z}_q$. A ring with two operations is not a group which associates with only one operation. After all, consider coding over the set $\mathbb{Z}_4 \times \mathbb{Z}_4$ for the mentioned example, [13, row 2 of TABLE III]. Our ring approach gives sum rate 3 (the less better rate achieved by Theorem V.1, not even the better one from Theorem V.2). This is strictly better than the group approach which achieves sum rate 3.5.

VI. Conclusion

For any data compression problem of Slepian–Wolf, we have proved that there always exist linear encoders over non-field rings which achieve the Slepian–Wolf region. 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.

Additionally, we have also demonstrated that linear encoder over non-field ring strictly outperforms its field counterpart in (infinitely) many circumstances regarding the computing problem, Problem 1.

References

[1] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Transactions on Information Theory*, vol. 19, pp. 471–480, July 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, pp. 585–592, July 1982.

[4] J. Körner and K. Marton, "How to encode the modulo-two sum of binary sources," *IEEE Transactions on Information Theory*, vol. 25, 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, pp. 396–411, May 1983.

[6] M. Sefidgaran and A. Tchamkerten, "Computing a function of correlated sources: A rate region," in *IEEE International Symposium on Information Theory*, pp. 1856–1860, Aug. 2011.

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

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

[9] S. Huang and M. Skoglund, "On linear coding over finite rings and applications to computing," *IEEE Transactions on Information Theory*, Submitted. Available: http://www.ee.kth.se/~sheng11

[10] S. Huang and M. Skoglund, "Linear source coding over rings and applications," in *IEEE Swedish Communication Technologies Workshop*, pp. 1–6, Oct. 2012.

[11] S. Huang and M. Skoglund, "On achievability of linear source coding over finite rings," in *IEEE International Symposium on Information Theory*, July 2013.

[12] S. Huang and M. Skoglund, *On Existence of Optimal Linear Encoders over Non-field Rings for Data Compression*. KTH Royal Institute of Technology. Available: http://www.ee.kth.se/~sheng11

[13] D. Krithivasan and S. Pradhan, "Distributed source coding using abelian group codes: A new achievable rate-distortion region," *IEEE Transactions on Information Theory*, vol. 57, no. 3, pp. 1495–1519, 2011.