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

Sheng Huang and Mikael Skoglund

Communication Theory
Electrical Engineering
KTH Royal Institute of Technology
Stockholm, Sweden

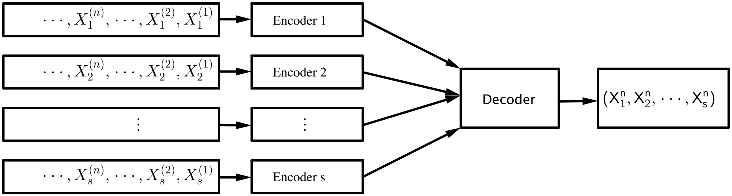
September 12, 2013
Seville, Spain

Outline

1. Introduction
   - Linear Source Coding over Finite Fields / Rings
   - Achievability Theorem
2. Optimality: Data Compression
   - Exist Optimal Linear Encoders over Non-field Rings
   - Other Rings
3. Application: Source Coding for Computing
   - Source Coding for Computing
   - LCoF is not optimal in the Sense of [Körner and Marton(1979)]
4. Conclusion
   - Non-field Ring vs Field
5. Thanks / References
   - Thanks
   - Bibliography

Linear Source Coding over Finite Fields / Rings (I)

Consider the Slepian–Wolf Source Network:



1. [Elias(1955), Csiszár(1982)] propose to use linear mappings (over finite fields) as encoders for Slepian–Wolf data compression;
2. Linear coding over finite fields (LCoF) is optimal, i.e. achieves the Slepian–Wolf region [Slepian and Wolf(1973)].

Linear Source Coding over Finite Fields / Rings (II)

How about linear coding over finite rings (LCoR)?

Definition 1

The tuple $[\mathfrak{R}, +, \cdot]$ is called a *ring* if the following criteria are met:

1. $[\mathfrak{R}, +]$ is an *Abelian group*;
2. There exists a *multiplicative identity* $1 \in \mathfrak{R}$, namely, $1 \cdot a = a \cdot 1 = a$, $\forall\, a \in \mathfrak{R}$;
3. $\forall\, a, b, c \in \mathfrak{R}$, $a \cdot b \in \mathfrak{R}$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
4. $\forall\, a, b, c \in \mathfrak{R}$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

Examples: real (complex) numbers $\mathbb{R}$ ($\mathbb{C}$), integers, $\mathbb{Z}_q$ (q is any positive integer), polynomials, matrices and etc. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ (p is a prime), invertible matrices are fields.

Linear Source Coding over Finite Fields / Rings (II)

How about linear coding over finite rings (LCoR)?

Definition 1

The tuple $[\mathfrak{R}, +, \cdot]$ is called a *ring* if the following criteria are met:

1. $[\mathfrak{R}, +]$ is an *Abelian group*;
2. There exists a *multiplicative identity* $1 \in \mathfrak{R}$, namely, $1 \cdot a = a \cdot 1 = a$, $\forall\, a \in \mathfrak{R}$;
3. $\forall\, a, b, c \in \mathfrak{R}$, $a \cdot b \in \mathfrak{R}$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
4. $\forall\, a, b, c \in \mathfrak{R}$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

Examples: real (complex) numbers $\mathbb{R}$ ($\mathbb{C}$), integers, $\mathbb{Z}_q$ (q is any positive integer), polynomials, matrices and etc. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ (p is a prime), invertible matrices are fields.

- † Will LCoR be optimal as LCoF for Slepian–Wolf coding?
- † What is the benefit?

Achievability Theorem (I)

Definition 2

A subset $\mathfrak{I}$ of a ring $[\mathfrak{R}, +, \cdot]$ is said to be a *left ideal* of $\mathfrak{R}$, denoted by $\mathfrak{I} \leq_l \mathfrak{R}$, if and only if

1. $[\mathfrak{I}, +]$ is a subgroup of $[\mathfrak{R}, +]$;
2. $\forall\, x \in \mathfrak{I}$ and $\forall\, a \in \mathfrak{R}$, $a \cdot x \in \mathfrak{I}$.

$\{0\}$ is a *trivial* left ideal, usually denoted by 0.

Examples: all even numbers of integers, $\{0, 2\}$ of $\mathbb{Z}_4$, the ring itself.

Achievability Theorem (I)

Definition 2

A subset $\mathfrak{I}$ of a ring $[\mathfrak{R}, +, \cdot]$ is said to be a *left ideal* of $\mathfrak{R}$, denoted by $\mathfrak{I} \leq_l \mathfrak{R}$, if and only if

1. $[\mathfrak{I}, +]$ is a subgroup of $[\mathfrak{R}, +]$;
2. $\forall\, x \in \mathfrak{I}$ and $\forall\, a \in \mathfrak{R}$, $a \cdot x \in \mathfrak{I}$.

$\{0\}$ is a *trivial* left ideal, usually denoted by 0.

Examples: all even numbers of integers, $\{0, 2\}$ of $\mathbb{Z}_4$, the ring itself.

Definition 3

Given a finite ring $\mathfrak{R}$ and one of its left ideal $\mathfrak{I}$, the *coset* $\mathfrak{R}/\mathfrak{I}$ is the set

$$\{r_1 + \mathfrak{I}, r_2 + \mathfrak{I}, \cdots, r_m + \mathfrak{I}\},$$

where $m = |\mathfrak{R}| \,/\, |\mathfrak{I}|$, $r_i \in \mathfrak{R}$ for all feasible i and $r_i + \mathfrak{I} \cap r_j + \mathfrak{I} = \emptyset \Leftrightarrow i \neq j$. $\mathfrak{R}/\mathfrak{I}$ forms a *left module* over $\mathfrak{R}$.

Achievability Theorem (II)

Assume that the sample space of X_i $(1 \leq i \leq s)$ is a finite set $\mathscr{X}_i$, and write

$$X_T = \prod_{i \in T} X_i, \; \mathfrak{R}_T = \prod_{i \in T} \mathfrak{R}_i$$

for $\emptyset \neq T \subseteq \{1, 2, \cdots, s\}$ and $\mathfrak{I}_T = \prod_{i \in T} \mathfrak{I}_i$ where $\mathfrak{I}_i \leq_l \mathfrak{R}_i$.

Let $\Phi = \{\Phi_1, \Phi_2, \cdots, \Phi_s\}$, where $\Phi_i : \mathscr{X}_i \rightarrow \mathfrak{R}_i$ is any injective mapping.

Achievability Theorem (II)

Assume that the sample space of X_i $(1 \leq i \leq s)$ is a finite set $\mathscr{X}_i$, and write

$$X_T = \prod_{i \in T} X_i, \; \mathfrak{R}_T = \prod_{i \in T} \mathfrak{R}_i$$

for $\emptyset \neq T \subseteq \{1, 2, \cdots, s\}$ and $\mathfrak{I}_T = \prod_{i \in T} \mathfrak{I}_i$ where $\mathfrak{I}_i \leq_l \mathfrak{R}_i$.

Let $\Phi = \{\Phi_1, \Phi_2, \cdots, \Phi_s\}$, where $\Phi_i : \mathscr{X}_i \to \mathfrak{R}_i$ is any injective mapping.

Theorem 4 ([Huang and Skoglund(2013a)])

The region $\mathcal{R}_\Phi$ containting coding rate $(R_1, R_2, \cdots, R_s) \in \mathbb{R}^s$ that satisfies

$$\sum_{i \in T} \frac{R_i \log |\mathfrak{I}_i|}{\log |\mathfrak{R}_i|} > H(X_T | X_{T^c}) - H(Y_{\mathfrak{R}_T / \mathfrak{I}_T} | X_{T^c}), \tag{1}$$

$$\forall \, \emptyset \neq T \subseteq \{1, 2, \cdots, s\} \text{ and for all } 0 \neq \mathfrak{I}_i \leq_l \mathfrak{R}_i,$$

where $Y_{\mathfrak{R}_T / \mathfrak{I}_T} = \prod_{i \in T} \Phi_i(X_i) + \mathfrak{I}_T$ *(which has sample space $\mathfrak{R}_T / \mathfrak{I}_T$), is achievable with linear coding over* $\mathfrak{R}_1, \mathfrak{R}_2, \cdots, \mathfrak{R}_s$.

Exist Optimal Linear Encoders over Non-field Rings (I)

Theorem 5 ([Huang and Skoglund(2013b)])

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 the convex hull of $\bigcup_{\Phi} \mathcal{R}_{\Phi}$ coincides with the Slepian–Wolf region.

Examples: All finite fields, $\mathbb{Z}_{p^2}$ (p is a prime) and

$$\mathbb{M}_{L,p} = \left\{ \begin{bmatrix} a & 0 \\ b & a \end{bmatrix} a, b \in \mathbb{Z}_p \right\}.$$

Exist Optimal Linear Encoders over Non-field Rings (II)

Proof of Theorem 5 (for Single Source): There is nothing to prove if $\mathfrak{R}_1$ is a field. Assume that $\mathfrak{R}_1$ is a non-field ring. Then $\bigcup_{\Phi} \mathcal{R}_\Phi$ is the Slepian–Wolf region if and only if there exists $\tilde{\Phi}_1 : \mathscr{X}_1 \to \mathfrak{R}_1$ such that

$$\frac{\log |\mathfrak{R}_1|}{\log |\mathfrak{I}_{01}|}[H(X_1) - H(\tilde{\Phi}_1 + \mathfrak{I}_{01})] \leq H(X_1) \tag{2}$$

$$\Leftrightarrow H(X_1) \leq 2H(\tilde{\Phi}_1 + \mathfrak{I}_{01}) \qquad \left(\text{since } \sqrt{|\mathfrak{R}_1|} = |\mathfrak{I}_{01}|\right). \tag{3}$$

The existence of such a injection $\tilde{\Phi}_1$ is guaranteed by Lemma 6. ■

Exist Optimal Linear Encoders over Non-field Rings (III)

Lemma 6 ([Huang and Skoglund(2012)])

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

$$H(X|Y) \leq 2H(\tilde{\Phi}(X) + \mathfrak{I}|Y). \quad (4)$$

Exist Optimal Linear Encoders over Non-field Rings (III)

Lemma 6 ([Huang and Skoglund(2012)])

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

$$H(X|Y) \leq 2H(\tilde{\Phi}(X) + \mathfrak{I}|Y). \tag{4}$$

Sketch of the Proof: Let $\tilde{\Phi} = \arg\max_{\Phi} H(\Phi(X) + \mathfrak{I}|Y)$. By the grouping rule for entropy, there exists $\overline{\Phi} : \mathscr{X} \to \mathfrak{R}$ such that

$$H(X|Y) - H(\tilde{\Phi}(X) + \mathfrak{I}|Y) = H(\overline{\Phi}(X) + \mathfrak{I}|Y).$$

Since

$$H(\tilde{\Phi}(X) + \mathfrak{I}|Y) \geq H(\overline{\Phi}(X) + \mathfrak{I}|Y)$$

by definition, the statement follows. ■

Other Rings

Example 7

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

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

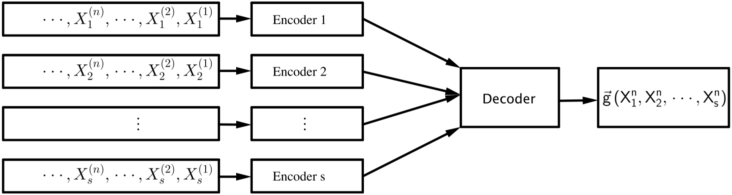
By Theorem 4,

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

is achievable with linear coding over ring $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$. Obviously, $\mathcal{R}$ is just the Slepian–Wolf region. Optimality is claimed.

Source Coding for Computing

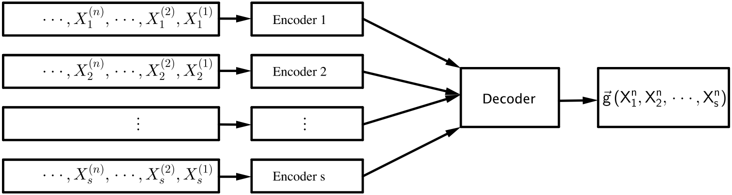
Source Coding for Computing g (a discrete function):



First considered by [Körner and Marton(1979), Ahlswede and Han(1983)] for g being the modulo-two sum/binary sum.

Source Coding for Computing

Source Coding for Computing g (a discrete function):



First considered by [Körner and Marton(1979), Ahlswede and Han(1983)] for g being the modulo-two sum/binary sum.

One trick: Let $Z^{(n)} = g\left(X_1^{(n)}, X_2^{(n)}, \cdots, X_s^{(n)}\right)$ and ϕ be a linear encoder (over some field / ring) such that

$$\begin{aligned}\epsilon &> \Pr\{\psi(\phi(Z^n)) \neq Z^n\} \\ &\overset{(a)}{=} \Pr\{\psi(\vec{g}(\phi(X_1^n), \phi(X_2^n), \cdots, \phi(X_s^n))) \neq Z^n\},\end{aligned}$$

where (a) holds when g is a linear function over some field / ring.

LCoF is not optimal in the Sense of [Körner and Marton(1979)] (I)

Consider linear function over $\mathbb{Z}_4$

$$g(x, y, z) = x + 2y + 3z \text{ defined on the domain } \{0, 1\}^3 \subsetneq \mathbb{Z}_4^3.$$

g can also be presented as polynomial function

$$\hat{h}(x + 2y + 4z) \text{ defined on domain } \{0, 1\} \subsetneq \mathbb{Z}_5^3,$$

where

$$\hat{h}(x) = \sum_{a \in \mathbb{Z}_5} a \left[1 - (x - a)^4\right] - \left[1 - (x - 4)^4\right]$$

is not injective. Linear coding (LC) techniques (over non-field ring $\mathbb{Z}_4$ or field $\mathbb{Z}_5$) are used for encoding g.
However, the achievable region $\mathcal{R}_{\mathbb{Z}_4}$ achieved linear LC over $\mathbb{Z}_4$ always dominates the one $\mathcal{R}_{\mathbb{Z}_5}$ achieved by LC over $\mathbb{Z}_5$. In fact, $\mathcal{R}_{\mathbb{Z}_4}$ dominates the region achieved by LC over each and every finite field for encoding g.

LCoF is not optimal in the Sense of [Körner and Marton(1979)] (II)

Definition 8

The *characteristic* of a finite ring $\mathfrak{R}$ is defined to be the smallest positive integer m, such that $\sum_{j=1}^{m} 1 = 0$, where 0 and 1 are the zero and the multiplicative identity of $\mathfrak{R}$, respectively.

LCoF is not optimal in the Sense of [Körner and Marton(1979)] (II)

Definition 8

The *characteristic* of a finite ring $\mathfrak{R}$ is defined to be the smallest positive integer m, such that $\sum_{j=1}^{m} 1 = 0$, where 0 and 1 are the zero and the multiplicative identity of $\mathfrak{R}$, respectively.

The essential reason for the "domination" to happen is due to the fact that:

1. the characteristic of a finite field much be a prime (by the theory of splitting field);
2. the characteristic of a finite ring can be any integer ≥ 2.

LCoF is not optimal in the Sense of [Körner and Marton(1979)] (II)

Definition 8

The *characteristic* of a finite ring $\mathfrak{R}$ is defined to be the smallest positive integer m, such that $\sum_{j=1}^{m} 1 = 0$, where 0 and 1 are the zero and the multiplicative identity of $\mathfrak{R}$, respectively.

The essential reason for the "domination" to happen is due to the fact that:

1. the characteristic of a finite field much be a prime (by the theory of splitting field);
2. the characteristic of a finite ring can be any integer ≥ 2.

Basic on this fact, one can construct infinitely many functions, say g, such that LC over a finite field is always suboptimal (in the sense of [Körner and Marton(1979)]) for encoding g.

Non-field Ring vs Field

	field	non-field ring	properties
Slepian–Wolf coding (side information)	$\surd$	exist optimal encoders for all scenarios	inverse & typicality lemma
Slepian–Wolf coding (memory[1])	$\surd$	not yet proved, optimal shown by examples	inverse & typicality lemma
Implementation Complexity		$\surd$	polynomial long division algorithm
Alphabet sizes of encoders		$\surd$	prime subfield
Coding for Computing		$\surd$	characteristic & zero divisor
Coding for Computing (memory)		$\surd$	characteristic & zero divisor

[1] Please kindly refer to [Huang and Skoglund(2013c)] for details.

Thanks

♫ ♬

Thanks!

Bibliography I

- 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.
- P. Elias, "Coding for noisy channels," *IRE Conv. Rec.*, pp. 37–46, Mar. 1955.
- 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.
- 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.
- S. Huang and M. Skoglund, "On achievability of linear source coding over finite rings," in *IEEE International Symposium on Information Theory*, July 2013.

Bibliography II

- ——, "On existence of optimal linear encoders over non-field rings for data compression with application to computing," in *IEEE Information Theory Workshop*, September 2013.
- ——, *On Existence of Optimal Linear Encoders over Non-field Rings for Data Compression*, KTH Royal Institute of Technology, December 2012. [Online]. Available: http://www.ee.kth.se/~sheng11
- 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.
- S. Huang and M. Skoglund, *Coding for Computing Irreducible Markovian Functions of Sources with Memory*, KTH Royal Institute of Technology, May 2013. [Online]. Available: http://www.ee.kth.se/~sheng11