An Achievable Low Complexity Encoding Scheme for Coloring Cyclic Graphs

Mohammad Reza Deylam Salehi, Derya Malak
Communication Systems Department, EURECOM, Sophia Antipolis, France
{deylam, malak}@eurecom.fr

***Abstract*—In this paper, we utilize graph coloring for functions captured by cycle graphs to achieve lossless function compression. For functional compression of characteristic graphs or cycles and their OR graphs, we present a feasible scheme for coloring the odd cycles and their OR power graphs. In addition, we calculate the chromatic number for coloring the n-th power of even cycles, which paves the way for calculating the minimum entropy coloring. Moreover, we determine the number of distinct eigenvalues in each OR power and the largest eigenvalue for each power, which allows us to derive a bound on the chromatic number of each OR power of a cycle. Our method provides a proxy for understanding the fundamental limits of compressing cyclic graphs, which has broad applications in various practical use cases of cryptography and computer algebra.**

***Index Terms*—Function compression, characteristic graph, graph coloring, graph entropy, eigenvalues, chromatic number.**

I. Introduction

The concept of data compression in information theory describes the process of encoding and decoding a source using fewer bits than its original size of the source, which is given by Shannon's entropy [1]. When the sources are distributed and the goal is to recover them jointly at a user, the Slepian-Wolf theorem gives the fundamental limits of compression [2]. In the case of recovering or computing a deterministic function of distributed sources but not sources themselves, we can provide a further reduction in compression via accounting for the structure of the function [3]. This is known as functional compression, where the function is an abstraction of a task.

A. Motivation and Literature Review

Let us begin with an example. Consider a student database with information including the rental records, and health, etc., of individuals. The Ministry of Science wants to offer housing aid to a particular group of students, by only requiring information on the rental contracts, and the payslips of the students, and without disclosing their personal data, due to privacy and redundancy constraints. This scenario is an example of functional compression, which aims to avoid compressing and transmitting large volumes of data, and is instead tailored to the specifics (i.e., the structure, distribution, sensing, or whatever) of the function.

This work is partially supported from a Huawei France-funded Chair towards Future Wireless Networks. Co-funded by the European Union (ERC, SENSIBILITÉ, 101077361). Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Council. Neither the European Union nor the granting authority can be held responsible for them.

In Shannon's breakthrough work in [1], the function to be recovered at the user is the identity function of the source, i.e., the source itself. In [2], the authors have generalized the noiseless coding of a discrete information source, given in [1], to distributed compression and joint decoding of two jointly distributed and finite alphabet sources. Slepian-Wolf theorem gives a theoretical bound for the lossless coding rate of distributed coding of such sources [2]. As shown in their work, these two data sequences $\{X_i\}_{i=1}^{\infty}$, and $\{Y_i\}_{i=1}^{\infty}$ are obtained by repeated independent drawings from a discrete bivariate distribution. The encoder of each source is constrained to operate without the knowledge of the other source, while the joint distribution is available to the decoder. Practical schemes for Slepian-Wolf compression have been proposed in [4]–[6].

Different from distributed source compression, in functional compression, the goal is to separately compress the distributed sources such that a deterministic function $f(X, Y)$ of these sources can be calculated by a receiver. Prior attempts on functional compression can be categorized into works focusing on lossless compression of functions, [1]–[3], [7]–[19], and those for which the compression schemes tolerate distortion for lossy reconstruction of functions [20]–[25]. In [10], Orlitsky and Roche have provided a single letter characterization for general functions of two variables. The authors have used characteristic graphs, where each graph represents the outcomes of one source and the pairwise relationships between each source's outcomes while maintaining the function structure [10].

Applications of distributed compression problem include the two special cases studied by Ahlswede and Körner, i.e., when $f(X_1, X_2) = X_1$, and $f(X_1, X_2) = (X_1 + X_2) \mod 2$ [15]. Körner and Marton, in [14], have derived the rate region for distributed encoding of two binary sources to compute their modulo-two sum at the receiver. In [22], Yamamato has considered a source coding problem for Wyner-Ziv systems, in which the receiver estimates the value of $f(X, Y)$ of the input X given side information Y. In [17], Han and Kobayashi have established an achievable functional reconstruction scheme, which depends on the structure of $f(X_1, X_2)$, but free of the joint distribution of (X_1, X_2). Optimal coding schemes and achievable rate regions for lossless and lossy computation of $f(X, Y)$ with side information Y, and distributed compression of $f(X, Y)$ have been derived in [9].

B. Overview and Contributions

In this paper, we propose a coding scheme for distributed functional compression problems; where the source characteristic graphs can be represented as cycles, i.e., each source outcome must be distinguished from the two neighboring (or adjacent) outcomes of the same source. We focus on asymptotically lossless compression and decoding of functions with such cyclic characteristic graphs.

Cycle graphs (or cyclic graphs) show up in many practical scenarios, such as periodic functions, and mod functions, which are widely used in cryptography, computer algebra, and science. More specifically, in cryptography, Caesar Ciphers, Rivest-Shamir-Adleman (RSA) algorithm [26], Diffie-Hellman [27], as well as Advanced Encryption Standard (AES) [28], International Data Encryption Algorithm (IDEA), are several practical examples [29]. The calculation of checksums within serial numbers is another application of interest [30]. For example, ISBNs (International Standard Book Numbers) use mod 11 arithmetic for 10-digit ISBNs or mod 10 for 13-digit ISBNs to detect errors. In addition, International Bank Account Numbers (IBANs) use mod 97 arithmetic to identify mistakes in bank account numbers entered by users.

Why cyclic graphs? There are several key advantages to having cycles as characteristic graphs and their coloring. When we color cyclic structures, we can reuse coloring much more efficiently than when coloring any other connected graph with a higher average degree, as we will discuss later in Sect. III-C. In particular, to model a length n source sequence, we use the n-th OR power[1] of the characteristic graph [10] and its valid coloring to compress the source information for computing the desired function in a lossless manner as the blocklength n tends to infinity. The minimum entropy valid coloring gives a lower bound to the compression length required in bits for the lossless reconstruction of the desired function. Due to the features that cycles and their powers can capture, in this paper, we aim to find valid coloring for both even and odd cycles.

The main contributions of this paper can be listed as follows:

- We characterize the exact degree of a vertex of n-th OR power for both odd and even cycles.
- We derive the exact chromatic number, denoted by $\chi_{C_{2l}}$, for even cycles C_{2l} and their OR powers, for $l \in \mathbb{Z}^+$.
- We devise an achievable coloring scheme for odd cycles C_{2l+1} for $l \in \mathbb{Z}^+$.
- We compute the largest eigenvalue, $\lambda_1(C_i^n)$, of the adjacency matrix A_f^n for the n-th OR power of cycle graphs.
- We compute a valid coloring of a characteristic graph, which is in the form of a cycle, in polynomial time[2], exploiting the structure of the graph and its OR powers.
- We derive lower and upper bounds on the chromatic numbers of OR powers of cycle graphs, $\chi_{C_i^j}$, based on the relationship between the adjacency matrices of cycle graphs and the eigenvalues of these matrices.

[1] In this paper, we exclusively focus on the OR graph powers for realizing lossless compression of multi-letter source realizations [31].

[2] Note that the problem of finding a minimum entropy coloring in general graphs (beyond cyclic graphs) is in general NP-hard [32].

C. Organization

The rest of this article is organized as follows. The second section, II, consists of a review of some technical literature on graphs, cycles, and their valid coloring. Main results section, III, contains theorems, and coloring schemes, drawing on the bounds of the degrees, eigenvalues, and the chromatic numbers of cycle graphs. In Sect. IV, we summarize our key results and outline avenues for exploration.

D. Notation

Capital letter X denotes a discrete random variable with distribution $p(x)$ over the finite alphabet $\mathcal{X}$, whereas x is a realization of X, and $\{X_j\}_{j=1}^{\infty}$ is an i.i.d. sequence where each element is distributed according to $p(x)$. The joint distribution of the source variables X_1 and X_2 is denoted by $p(x_1, x_2)$. For a length n i.i.d. vector realization of X_1, we use the boldface notation $\mathbf{x}_1^n = x_{11}, \dots, x_{1n}$ to represent the length n source realization. We also let $[n] = \{1, \dots, n\}$ for $n \in \mathbb{Z}^+$.

The distributed sources X_1 and X_2 build the characteristic graphs G_{X_1} and G_{X_2}, respectively, to compute function $f(X_1, X_2)$. We denote by χ_{G_X} the chromatic number of G_X, by C_i a cycle graph with i vertices, by C_i^n its n-th OR power, and by $\mathcal{C}_i^j(l)$ the set of distinct colors in sub-graph $l \in \mathcal{V}$ (detailed in Sect. III) of the j-th power of C_i.

We denote by J_V and I_V an all-one and identity matrices of size $V \times V$ each, by A_f the adjacency matrix of $C_i = G(\mathcal{V}, \mathcal{E})$, where $A_f = (a_{xx'})_{1 \le x,\, x' \le V}$ is a symmetric $(0,1)$-matrix with zeros on its diagonal, i.e., $a_{xx} = 0$, and $a_{xx'} = 1$ indicates that vertices x, $x' \in \mathcal{V}$ are adjacent, and $a_{xx'} = 0$ when there is no edge between them. We denote by $deg(x)$ the degree of $x \in \mathcal{V}$. The largest and the smallest eigenvalues of A_f are denoted by λ_1, and λ_V, respectively, and $\vartheta(C_i^j)$ is the set of distinct eigenvalues of the adjacency matrix of C_i^j, i.e., A_f^j.

II. Technical Preliminary

This section introduces the fundamental concepts related to graphs, such as degree, independent sets, and cycles [33]–[37]. Furthermore, it discusses some graph-theoretic concepts used in distributed functional compression, such as characteristic graphs, OR power graphs, and their coloring [37]–[39].

A. Regular Graphs, Characteristic Graphs, and OR Powers

Consider a graph $G(\mathcal{V}, \mathcal{E})$ on a set of vertices $\mathcal{V} = [V]$ and set of edges $\mathcal{E}$, with the number of vertices being $|\mathcal{V}| = V$.

Definition 1. *(Degree of a vertex [33].) The degree of a vertex $x \in \mathcal{V}$, represented by $deg(x)$, of $G(\mathcal{V}, \mathcal{E})$ is the number of edges it is connected to, i.e., the number of its neighbors.*

The number of edges in G is determined as

$$|\mathcal{E}| = (\sum_{l \in [V]} deg(x_l))/2 \ . \tag{1}$$

Along with the notion of the degree of a vertex, we next introduce the concept of an independent set, which is critical for determining the valid coloring of a characteristic graph that we discuss later in Sect. II-B.

Definition 2. *(Independent set, and maximal independent set [34].) An independent set, $I(G)$, in $G(\mathcal{V}, \mathcal{E})$ is a subset of vertices of $\mathcal{V}$, such that no two are adjacent. A maximal independent set, $MIS(G)$, is an independent set that is not a subset of any other independent set $I(G)$ of $G(\mathcal{V}, \mathcal{E})$.*

In the distributed functional compression setting we focus on here, the function outputs at the receiver can be captured through source characteristic graphs. To that end, we next define characteristic graphs to help distinguish between function outcomes toward providing compression savings.

Definition 3. *(Characteristic graph, G_X [36].) Source X_1 builds a characteristic graph or confusion graph $G_{X_1} = G(\mathcal{V}, \mathcal{E})$ to distinguish the outcomes of a function $f(X_1,\, X_2)$ of the distributed sources X_1 and X_2 with a joint distribution $p(x_1, x_2)$. This graph is constructed using source outcomes, where $\mathcal{V} = \mathcal{X}_1$, and for $x_1^1, x_1^2 \in \mathcal{V}$ that are distinct vertices, $\exists$ an edge $(x_1^1, x_1^2) \in \mathcal{E}$ if and only if there exists a $x_2^1 \in \mathcal{X}_2$ such that $p(x_1^1, x_2^1) \cdot p(x_1^2, x_2^1) > 0$ and $f(x_1^1, x_2^1) \neq f(x_1^2, x_2^1)$, i.e., these two vertices of G_{X_1} should be distinguished.*

The type of characteristic graphs we use in the current paper falls into the category of cyclic graphs. We note that a characteristic graph can be either cyclic or non-cyclic based on the function which it represents. As our next step, we will define k-regular graphs that contain cycles.

Definition 4. *(k-regular graph, and cycles [35], [37].) In a regular graph $G(\mathcal{V}, \mathcal{E})$, each vertex $x \in \mathcal{V}$ has the same number of neighbors. The term k-regular graph refers to a regular graph with a degree of $k = deg(x)$ for all $x \in \mathcal{V}$.*

Cyclic graphs are members of k-regular graphs. More specifically, cyclic graphs are 2-regular graphs and their adjacency matrices are symmetric $(0, 1)$ matrices.

To present the concept of characteristic graphs clearly, the following example is provided.

Example 1. *Consider the problem of distributed functional compression of $f(X_1, X_2) = (X_1 + X_2) \mod 2$ with two sources X_1 and X_2 and one receiver. Source one X_1 is uniform over the alphabet $\mathcal{X}_1 = \{0, 1, 2, 3, 4, 5\}$, and X_2 is uniform over $\mathcal{X}_2 = \{0, 1\}$. Because for even X_1, the function output is $f(X_1, X_2) = X_2$, and for the odd values of X_1, we have $f(X_1, X_2) = X_2 + 1$. At source X_1 even outcomes do not need to be distinguished from each other and are assigned the color G, while odd outcomes of X_1 are assigned the color Y, and similarly for X_2. We illustrate the coloring of G_{X_1} and G_{X_2} in Fig. 1. For decoding f, it is necessary and sufficient [12], if the receiver has the color pairs (Y, G) or (G, Y), to determine the function outcome, which is 1, whereas, for the pairs (Y, Y) and (G, G), to infer that the outcome is 0.*

To determine the number of bits needed for multiple source instances, and realize the fundamental limits of functional compression of a source sequence [3], we exploit the notion of *OR powers* of graphs, as introduced next.

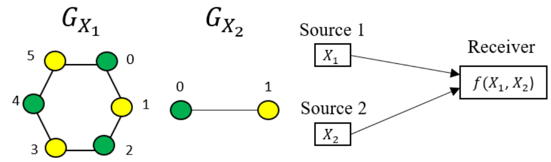

Fig. 1. The problem of a distributed functional compression with two sources, with the characteristic graph for X_1, i.e., G_{X_1}, being cyclic, and a receiver.

Definition 5. *(n-th OR power graph, $G_{\mathbf{X}}^n$ [37]–[39].) For $n > 1$, the n-th OR power of $G_X = G(\mathcal{V}, \mathcal{E})$ is represented as $G_{\mathbf{X}}^n = (\mathcal{V}^n, \mathcal{E}^n)$ where $\mathcal{V}^n = \mathcal{X}^n$, and for distinct vertices $\mathbf{x}_1^n = x_{11}^1, \ldots, x_{1n}^1 \in \mathcal{V}^n$, and $\mathbf{x}_2^n = x_{21}^1, \ldots, x_{2n}^1 \in \mathcal{V}^n$ it holds that $(\mathbf{x}_1^n, \mathbf{x}_2^n) \in \mathcal{E}^n$, when $\exists$ at least one $l \in [n]$ such that $(x_{1l}^1, x_{1l}^2) \in \mathcal{E}$, where recall that this condition is determined by the rule in Defn. 3 for building G_X.*

The total number of vertices in $\mathcal{V}^n$ is represented by V^n. The total number of edges in $G_{\mathbf{X}}^n$, i.e., $|\mathcal{E}^n|$, can be determined evaluating $deg(\mathbf{x}_l^n)$, $l \in [V^n]$ and using (1).

Definition 6. *(Sub-graphs of $G_{\mathbf{X}}^n$.) Given the n-th power graph $G_{\mathbf{X}}^n$, the set of V graphs $\{G_{\mathbf{X}}^{n-1}(l)\}_{l \in [V]}$ in $G_{\mathbf{X}}^n$, each corresponding to a replica of the $(n-1)$-th power of $G_{\mathbf{X}}$, is denoted as the sub-graphs of $G_{\mathbf{X}}^n$.*

The use of OR powers in determining the rate regions in the asymptotic regime for distributed lossless compression of functions is explored in [12] and [13], where the authors have demonstrated that the lowest sum rate could be achieved by encoding the n-th OR power graphs built using $\mathbf{X}_1^n$ and $\mathbf{X}_2^n$, $p(\mathbf{x}_1^n, \mathbf{x}_2^n)$, and $f(x_1, x_2)$ in the limit as n goes to infinity.

Having defined these theoretical tools for our functional compression problem, we next focus on how to utilize them.

B. Coloring of Characteristic Graphs

In this paper, we envision a vertex coloring perspective for the encoding of characteristic graphs. A valid or proper coloring of G_{X_1} is such that each vertex of G_{X_1} is assigned a color, and adjacent vertices of G_{X_1} receive distinct colors. In other words, a valid coloring in our distributed compression setting determines which source realizations should be assigned different codes (colors). Nonadjacent vertices can be assigned the same or different colors. The minimum number of colors required to achieve a valid coloring of G_{X_1} is called the chromatic number, $\chi_{G_{X_1}}$. The problem of determining $\chi_{G_{X_1}}$ is connected to finding the maximal independent sets of G_{X_1}, and is in general NP-complete [32]. A sufficient condition for achieving a minimum entropy coloring is as follows. Provided that $p(x_1,\, x_2) > 0$, $\forall\ (x_1,\, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2$, the maximal independent sets of G_{X_1} and of its power $G_{\mathbf{X}_1}^n$, for $n > 1$, are some non-overlapping fully-connected sets [12]. Under this condition, the minimum entropy coloring of G_{X_1} can be achieved by assigning different colors to its different maximal independent sets (see e.g., Sect. III-A).

Next, in Sect. III, we detail our coloring approach devised specifically for cycle graphs.

III. Main Results

Let C_i be a cycle graph with i vertices that represents the characteristic graph source X_1 builds for computing f, where for an even cycle we have $i = 2l$, and for an odd cycle, we have $i = 2l + 1$, for some $l \in \mathbb{Z}^+$. We seek to achieve an asymptotically lossless functional compression of sources to recover the colors of C_i. To that end, we need to determine the optimal coloring for the n-th power of C_i, denoted by C_i^n.

We start this section by determining the degree of each vertex of the j-th power of C_i, i.e., C_i^j.

Theorem 1. *The degrees in the n-th OR power of a cycle graph, C_i^n for $n \geq 2$, are calculated as follows:*

$$deg(\mathbf{x}^n) = 2 + \sum_{j\in[n-1]} 2(V^j) \ , \quad \forall \mathbf{x}^n \in \mathcal{V}^n \ . \tag{2}$$

Proof. See Appendix A. □

From Theorem 1, when $G_X = C_i$ is a cycle, $G_{\mathbf{X}}^n = C_i^n$ is a k-regular graph, i.e., $deg(\mathbf{x}_l^n) = k$, for some even number $k \in \mathbb{Z}^+$, $\forall\ l \in [V^n]$, as given by (2). We will next calculate the chromatic number of $\chi_{C_i^n}$, $n \geq 1$, for $i = 2l$, $l \in \mathbb{Z}^+$.

A. Coloring Cyclic Graphs

In this part, we first discuss even cycles and their j-th powers, and determine their chromatic numbers (see Theorem 2). Then, we analyze odd cycles, for which we introduce a valid coloring scheme (see Prop. 1 and App. B).

1) Even Cycles: We first consider even cycles, which are denoted by C_{2l}, $l \in \mathbb{Z}^+$. Vertices are sequentially numbered in a clockwise direction, e.g., see G_{X_1} in Fig. 1, and alternately colored. Even vertices are represented by one color, while odd vertices are denoted with a different color.

Theorem 2. *The chromatic number of C_{2l}^n is given as*

$$\chi(C_{2l}^n) = 2^n \ , \quad l \in \mathbb{Z}^+ \ , \ n \geq 1 \ . \tag{3}$$

Proof. In order to cover all vertices in C_{2l}^n, $l \in \mathbb{Z}^+$, only two colors are required. Subsequently, for C_{2l}^2, the sub-graphs are $\{C_{2l}(1), C_{2l}(2), \dots, C_{2l}(2l)\}$. The reason for having $2l$ sub-graphs in C_{2l}^2 can be explained as follows. There are $(2l)^2$ vertices in C_{2l}^2 such that each sub-graph $C_{2l}(\cdot)$, i.e., a 1-st power graph, has $2l$ vertices. Due to the fact that each sub-graph is two colorable, and the vertices of adjacent sub-graphs are fully connected, the colors of the two sub-graphs should differ. For example, consider $\{C_{2l}(l_1 \mod (V)), C_{2l}(l_1 + 1 \mod (V))\}$. Consequently, each of these sub-graphs requires two different colors disjoint across $C_{2l}(l_1 \mod (V))$ and $C_{2l}(l_1{+}1 \mod (V))$, resulting in a total of 4 colors. However, due to the cyclic characteristic of power graphs, it is possible to alternate colors from $C_{2l}(l_1 \mod (V))$ to cover the vertices of $C_{2l}(l_1 + 2 \mod (V))$ for any $l_1 \in [2l]$, and so on, and similarly for the sub-graphs of C_{2l}^2 with even indices.

Using induction, we can calculate the number of colors needed to reach a valid coloring from $(n{-}1)$-th to n-th powers. Finally, we can calculate $\chi_{C_{2l}^n}$ by the relation in (3). □

We show a valid coloring for the $3-rd$ power graph C_4^3 of the even cycle C_4 in Fig. 2.

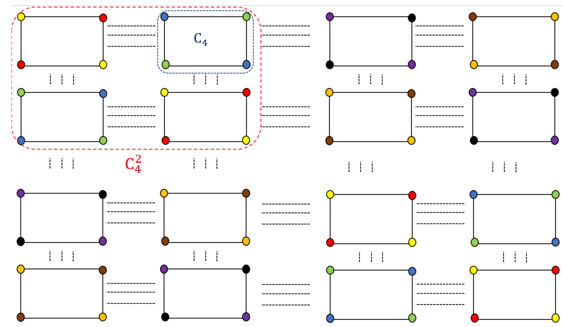

Fig. 2. A valid coloring of C_4^3 with 8 colors.

2) Odd Cycles: Our next consideration is odd cycles, namely C_{2l+1}, $l \in \mathbb{Z}^+$. In the special case with 3 vertices, i.e., for C_3, a valid coloring requires 3 distinct colors to successfully recover the coloring information of the vertices in decoding. In C_3^2, each sub-graph of a power graph, i.e., $C_3(1)$, $C_3(2)$, and $C_3(3)$, requires 3 different colors since C_3 is a complete graph. Similarly, using induction we can show that for a valid coloring of C_3^n the minimum number of required colors is given as $\chi_{C_3^n} = 3^n$, $n \geq 1$. In fact, because C_3 is complete, one cannot exploit color reuse.

Unlike C_3, for coloring C_5, which is not complete, one could reuse the colors. A valid coloring of C_5 has $\chi_{C_5} = 3$. We next present an achievable scheme for valid coloring of general odd cycles C_{2l+1} and their powers, namely, C_{2l+1}^n.

Proposition 1. (Chromatic number of odd cycles.) *The chromatic number can be recursively computed as follows:*

$$\chi_{C_i^{n+1}} = 2\chi_{C_i^n} + \left\lceil \frac{\chi_{C_i^n}}{2} \right\rceil \ , \ n \geq 1 \tag{4}$$

where $\chi_{C_i^n}$ is the chromatic number of C_i^n, i.e., the n-th OR power of an odd cycle, where $i = 2l+1$ for some $l \in \mathbb{Z}^+$.

Proof. See Appendix B. □

The value of $\chi_{C_{2l}^n}$ in Theorem 2 for even cycles is exact, but for odd cycles, it is not. However, we note from Prop. 1 that, $\chi_{C_i^n}$ for $n \geq 1$ can be determined from χ_{C_i}. It remains unclear whether, in general, we can lower and upper bound chromatic numbers χ_{G_X} of characteristic graphs. By exploiting the eigenvalues of the adjacency matrix, we will next bound χ_{G_X}.

B. Eigenvalues of An Adjacency Matrix of Cyclic Graphs

It is possible to bound χ_{C_i} for a cycle graph $C_i = G(\mathcal{V}, \mathcal{E})$ using the eigenvalues $\lambda_i(C_i)$ (where C_i has V eigenvalues) of its adjacency matrix A_f distinguishing the outcomes of a function f. We can calculate the largest eigenvalue $\lambda_{V^n}(C_i^n)$ of the adjacency matrix of n-th power of C_i, i.e., A_f^n, exploiting the eigenvalues of the $V \times V$ all-ones matrix, denoted by J_V. To begin with, let us describe the characteristics of J_V.

Lemma 1. *The eigenvalues of the all-ones matrix J_V are 0 and V, with algebraic multiplicities $V-1$ and 1, respectively.*

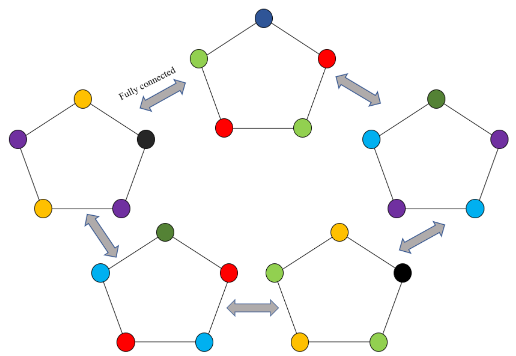

Fig. 3. The 2-nd power of C_5 and its valid coloring.

Proof. See Appendix C. □

The adjacency matrix of the n-th OR power, A_f^n, of a cycle $C_i = G(\mathcal{V}, \mathcal{E})$ is presented as follows:

$$A_f^n = \begin{bmatrix} A_f^{n-1} & J_{V^{n-1}} & 0_{V^{n-1}} & \dots & 0_{V^{n-1}} & J_{V^{n-1}} \\ J_{V^{n-1}} & A_f^{n-1} & J_{V^{n-1}} & 0_{V^{n-1}} & \dots & 0_{V^{n-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ J_{V^{n-1}} & 0_{V^{n-1}} & 0_{V^{n-1}} & \dots & J_{V^{n-1}} & A_f^{n-1} \end{bmatrix} , \quad (5)$$

which has a block structure, with V row partitions of size V for each partition. In every block row of A_f^n, i.e., a sub-matrix of A_f^n that is obtained by selecting a set of consecutive rows from the matrix, with the number of rows equal to the number of rows in A_f^{n-1}, and there are exactly two J_V matrices. From Lemma 1, the largest eigenvalue of the J_V matrix is equal to V, i.e., $\lambda_1(J_V) = V$. In order to calculate the eigenvalues of A_f^n, one needs to solve $|A_f^n - \lambda(C_i^n) I_{V^n}| = 0$.

Let $\lambda_l(C_i), l \in [V]$ be the eigenvalues of A_f, and $\nu_l(C_i^2), l \in [V^2]$ be the eigenvalues of A_f^2 which is a $V^2 \times V^2$ matrix. Let $\mathbf{u}_l$, $l \in [V]$ be the set of eigenvectors of A_f. We also let $\mathbf{v}_l$, $l \in [V^2]$ be the set of eigenvectors of A_f^2.

We solve the equations $A_f \mathbf{u} = \lambda(C_i)\mathbf{u}$ to determine the eigenvalues $\lambda(C_i)$ of A_f. Similarly, for the 2-nd power graph, we have $A_f^2 \mathbf{v} = \nu(C_i^2)\mathbf{v}$ for A_f^2. The eigenvalues $\nu(C_i^2)$ of A_f^2 can be determined by solving the following matrix:

$$\begin{bmatrix} A_f & J_V & 0_V & \dots & 0_V & J_V \\ J_V & A_f & J_V & \dots & 0_V & 0_V \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ J_V & 0_V & 0_V & \dots & J_V & A_f \end{bmatrix} \mathbf{v} = \nu(C_i^2)\mathbf{v} , \quad (6)$$

where $\mathbf{v} = [\mathbf{v}_1^\intercal, \mathbf{v}_2^\intercal, \dots, \mathbf{v}_V^\intercal]^\intercal$, and each $\mathbf{v}_l$, $l \in [V]$ is $V \times 1$. In other words, for each $\nu(C_i^2)$, we have a set of V block row equations, each containing V scalar equations. More specifically, $\nu(C_i^2)$ satisfy the following V block equations:

$$A_f \mathbf{v}_l + J_V \mathbf{v}_{l+1} + J_V \mathbf{v}_{l-1} = \nu(C_i^2)\mathbf{v}_l , \quad l \in [V] . \quad (7)$$

Using (7), we next derive the eigenvalues of A_f^n.

Theorem 3. *The adjacency matrix A_f^n for the n-th OR power of cyclic graphs, where $n \geq 2$, has the same distinct eigenvalues of A_f^{n-1} as well as two new distinct eigenvalues.*

Proof. See Appendix D. □

Let us consider G to be a general characteristic graph with an adjacency matrix A_f. The following section presents bounds on the eigenvalues of A_f^n for n-th OR powers of G.

C. Bounds on Chromatic Number Derived from Eigenvalues

The following inequality provides bounds on χ_G, i.e., the chromatic number of graph $G = (\mathcal{V}, \mathcal{E})$:

$$1 - \frac{\lambda_1(G)}{\lambda_V(G)} \leq \chi_G \leq \lfloor \lambda_1(G) \rfloor + 1 , \quad (8)$$

where $\lambda_1(G)$ is the largest eigenvalue, and $\lambda_V(G)$ is the smallest eigenvalue of G, respectively [40], and the lower and the upper bounds are derived from [41] and [42], respectively.

Our objective is next to refine the bound in (8) for $\chi_{C_i^j}$ derived from A_f^j, $j \in [n]$. To that end, we first consider the smallest eigenvalue of matrix A_f, which is $\lambda_V(C_i)$. In accordance with Brigham and Dutton [43], we have the following lower bound on the V-th eigenvalue in A_f of C_i:

$$\lambda_V(C_i) \geq -\sqrt{2|\mathcal{E}|(V-1)/2} . \quad (9)$$

For the 2-nd power graph C_5^2, (9) yields $\lambda_{V^2}(C_5^2) \geq -60$. The set of distinct eigenvalues, ϑ, for A_f^2 are calculated as $\vartheta(C_5) = \{-1.618, 0.618, 2\}$, and similarly $\vartheta(C_5^2) = \{-6.090, -1.61803, 0.61803, 5.09016, 12\}$ for C_5^2.

Consider the set $\vartheta(C_5^2)$, where $\lambda_{V^2}(C_5^2) = -6.09$, which satisfies the bound presented in (9). Later, Hong [44] has derived the following lower bound for graph G:

$$\lambda_V(G) \geq -\sqrt{(V/2)[(V+1)/2]} , \quad (10)$$

where we note that for C_5^2, it holds that $\lambda_{V^2}(C_5^2) \geq -12.748$. By observing the lower bounds on $\lambda_{V^2}(C_5^2)$ from (9), and (10), for the 2-nd power, one can find that the bound by Hong in [44] is tighter. Hence, we can enhance the bounds on $\chi_{C_i^j}$ in (8) using the bound for $\lambda_V(G)$ in (10) given by Hong [44].

For cyclic graphs, we recall from Theorem 1 that all vertices of C_i^n for $n \geq 2$ have the same degree. Using this result, we next derive an exact characterization for $\lambda_1(C_i^n)$, $n \geq 2$.

Theorem 4. *The largest eigenvalue $\lambda_1(C_i^n)$ of the n-th OR power of a cycle graph C_i^n is determined as follows:*

$$\lambda_1(C_i) = 2 , \quad \lambda_1(C_i^n) = 2 + \sum_{j \in [n-1]} (2V^j) , \; n \geq 2 . \quad (11)$$

Proof. See Appendix E. □

The bounds in (8) are enhanced by utilizing the exact values for $\lambda_1(C_i^n)$ given in Theorem 4. Ideally, we aim to sharpen these and extend them to include a wider range of characteristic graphs beyond cycles. Our method for constructing A_f^n results in a lower complexity versus methods that do not exploit the structure of a given function (e.g., [45] and [46]), hence, leading to a reduced functional compression rate.

By exploiting the bounds on the eigenvalues of A_f given above, we next derive new lower and upper bounds on $\chi_{C_i^n}$.

Proposition 2. *The following bound holds for $\chi_{C_i^n}$:*

$$1-\frac{2+\sum_{j=1}^{n-1}(2V^j)}{-\sqrt{(V^n/2)[(V^n+1)/2]}}\leq\chi_{C_i^n}\leq\sum_{j=1}^{n-1}(2V^j)\ +3\ .$$

Proof. See Appendix G. □

Remark 1. *From Theorem 1, the total number of edges $|\mathcal{E}|$ given in (1), and the lower bound on $\lambda_V(C_i)$ given in (9), we derive the following new bound for $\chi_{C_i^n}$:*

$$1-\frac{2+\sum_{j=1}^{n-1}(2V^j)}{-\sqrt{2|\mathcal{E}|(V^n-1)/2}}\leq\chi_{C_i^n}\leq 1+(2+\sum_{j=1}^{n-1}(2V^j))\ ,$$

where the term $2+\sum_{j=1}^{n-1}(2V^j)$ that appears both in the LHS and RHS is equal to the largest eigenvalue of A_f^n (see (11)).

We provide a more comprehensive overview of the largest and smallest eigenvalues and bounds on chromatic numbers in Appendix F. These bounds were utilized for deriving bounds on the chromatic number of a general graph and comparison purposes alongside the bounds presented in this section.

IV. Conclusions and Future Directions

In this study, we present a new method for distributed compression of functions with characteristic graphs that are represented as cycles and multi-shot computing of functions through OR graph powers. Our approach can achieve the minimum entropy coloring (see e.g., Theorem 1 and Prop. 1) for cycle graphs, while it might not be possible to achieve such a coloring for other connected graph types. Our findings include the analysis of the degree of a vertex for the n-th OR power of cycles and the chromatic number required for coloring even cycles. Additionally, our contributions include a novel scheme for coloring odd cycles that reduces entropy, offering improved compression efficiency. Furthermore, we examine the properties of the adjacency matrices of power graphs, particularly for cycles, and establish bounds for the chromatic number based on the eigenvalues of the adjacency matrices of such graphs. Our approach introduces a new and efficient cyclic coloring technique, as outlined in Prop. 1 and App. B, for the purpose of function compression. Possible future directions include improving the bound in Prop. 2 for general graphs based on the properties in Theorem 2, Lemma 1, and Prop. 1. Specifically, we aim to determine the distribution of coloring, to derive bounds on the entropy of cycle graphs, which will be followed by achieving the entropy of fractional coloring for the n-th OR powers of such graphs (cf. [13]). These bounds can also be applied to characteristic graphs beyond cycles to realize the limits of functional compression for more general computation scenarios.

Appendix

A. Proof of Theorem 1

Consider a cycle $C_i=(\mathcal{V},\mathcal{E})$, with a total number of vertices V. It is known that each vertex in C_i has a degree of two from Defn. 4. The second power can be represented by $C_i^2=(\mathcal{V}^2,\mathcal{E}^2)$, and it has V sub-graphs $\{C_i(1),C_i(2),\dots,C_i(V)\}$. For a given sub-graph, say $C_i(l)$, $l\in[V]$, any $x_1(l)\in C_i(l)$, where $x_1(l)$ denotes a vertex in the l-th replica of C_i, is connected to any vertex of the adjacent sub-graphs, namely $\in\{C_i((l-1) \mod (V)),C_i((l+1) \mod (V))\}$. Therefore, each vertex in $C_i(l)$ has V edges to $C_i((l-1) \mod (V))$ and $C_i((l+1) \mod (V))$ each. For $n=2$, taking the sum of the number of edges between adjacent sub-graphs, and each vertex's degree in the sub-graph itself, the degree of each vertex in C_i^2 is $deg(\mathbf{x}_1^2)=2+2V$. When $n=3$, the degree of vertex $\mathbf{x}_1^3$ can be calculated by adding the number of edges connecting it to adjacent sub-graphs and the degree of the vertex in $n=2$. This results in $deg(\mathbf{x}_1^3)=2+2V+2V^2$.

For a given sub-graph $C_i^{n-1}(l)$, each vertex $\mathbf{x}_1^{n-1}(l)$ is connected to all vertices in the adjacent sub-graphs, $C_i^{n-2}((l-1) \mod (V))$ and $C_i^{n-2}((l+1) \mod (V))$. Therefore, the degree for the $(n-1)$-th power, by considering the previous power's degree and using induction, is going to be $deg(\mathbf{x}_1^{n-1})=2+2V+2V^2+\cdots+2V^{n-2}=2+\sum_{j=1}^{n-2}2(V^j)$.

Similarly, for building the n-th power graph of a cycle, using the same procedure, there are V sub-graphs $\{C_i^{n-1}(1),C_i^{n-1}(2),\dots,C_i^{n-1}(V)\}$. Like the second power graph, the sub-graph $C_i^{n-1}(l)$, $l\in[V]$, is fully connected to the adjacent sub-graphs $\{C_i^{n-1}((l-1) \mod (V)),C_i^{n-1}((l+1) \mod (V))\}$. Therefore, for the n-th power, the degree for each vertex $\mathbf{x}^n$ can be found using (2).

B. Proof of Proposition 1

The cycle characteristic graph C_5 is 3 colorable. The second power, C_5^2, has a valid coloring using 8 colors, as shown in Fig. 3, which provides a saving from the greedy coloring algorithm with 9 colors. We use coloring sets for sub-graphs instead of coloring the entire structure at once and encountering difficulties finding optimal coloring. The coloring set, namely $\mathcal{C}_i(l)$, is a set of colors that can be used for the valid coloring of sub-graph l. It is important to ensure that no two neighboring coloring sets share the same color.

To achieve a valid coloring, we divide the set of vertices into sub-graphs and assign to each a set of colors. The minimum number of colors required for coloring these sets is known. The following example will help us understand it better.

As previously mentioned, coloring C_5 requires three distinct colors, e.g., $\{c_1,c_2,c_3\}$. It is also evident that the cardinality of the color set for C_i^n changes based on $\chi_{C_i^{n-1}}$ that is, the set contains the number of distinct colors needed to color the sub-graph. However, the number of coloring sets is always constant and equal to the number of vertices on C_i, $|\mathcal{V}|=V$. In the case of C_5, there are 5 sets of coloring assigned to the sub-graphs. To cover the sub-graphs assigned to the first two color sets, the adjacent coloring sets cannot share the same colors. Thus, $\{c_1,c_2,\dots,c_6\}$ are required in the first two coloring sets, namely $\mathcal{C}_5^2(1)$ and $\mathcal{C}_5^2(2)$. Consequently, we can reuse the colors from the first set, since there is no edge between the first $C_5^2(1)$ and third $C_5^2(3)$ sub-graphs. It is easy to note that by adding only 2 colors to the third color set and using them in a cyclic manner, all vertices are colored with only 8 colors, which allows us to express $\mathcal{C}_5^2(l)$ for $l \in [5]$ as:

$$\mathcal{C}_5^2(1) = \{c_1, c_2, c_3\}, \qquad \mathcal{C}_5^2(2) = \{c_4, c_5, c_6\},$$
$$\mathcal{C}_5^2(3) = \{c_7, c_8, c_1\}, \qquad \mathcal{C}_5^2(4) = \{c_2, c_3, c_4\},$$
$$\mathcal{C}_5^2(5) = \{c_5, c_6, c_7\} \ .$$

Based on the number of colors used on coloring sets, the size of five coloring sets for the next power will be adjusted. In this case, the set size for the next power is 8. For C_5^3, we will follow the same method, which results in a chromatic number of 20. Hence, we can express $\mathcal{C}_5^3(l)$ for $l \in [5]$ as

$$\mathcal{C}_5^3(1) = \{c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8\},$$
$$\mathcal{C}_5^3(2) = \{c_9, c_{10}, c_{11}, c_{12}, c_{13}, c_{14}, c_{15}, c_{16}\},$$
$$\mathcal{C}_5^3(3) = \{c_{17}, c_{18}, c_{19}, c_{20}, c_1, c_2, c_3, c_4\},$$
$$\mathcal{C}_5^3(4) = \{c_5, c_6, c_7, c_8, c_9, c_{10}, c_{11}, c_{12}\},$$
$$\mathcal{C}_5^3(5) = \{c_{13}, c_{14}, c_{15}, c_{16}, c_{17}, c_{18}, c_{19}, c_{20}\}.$$

Using induction, we can show that C_5^4 requires 50 colors. The followings are the chromatic numbers for the graph powers: $\chi_{C_5^1} = 3$, $\chi_{C_5^2} = 8$, $\chi_{C_5^3} = 20$, $\chi_{C_5^4} = 50$, $\chi_{C_5^5} = 125$, and $\chi_{C_5^6} = 313$, and so on. From this pattern, it is easy to note that, by induction, $\chi_{C_i^{n+1}}$ can be determined as (4).

C. Proof of Lemma 1

Let I_V be the $V \times V$ identity matrix, and J_V be the square $V \times V$ all-ones matrix, which can be represented as follows:

$$J_V = (1_{xx'})_{1 \leq x,\, x' \leq V} \ . \tag{12}$$

For computing the eigenvalues, first, we need to solve the characteristic equation of J_V, which is $J_V \mathbf{u}_V = \lambda(J_V)\mathbf{u}_V$, or equivalently, $|J_V - \lambda(J_V) I_V| = 0$, where $\mathbf{u}$ represents an eigenvector that satisfies the following relationship:

$$J_V \mathbf{u}_V = \lambda(J_V)\mathbf{u}_V = \begin{bmatrix} \mathbf{u}_1 + \mathbf{u}_2 + \cdots + \mathbf{u}_V \\ \vdots \\ \mathbf{u}_1 + \mathbf{u}_2 + \cdots + \mathbf{u}_V \end{bmatrix} = \begin{bmatrix} \lambda(J_V)\mathbf{u}_1 \\ \vdots \\ \lambda(J_V)\mathbf{u}_V \end{bmatrix} .$$

Hence, multiplying J_V by the eigenvectors $\mathbf{u_V}$, clearly, the above relation implies that the eigenvalues $\lambda(J_V)$ satisfy

$$\lambda(J_V) = \begin{cases} V & \text{with multiplicity } \ 1, \\ 0 & \text{with multiplicity } \ V-1 \ , \end{cases}$$

which gives the final result.

D. Proof of Theorem 3

Assume that A_f has V eigenvalues. To find the eigenvalues of A_f^2, one needs to solve the equation, (7), that comes from computing the eigenvalues of (6), which gives V equations for each block row, with V eigenvalues. Hence, there are V^2 equations, from which the remaining $(V-1) \times V$ equations are just replicas of the eigenvalues of any given block row, due to cyclic symmetry. In (7), due to the cyclic nature, the terms with indices $l+1$ and $l-1$ are in modulo V. There are two additional equations necessary for calculating eigenvalues of the adjacency matrix as the power increases from $n-1$ to n. Both A_f and J_V are diagonalizable due to symmetry and can be transformed into diagonal matrices H_{A_f} and H_{J_V} using a matrix P. The relationship between the matrices is expressed as $A_f = P^{-1} H_{A_f} P$ and $J_V = P^{-1} H_{J_V} P$.

Note 1. *In symmetrical matrices, all eigenvalues are real [47].*

If we consider the sum of A_f and J_V, it holds that

$$A_f + J_V = P^{-1} H_{A_f} P + P^{-1} H_{J_V} P = P^{-1}(H_{A_f} + H_{J_V}) P \ .$$

The eigenvalues of $A_f + J_V$ can now be computed using the diagonal of $H_{A_f} + H_{J_V}$, where $\lambda(A_f)$ and $\lambda(J_V)$ represent the eigenvalue of A_f and J_V matrices, respectively.

$$\lambda(A_f + J_V) = \lambda(A_f) + \lambda(J_V) \tag{13}$$

From Lemma 1, the number of distinct eigenvalues of A_f^2 differs from the eigenvalues of A_f at most by two, and similarly for the eigenvalues of A_f^j, $j \in \{\mathbb{Z}^{+\geq 2}\}$ derived from A_f^{j-1} of the $(j-1)-th$ power graph. From (5), the sub-graph A_f^{j-1} in A_f^j will have the following form:

$$A_f^{j-1} \mathbf{v}_l + J_{V^{j-1}} \mathbf{v}_{l+1} + J_{V^{j-1}} \mathbf{v}_{l-1} = \nu \mathbf{v}_l, \quad l \in [V] \ , \tag{14}$$

where $j \in \{\mathbb{Z}^{+\geq 2}\}$, and the dimension of the column vector $\mathbf{v}_l$ is $V^{j-1} \times 1$. The adjacency matrix for the n-th power, namely A_f^n, is constructed by combining A_f^{n-1}, $J_{V^{n-1}}$ from the $(n-1)$-th power, and $V^{n-1} \times V^{n-1}$ zero matrices, as specified in (5). The first block row of A_f^n contains the matrix A_f^{n-1}, the two $J_{V^{n-1}}$ matrices representing full connections to adjacent two sub-graphs, and the remaining $V^{n-1} \times V^{n-1}$ zero matrices indicating the absence of edges between sub-graphs, which impacts the calculation of eigenvalues. Accordingly, the n-th power of the cycle graph has two more distinct eigenvalues from the $(n-1)$-th power of the cycle graph. As a result, by using Lemma 1, we can prove Theorem 3.

E. Proof of Theorem 4

The eigenvalues of the adjacency matrix of C_i^j can be derived through generalizing (7), From (13) and (14) it can be observed that the largest eigenvalue for a power graph C_i^n is obtained by adding up the largest eigenvalue of A_f^{n-1} corresponding to a sub-graph C_i^{n-1} with 2 times the largest eigenvalue of $J_{V^{n-1}}$, which is V^{n-1} (see Lemma 1). Hence, we can derive the final result given in Theorem 4.

F. Additional Bounds on the Largest and Smallest Eigenvalues of Graph Adjacency Matrices

In this section, we will explore several additional bounds on the largest $\lambda_1(G)$ and the smallest $\lambda_V(G)$ eigenvalues of adjacency matrices of a graph $G(\mathcal{V}, \mathcal{E})$, in addition to the ones in Sect. III-C. Barnes in [48] used the Hoffman-Wielandt inequality [49], and the eigenvalues and the eigenvectors of an adjacency matrix to partition the vertex set of a graph such that the resulting partitions have fewer edges between them than any other possible subsets, which ensures a tight upper bound for the largest eigenvalue of the matrix.

For the largest eigenvalue $\lambda_1(G)$, there exist several bounds [44], [50], [51]. For instance, Das and Kumar [50] proved that

$$\lambda_1(G) \geq \sqrt{2|\mathcal{E}| - (V-1)d_V + (d_V - 1)d_1} \ , \quad (15)$$

where $d_1 = \max_{x\in\mathcal{V}}(deg(x))$ and $d_V = \min_{x\in\mathcal{V}}(deg(x))$.

In [50], the authors also bounded $\lambda_V(G)$:

$$\lambda_V(G) \geq -\sqrt{2|\mathcal{E}| - (V-1)d_V + (d_V - 1)d_1} \ . \quad (16)$$

Hong obtained the following lower bound for $\lambda_V(G)$ [44]:

$$\lambda_V(G) \geq -\sqrt{V(V+1)}/2 \ , \quad (17)$$

Similarly, Brigham and Dutton bounded $\lambda_V(G)$ as [43]:

$$\lambda_V(G) \geq -\sqrt{2|\mathcal{E}|(V-1)/2} \ . \quad (18)$$

G. Proof of Proposition 2

Combining equation (8), which bounds $\lambda_1(G)$ and $\lambda_V(G)$ of A_f for $G = C_i^n$, with Theorem 4, as well as the Hong bound (10) for $\lambda_V(G)$ [44], we have

$$1 - \frac{2 + \sum_{j=1}^{n-1}(2V^j)}{-\sqrt{(n/2)[(n+1)/2]}} \leq \chi_G \leq \left\lfloor 2 + \sum_{j=1}^{n-1}(2V^j) \right\rfloor + 1 \ .$$

Further simplifying the floor function on the RHS by plugging a positive integer-valued $\lambda_1(C_i^n)$ (see Theorem 4), we obtain the result in Prop. 2.

References

[1] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, Jul. 1948.

[2] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, Jul. 1973.

[3] N. Alon and A. Orlitsky, "Source coding and graph entropies," *IEEE Trans. Inf. Theory*, vol. 42, no. 5, pp. 1329–1339, Sep. 1996.

[4] M. Pawlak, E. Rafajlowicz, and A. Krzyzak, "Postfiltering versus prefiltering for signal recovery from noisy samples," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3195–3212, Dec. 2003.

[5] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Sep. 2006.

[6] R. Ahlswede, N. Cai, S.-Y. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[7] C. Shannon, "The zero error capacity of a noisy channel," *IRE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, Sep. 1956.

[8] V. Doshi, D. Shah, M. Médard, and S. Jaggi, "Distributed functional compression through graph coloring," in *Proc., IEEE Data Compression Conf. (DCC)*, Snowbird, UT, USA, Mar. 2007, pp. 93–102.

[9] V. Doshi, D. Shah, M. Médard, and M. Effros, "Functional compression through graph coloring," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3901–3917, Jul. 2010.

[10] A. Orlitsky and J. R. Roche, "Coding for computing," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, p. 903–917, Mar. 2001.

[11] ——, "Coding for computing," in *Proc., Annu. IEEE Symp. Found. Comput. Sci.*, Milwaukee, WI, USA, Oct. 1995, pp. 502–511.

[12] S. Feizi and M. Médard, "On network functional compression," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5387–5401, Jun. 2014.

[13] D. Malak, "Fractional graph coloring for functional compression with side information," in *Proc., IEEE Inf. Theory Wksh.*, Mumbai, India, Nov. 2022.

[14] J. Korner and K. Marton, "How to encode the modulo-two sum of binary sources (corresp.)," *IEEE Trans. Inf. Theory*, vol. 25, no. 2, pp. 219–221, Mar. 1979.

[15] R. Ahlswede and J. Korner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Trans. Inf. Theory*, vol. 21, no. 6, pp. 629–637, Nov. 1975.

[16] T. P. Coleman, A. H. Lee, M. Médard, and M. Effros, "Low-complexity approaches to slepian–wolf near-lossless distributed data compression," *IEEE Trans. Inf. Theory*, vol. 52, no. 8, pp. 3546–3561, Jul. 2006.

[17] T. Han and K. Kobayashi, "A dichotomy of functions F(X, Y) of correlated sources (X, Y)," *IEEE Trans. Inf. Theory*, vol. 33, no. 1, pp. 69–76, Jan. 1987.

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

[19] D. Malak, "Weighted graph coloring for quantized computing," in *Proc., Int. Symp. on Inf. Theory*, Taipei, Taiwan, Jun. 2023.

[20] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, pp. 1–10, Jan 1976.

[21] H. Feng, M. Effros, and S. Savari, "Functional source coding for networks with receiver side information," in *Proc., Annu. Allerton Conf. Commun. Control Comput.*, Monticello, IL, Sep. 2004, pp. 1419–1427.

[22] H. Yamamoto, "Wyner-Ziv theory for a general function of the correlated sources (corresp.)," *IEEE Trans. Inf. Theory*, vol. 28, no. 5, pp. 803–807, Sep. 1982.

[23] T. Berger and R. W. Yeung, "Multiterminal source encoding with one distortion criterion," *IEEE Trans. Inf. Theory*, vol. 35, no. 2, pp. 228–236, Mar. 1989.

[24] J. Barros and S. D. Servetto, "On the rate-distortion region for separate encoding of correlated sources," in *Proc., IEEE Int. Symp. Inf. Theory*. Yokohama, Japon: IEEE, Jun. 2003, p. 171.

[25] A. B. Wagner, S. Tavildar, and P. Viswanath, "Rate region of the quadratic gaussian two-encoder source-coding problem," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 1938–1961, Apr. 2008.

[26] C. Paar and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.

[27] W. Diffie and M. E. Hellman, "Multiuser cryptographic techniques," in *Proc., Nat. Comp. Conf. and Expo.*, New York, NY, Jun 1976, pp. 109–112.

[28] D. Selent, "Advanced encryption standard," *Rivier Academic Journal*, vol. 6, no. 2, pp. 1–14, Sep. 2010.

[29] S. Basu, "International data encryption algorithm (idea)–a typical illustration," *J. Global Research in Computer Science*, vol. 2, no. 7, pp. 116–118, Aug. 2011.

[30] G. Knill, "Applications: International standard book numbers," *The Mathematics Teacher*, vol. 74, no. 1, pp. 47–48, Jan. 1981.

[31] J. Körner and A. Orlitsky, "Zero-error information theory," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2207–2229, Oct. 1998.

[32] J. Cardinal, S. Fiorini, and G. Joret, "Tight results on minimum entropy set cover," *Algorithmica*, vol. 51, no. 1, pp. 49–60, May. 2008.

[33] V. Havel, "A remark on the existence of finite graphs," *Casopis Pro Pestovani Matematiky*, vol. 80, pp. 477–480, 1955.

[34] R. Beigel, "Finding maximum independent sets in sparse and general graphs," in *Proc., SODA*, Baltimore, MD, Jan. 1999, pp. 856–857.

[35] W.-K. Chen, *Graph theory and its engineering applications*. World Scientific, 1997, vol. 5.

[36] J. Körner, "Coding of an information source having ambiguous alphabet and the entropy of graphs," in *Proc., Prague Conf. Inf. Theory*, Prague, Hungary, Sep. 1973, pp. 411–425.

[37] J. F. Nagle, "On ordering and identifying undirected linear graphs," *J. Math. Phys.*, vol. 7, no. 9, pp. 1588–1592, Sep. 1966.

[38] A. Nilli, "On the second eigenvalue of a graph," *Discrete Math.*, vol. 91, no. 2, pp. 207–210, Aug. 1991.

[39] N. Alon, "Graph powers," *Contemporary Combinatorics*, vol. 10, pp. 11–28, 2002.

[40] B. Aspvall and J. R. Gilbert, "Graph coloring using eigenvalue decomposition," *SIAM J. Algeb. Discrete Methods*, vol. 5, no. 4, pp. 526–538, Dec. 1984.

[41] A. J. Hoffman and L. Howes, "On eigenvalues and colorings of graphs, ii," *Ann. N. Y. Acad. Sci.*, vol. 175, no. 1, pp. 238–242, Jul. 1970.

[42] H. S. Wilf, "The eigenvalues of a graph and its chromatic number," *J. London Math. Soc.*, vol. 1, no. 1, pp. 330–332, Jan. 1967.

[43] R. C. Brigham and R. D. Dutton, "Bounds on graph spectra," *J. Comb. Theory Ser. B*, vol. 37, no. 3, pp. 228–234, Dec. 1984.

[44] Y. Hong, "Bounds of eigenvalues of a graph," *Acta Mathematicae Applicatae Sinica*, vol. 4, no. 2, pp. 165–168, May. 1988.

[45] T. R. Jensen and B. Toft, *Graph coloring problems*. John Wiley & Sons, 2011.

[46] H. Hajiabolhassan, "On colorings of graph powers," *Discrete Math.*, vol. 309, no. 13, pp. 4299–4305, 2009.

[47] B. N. Parlett, *The symmetric eigenvalue problem*. SIAM, 1998.

[48] E. R. Barnes, "An algorithm for partitioning the nodes of a graph," *SIAM J. Algeb. Discrete Methods*, vol. 3, no. 4, pp. 541–550, Dec. 1982.

[49] A. Hoffman and H. Wielandt, "The variation of the spectrum of a normal matrix," *Duke Math. J.*, vol. 20, pp. 37–39, 1953.

[50] K. C. Das and P. Kumar, "Some new bounds on the spectral radius of graphs," *Discrete Math.*, vol. 281, no. 1-3, pp. 149–161, Apr. 2004.

[51] O. Favaron, M. Mahéo, and J.-F. Saclé, "Some eigenvalue properties in graphs (conjectures of graffiti—ii)," *Discrete Math.*, vol. 111, no. 1-3, pp. 197–220, Feb. 1993.