Permute & Add Network Codes via Group Algebras

Lakshmi Prasad Natarajan and Smiju Kodamthuruthil Joy

***Abstract*—A class of network codes have been proposed in the literature where the symbols transmitted on network edges are binary vectors and the coding operation performed in network nodes consists of the application of (possibly several) permutations on each incoming vector and XOR-ing the results to obtain the outgoing vector. These network codes, which we will refer to as *permute-and-add* network codes, involve simpler operations and are known to provide lower complexity solutions than scalar linear codes. The complexity of these codes is determined by their *degree* which is the number of permutations applied on each incoming vector to compute an outgoing vector. Constructions of permute-and-add network codes for multicast networks are known. In this paper, we provide a new framework based on group algebras to design permute-and-add network codes for arbitrary (not necessarily multicast) networks. Our framework allows the use of any finite group of permutations (including circular shifts, proposed in prior work) and admits a trade-off between coding rate and the degree of the code. Further, our technique permits elegant recovery and generalizations of the key results on permute-and-add network codes known in the literature.**

2021 IEEE International Symposium on Information Theory (ISIT) | 978-1-5386-8209-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISIT45174.2021.9517898

I. Introduction

Network coding theory [1] is dominated by the study of linear network codes [2]–[6]. In *scalar linear network coding* the symbols carried by each network edge is an element of a finite field $\mathbb{F}_q$, and is obtained by computing an $\mathbb{F}_q$-linear combination of the symbols carried in its parent edges. It is well known that scalar linear network coding is sufficient to achieve the capacity of multicast networks as long as the size of the field $\mathbb{F}_q$ is sufficiently large [2], [3]. Note that a scalar linear network coding solution requires all the network nodes to perform arithmetic over a (possibly large) finite field.

An alternative to scalar linear network coding, which can simplify network coding operations, is to use vector linear network codes where the encoding kernels are linear combinations of permutation matrices [7]–[13]. For these network codes, the symbols carried by the network edges are length-n binary vectors, and the coding operation performed at a network node is the application of (possibly several) permutations on each incoming binary vector and adding (XOR-ing) the permuted vectors to determine the outgoing binary vector. Using the vocabulary of [7] (and by mildly generalizing its terminology), we will refer to such network codes as *permute-and-add* network codes. The *degree* of a permute-and-add network code is the maximum number of permutations applied on each incoming binary vector to compute an outgoing vector at any node [11], [12]. Note that the degree determines the number of XORs to be performed at each node. Since the task of performing permutations is cheap, the degree acts as a proxy for the complexity of a permute-and-add network code. It is known that permute-and-add network codes can provide lower complexity coding operations than scalar linear network coding [7], [11].

The permute-and-add codes of [7] were proposed for multicast networks using a random coding framework. These codes employ degree 1 permute-and-add operation at non-sink nodes, while the decoding matrices are dense, indicating high complexity at sink nodes. The prior works [8]–[13] all employ only circular shifts (i.e., cyclic permutations) for coding operations, and following [11], we will refer to these permute-and-add network codes as *circular-shift* network codes. A deterministic circular-shift network code was proposed in [8] for combination networks in which the coding operations performed at non-sink nodes are of degree 1. The existence of circular-shift network coding solutions for multicast networks was proved in [9]. Codes for repairing failed disks in distributed storage systems that make use of circular-shift network codes were proposed in [10]. Circular-shift network codes were designed in [11]–[13] for multicast networks by lifting scalar linear network codes. A similar code over $\mathbb{Z}_{256}$ was designed in [14]. Note that most of the prior works on permute-and-add network codes propose solutions for multicast networks only.

In this paper we provide a new algebraic framework for designing permute-and-add network codes. We use the ring theoretic platform of Connelly and Zeger [15], [16] and show that permute-and-add network codes can be obtained from linear network codes over ideals of group algebras. Unlike previous works, our technique applies to arbitrary directed acyclic multigraphs (which are not necessarily multicast networks), and both the encoding as well as the decoding procedures of our network codes employ permute-and-add operations. Further, our framework admits the use of any finite group of permutations (including circular-shifts) and allows the designer to trade-off the rate of the network code to achieve a smaller degree. The generality of our technique permits us to recover and generalize some of the key results from [11], [12]. We introduce the network model and establish our group-algebraic framework in Section II. We discuss the solvability of a network using permute-and-add operations in Section III. This paper's full version [17] contains proofs of all the claims.

Notation: For integers a, b, the symbol (a, b) denotes their gcd. Unless otherwise specified, all vectors are column vectors.

II. Network Coding using Group Algebras

We first review group codes, group algebras and their matrix representation, and then use these tools to obtain permute-and-

The authors are with the Department of Electrical Engineering, Indian Institute of Technology Hyderabad, Sangareddy 502 285, India (email: {lakshminatarajan, ee17resch11017}@iith.ac.in).

This work was supported by SERB-DST, Government of India (via projects MTR/2019/001454 and DST/INSPIRE/04/2015/002094).

add network codes.

A. Review of Group Algebras and Group Codes

Let G be a finite group (not necessarily commutative) and $\mathbb{F}_2 = \{0, 1\}$ the finite field of size 2. The group algebra $\mathbb{F}_2[G]$ is the set of all possible formal sums $\sum_{g\in G} a_g g$, where $a_g \in \mathbb{F}_2$. The addition and multiplication operations in $\mathbb{F}_2[G]$ are defined as $\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G}(a_g + b_g)g$ and $\big(\sum_{g\in G} a_g g\big)\cdot\big(\sum_{g\in G} b_g g\big) = \sum_{g\in G}\big(\sum_{h\in G} a_h b_{h^{-1}g}\big)g$, respectively. The ring $\mathbb{F}_2[G]$ is commutative if and only if G is Abelian. A *group code* $\mathbb{M}$ is a left-ideal of $\mathbb{F}_2[G]$, i.e., $\mathbb{M}$ is a subgroup of $(\mathbb{F}_2[G], +)$ such that $rm \in \mathbb{M}$ for all $r \in \mathbb{F}_2[G]$ and $m \in \mathbb{M}$. Any group code $\mathbb{M}$ is a left $\mathbb{F}_2[G]$-module where the action of a ring element on $\mathbb{M}$ is the same as the product of elements in $\mathbb{F}_2[G]$.

Using $n = |G|$ to denote the order of the group G, we observe that there is a natural $\mathbb{F}_2$-linear embedding $\tau_{\mathrm{nat}} : \mathbb{F}_2[G] \to \mathbb{F}_2^n$ that maps $m = \sum_{g\in G} m_g g$ to the column vector $(m_g)_{g\in G}$ using some fixed ordering of elements of G.

The *regular representation* [18] of G in $\mathbb{F}_2^n$ maps each $g \in G$ to a permutation matrix $\rho_g^{\mathrm{reg}} \in \mathbb{F}_2^{n\times n}$. If the rows and columns of ρ_g^{reg} are indexed by the elements of G, the entry in the k^{th} row and h^{th} column of ρ_g^{reg}, where $k, h \in G$, is

$$\rho_g^{\mathrm{reg}}(k, h) = 1 \text{ if } k = gh \quad \text{and} \quad \rho_g^{\mathrm{reg}}(k, h) = 0 \text{ otherwise.}$$

The *regular matrix representation* [19] of the algebra $\mathbb{F}_2[G]$ is the injective algebra homomorphism $\sum_{g\in G} r_g g \to \sum_{g\in G} r_g \rho_g^{\mathrm{reg}}$ from $\mathbb{F}_2[G]$ into $\mathbb{F}_2^{n\times n}$. For any choice of $r = \sum_{g\in G} r_g g \in \mathbb{F}_2[G]$ and $m \in \mathbb{F}_2[G]$, we have

$$\tau_{\mathrm{nat}}(rm) = \Big(\sum_{g\in G} r_g \rho_g^{\mathrm{reg}}\Big) \times \tau_{\mathrm{nat}}(m) \tag{1}$$

where $\times$ denotes the matrix-vector product.

Example 1. To illustrate the matrix representation of a group algebra, consider the ring $\mathbb{F}_2[C_3]$ where $C_3 = \{e, \gamma, \gamma^2\}$ is the cyclic group of order 3 and $e \in C_3$ is the identity element. Let $\tau_{\mathrm{nat}} : \mathbb{F}_2[C_3] \to \mathbb{F}_2^3$ be the map $m_e e + m_\gamma \gamma + m_{\gamma^2}\gamma^2 \to (m_e, m_\gamma, m_{\gamma^2})$. The matrix representation ρ_e^{reg} of the identity element e is the 3×3 identity matrix over $\mathbb{F}_2$ while

$$\rho_\gamma^{\mathrm{reg}} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \text{ and } \rho_{\gamma^2}^{\mathrm{reg}} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

The matrix representation of $r_e e + r_\gamma \gamma + r_{\gamma^2}\gamma^2 \in \mathbb{F}_2[C_3]$ is

$$\begin{bmatrix} r_e & r_{\gamma^2} & r_\gamma \\ r_\gamma & r_e & r_{\gamma^2} \\ r_{\gamma^2} & r_\gamma & r_e \end{bmatrix}.$$

□

B. Permute-and-Add Network Codes from Group Algebras

Consider a group algebra $\mathbb{F}_2[G]$ and a left ideal $\mathbb{M} \subset \mathbb{F}_2[G]$. We use the ring theoretic model of Connelly and Zeger [15], [16], where $\mathbb{F}_2[G]$ and $\mathbb{M}$ play the roles of the ring and the module, respectively. We will assume that the network is a directed acyclic multigraph with finitely many nodes and edges. We let each edge carry an element $m \in \mathbb{M}$ by communicating $\tau_{\mathrm{nat}}(m) \in \mathbb{F}_2^n$. The linear coding operations performed at the nodes are over $\mathbb{F}_2[G]$ and $\mathbb{M}$, while the alphabet used for communicating along the edges is $\mathbb{F}_2^n$.

A *message* is an information-bearing random variable taking values in $\mathbb{M}$. We assume that there are finitely many messages generated in the network, and each message can be demanded by more than one sink node. The set of incoming edges at a node v will be denoted as $\mathrm{In}(v)$ and the set of outgoing edges of v is $\mathrm{Out}(v)$. Without loss of generality, we assume: *(i)* there are s messages $Z_1, \ldots, Z_s$, each generated at a unique source node; *(ii)* source nodes have no incoming edges; and *(iii)* if v is a source node generating $Z_i \in \mathbb{M}$ then every outgoing edge of v carries the vector $\tau_{\mathrm{nat}}(Z_i)$.

We will use $X_e \in \mathbb{F}_2^n$ to denote the vector carried along the edge e. An encoding coefficient $k^{d,e} \in \mathbb{F}_2[G]$ is assigned to each pair (d, e) of adjacent edges, i.e., if there exists a node v such that $d \in \mathrm{In}(v)$ and $e \in \mathrm{Out}(v)$. For every outgoing edge $e \in \mathrm{Out}(v)$ of a non-source node v, we have $X_e = \tau_{\mathrm{nat}}(\sum_{d\in\mathrm{In}(v)} k^{d,e}\tau_{\mathrm{nat}}^{-1}(X_d))$. Similarly, a sink node v demanding a message Z_i uses a linear operation $\tau_{\mathrm{nat}}(\sum_{d\in\mathrm{In}(v)} k^{d,i}\tau_{\mathrm{nat}}^{-1}(X_d))$ to decode $\tau_{\mathrm{nat}}(Z_i)$, where the decoding coefficients $k^{d,i} \in \mathbb{F}_2[G]$. For brevity, we denote the set of all encoding and decoding coefficients as $\{k^{d,e}\}$ and $\{k^{d,i}\}$, respectively. Let the expansions of these coefficients be $k^{d,e} = \sum_{g\in G} k_g^{d,e} g$ and $k^{d,i} = \sum_{g\in G} k_g^{d,i} g$, where $k_g^{d,e}, k_g^{d,i} \in \mathbb{F}_2$. Using (1) and the fact that τ_{nat} is a $\mathbb{F}_2$-linear map, we observe that the encoding and decoding operations performed in the network can be realized as

$$X_e = \tau_{\mathrm{nat}}\Big(\sum_{d\in\mathrm{In}(v)} k^{d,e}\tau_{\mathrm{nat}}^{-1}(X_d)\Big) = \sum_{d\in\mathrm{In}(v)} \sum_{\substack{g\in G:\\ k_g^{d,e}=1}} \rho_g^{\mathrm{reg}} \times X_d,$$

$$\tau_{\mathrm{nat}}(Z_i) = \tau_{\mathrm{nat}}\Big(\sum_{d\in\mathrm{In}(v)} k^{d,i}\tau_{\mathrm{nat}}^{-1}(X_d)\Big) = \sum_{d\in\mathrm{In}(v)} \sum_{\substack{g\in G:\\ k_g^{d,i}=1}} \rho_g^{\mathrm{reg}} \times X_d, \tag{2}$$

respectively. This is a permute-and-add network code since the encoding and decoding operations involve the application of (possibly several) permutations ρ_g^{reg} on each incoming vector X_d and computing their sum.

We also note that this network code is a linear code over the $\mathbb{F}_2[G]$-left module $\mathbb{M}$. The embeddings τ_{nat} and ρ^{reg} simply allow us to realize the coding operations as sums of matrix-vector products, i.e., as a fractional linear network code [4] over $\mathbb{F}_2$. Hence, we can use the framework of [15], [16] to study the existence of network coding solutions.

Remark 1. The *circular-shift network codes* proposed in [11], [12] correspond to the case where G is a cyclic group of odd order. Since G is cyclic, the permutations ρ_g^{reg}, $g \in G$, used for encoding and decoding are all cyclic permutation matrices. The odd order of the group implies that the characteristic of $\mathbb{F}_2$ does not divide $|G|$, and hence, $\mathbb{F}_2[G]$ is semi-simple. □

A *network code* over $\mathbb{M}$ is the collection of all encoding and decoding coefficients $\{k^{d,e}\}$ and $\{k^{d,i}\}$. A network code is a *solution* if each sink node can decode its demand.

C. The Degree of Permute-and-Add Network Codes

In the literature [11], [12], the complexity of a permute-and-add network code is measured in terms of the number of permutations applied on each incoming vector X_d. From (2), the number of permutations applied on X_d to compute X_e is $|\{g \in G \mid k_g^{d,e} = 1\}| = \mathsf{wt}(\tau_{\mathrm{nat}}(k^{d,e}))$, which is the Hamming weight of the vector $\tau_{\mathrm{nat}}(k^{d,e})$. We abuse the notation mildly to denote this quantity as $\mathsf{wt}(k^{d,e})$. Similarly, the number of permutations applied on X_d to decode $\tau_{\mathrm{nat}}(Z_i)$ is $\mathsf{wt}(k^{d,i})$.

Definition 1. An $\mathbb{F}_2[G]$-linear network code over a left-ideal $\mathbb{M}$ is of *degree* δ if $\mathsf{wt}(k^{d,e}), \mathsf{wt}(k^{d,i}) \leq \delta$ for all the network coding coefficients $k^{d,e}$ and $k^{d,i}$.

We now show that the annihilator of $\mathbb{M}$ can be used to upper bound the degree of a linear network code over $\mathbb{M}$. The annihilator of $\mathbb{M}$ in the ring $\mathbb{F}_2[G]$ is $\mathrm{Ann}(\mathbb{M}) = \{r \in \mathbb{F}_2[G] \mid rm = 0 \text{ for all } m \in \mathbb{M}\}$. As a module over $\mathbb{F}_2[G]$, $\mathbb{M}$ is *unfaithful* if $\mathrm{Ann}(\mathbb{M}) \neq \{0\}$. We first make a simple observation.

Lemma 1. *For any choice of $a^{d,e}, a^{d,i} \in \mathrm{Ann}(\mathbb{M})$, if the original network code $\{k^{d,e}\}$, $\{k^{d,i}\}$ is a solution to the given network, then the modified network code $\{k^{d,e}+a^{d,e}\}$, $\{k^{d,i}+a^{d,i}\}$ is also a solution to this network.*

Proof Idea: The modified network code is obtained by adding an arbitrary element of $\mathrm{Ann}(\mathbb{M})$ to each coefficient of the original network code. Hence, $(k^{d,e}+a^{d,e})\tau_{\mathrm{nat}}^{-1}(X_d) = k^{d,e}\tau_{\mathrm{nat}}^{-1}(X_d)$, since $\tau_{\mathrm{nat}}^{-1}(X_d) \in \mathbb{M}$. We use this property to show that for each edge of the network, the symbols carried by the original network code and the modified network code are identical. See Lemma 1 of [17] of for a full proof in a general setting where $\mathbb{F}_2[G]$ and $\mathbb{M}$ are replaced by any ring R and a module M over the ring R, respectively. □

We know that the annihilator $\mathrm{Ann}(\mathbb{M})$ is a two-sided ideal of $\mathbb{F}_2[G]$, see [20]. In particular, $\mathrm{Ann}(\mathbb{M})$ is an additive subgroup of $\mathbb{F}_2[G]$. Since τ_{nat} is a $\mathbb{F}_2$-linear map we deduce that $\tau_{\mathrm{nat}}(\mathrm{Ann}(\mathbb{M})) = \{\tau_{\mathrm{nat}}(a) \mid a \in \mathrm{Ann}(\mathbb{M})\}$ is a subgroup of $\mathbb{F}_2^n$, i.e., $\tau_{\mathrm{nat}}(\mathrm{Ann}(\mathbb{M}))$ is a binary linear code. The *covering radius* of this linear code is $r_{\mathrm{cov}} = \max_{\boldsymbol{v}\in\mathbb{F}_2^n} \left\{\min_{\boldsymbol{a}\in\tau_{\mathrm{nat}}(\mathrm{Ann}(\mathbb{M}))} \mathsf{wt}(\boldsymbol{v}+\boldsymbol{a})\right\}$. For any vector in $\mathbb{F}_2^n$ there exists a vector in $\tau_{\mathrm{nat}}(\mathrm{Ann}(\mathbb{M}))$ at a distance of at the most r_{cov}. By abusing the notation mildly, we use $r_{\mathrm{cov}}(\mathrm{Ann}(\mathbb{M}))$ to denote the covering radius of $\tau_{\mathrm{nat}}(\mathrm{Ann}(\mathbb{M}))$.

We modify a given network code $\{k^{d,e}\}, \{k^{d,i}\}$ as follows. For each coefficient $k^{d,e}$ we choose a vector $\boldsymbol{a}^{d,e} \in \tau_{\mathrm{nat}}(\mathrm{Ann}(\mathbb{M}))$ such that $\mathsf{wt}(\tau_{\mathrm{nat}}(k^{d,e}) + \boldsymbol{a}^{d,e}) \leq r_{\mathrm{cov}}$. We then use $a^{d,e} = \tau_{\mathrm{nat}}^{-1}(\boldsymbol{a}^{d,e})$ to modify the coefficient $k^{d,e}$ to $k^{d,e}+a^{d,e}$. We observe that $a^{d,e} \in \mathrm{Ann}(\mathbb{M})$ and the weight of the modified coefficient $k^{d,e}+a^{d,e}$ is at the most r_{cov}. Using a similar strategy, for each decoding coefficient $k^{d,i}$ we choose $a^{d,i} \in \mathrm{Ann}(\mathbb{M})$ such that $\mathsf{wt}(k^{d,i}+a^{d,i}) \leq r_{\mathrm{cov}}$. We conclude that the modified network code is of degree r_{cov}.

Using Lemma 1, we see that any $\mathbb{F}_2[G]$-linear network code over a group code $\mathbb{M}$ can be modified to a degree-r_{cov} network code without affecting the messages passed in any of the edges or the ability of the sinks to decode their demands. Hence, without loss of generality, we identify a given network code with its modified counterpart. By doing so we have proved

Theorem 1. *Any $\mathbb{F}_2[G]$-linear network code over a left-ideal $\mathbb{M}$ is a degree $r_{\mathrm{cov}}(\mathrm{Ann}(\mathbb{M}))$ permute-and-add network code.*

Since the network edges carry length n binary vectors and the messages belong to $\mathbb{M}$, the rate of this fractional linear network code is $\log_2|\mathbb{M}|/n = \dim(\mathbb{M})/n$, which is the ratio of the dimension of $\mathbb{M}$ (as a vector space over $\mathbb{F}_2$) to $|G|$.

Remark 2. There exists a trade-off between rate and degree. If ideals $\mathbb{M}'$ and $\mathbb{M}$ are such that $\mathbb{M}' \subset \mathbb{M}$, then $\mathrm{Ann}(\mathbb{M}') \supset \mathrm{Ann}(\mathbb{M})$, and hence, $r_{\mathrm{cov}}(\mathrm{Ann}(\mathbb{M}')) \leq r_{\mathrm{cov}}(\mathrm{Ann}(\mathbb{M}))$. Thus a network code designed over a smaller ideal will achieve a smaller degree at the cost of yielding a lower rate. See Example 2 (Section III) for an illustration. □

We have the following result as a corollary to Theorem 1.

Corollary 1. *If $\mathbb{M}$ is a left-ideal of $\mathbb{F}_2[G]$ such that the weight of every element of $\mathbb{M}$ is even, then every $\mathbb{F}_2[G]$-linear network code over $\mathbb{M}$ is a degree $\left\lfloor \frac{n}{2} \right\rfloor$ network code, where $n = |G|$.*

Proof. We first observe that $\sum_{h\in G} 1h \in \mathrm{Ann}(\mathbb{M})$, since for any $\sum_{g\in G} m_g g \in \mathbb{M}$ we have $(\sum_{h\in G} 1h) \cdot (\sum_{g\in G} m_g g) = \sum_{g\in G}(\sum_{h\in G} m_h)g = 0$. Clearly, $\sum_{g\in G} 0g \in \mathrm{Ann}(\mathbb{M})$. Thus, $\tau_{\mathrm{nat}}(\mathrm{Ann}(\mathbb{M}))$ contains the all-zeros and the all-ones vectors, i.e., the repetition code is a subcode of $\tau_{\mathrm{nat}}(\mathrm{Ann}(\mathbb{M}))$. Since the covering radius of the repetition code is $\left\lfloor \frac{n}{2} \right\rfloor$, we conclude that $r_{\mathrm{cov}}(\mathrm{Ann}(\mathbb{M})) \leq \left\lfloor \frac{n}{2} \right\rfloor$. □

Note that Theorem 1 does not address the question of whether a $\mathbb{F}_2[G]$-linear network coding *solution* over the left-ideal $\mathbb{M}$ exists. We consider this in Section III.

III. Existence of Network Coding Solutions

We first recall some basic results related to network coding over modules [16] in Section III-A, and use them to analyze network codes over ideals of $\mathbb{F}_2[G]$ in the rest of this section.

A. Review of Linear Network Codes over Modules

We sometimes denote a left R-module M as ${}_RM$, where R is the underlying ring. A module ${}_RM$ is *unfaithful* if its annihilator $\mathrm{Ann}(M) \triangleq \{r \in R \mid rm = 0 \text{ for all } m \in M\}$ is not equal to $\{0\}$, and is *faithful* otherwise. In a linear network code over ${}_RM$ the symbols transmitted on network edges belong to M while the coding coefficients belong to R. A code over ${}_RR$ is a *scalar linear code* over R. A network is *solvable* over ${}_RM$ if it has a linear solution over ${}_RM$.

Theorem 2. *[16, Lemma I.6] Let the rings R and S be such that there exists a ring homomorphism from R to S. If a*

network is solvable over some faithful R-module then it is solvable over every S-module.

Every ring is a faithful module over itself. Hence, if a network is scalar linearly solvable over R and if there is a homomorphism from R to S, then the network is scalar linearly solvable over S. Also, choosing $S = R$ in Theorem 2, we deduce that solvability over a faithful R-module implies scalar linear solvability over R.

A scalar linear solution over $\mathbb{F}_2[G]$ uses $\mathbb{M} = \mathbb{F}_2[G]$, and hence, provides the highest rate among all choices of ideals $\mathbb{M}$. In [12] it was shown that if G is a cyclic group of odd order a *multicast* network has a scalar linear solution over $\mathbb{F}_2[G]$ if and only if it is scalar linearly solvable over $\mathbb{F}_2$. We generalize this result to arbitrary networks and finite groups.

Corollary 2. *A network has a scalar linear solution over $\mathbb{F}_2[G]$ if and only if it has a scalar linear solution over $\mathbb{F}_2$.*

Proof. The function that maps $\sum_g a_g g$ to $\sum_g a_g$ is a ring homomorphism from $\mathbb{F}_2[G]$ onto $\mathbb{F}_2$. Similarly, the function that maps $a \in \mathbb{F}_2$ to $a\,e \in \mathbb{F}_2[G]$, where e is the identity element of G, is a ring homomorphism. The proof follows by invoking Theorem 2 using both these homomorphisms. □

Lemma II.6 of [16] analyzes the case where a network is solvable over an unfaithful R-module M. Its proof uses the fact that $\mathrm{Ann}(M)$ is a two-sided ideal in R and that M is a faithful $R/\mathrm{Ann}(M)$-module, see [20]. Using the natural homomorphism from R to $R/\mathrm{Ann}(M)$ the proof shows that the existence of an ${}_R M$ linear solution implies the existence of an ${}_{R/\mathrm{Ann}(M)}M$ linear solution. Since M is faithful over $R/\mathrm{Ann}(M)$, using Theorem 2, we conclude that the existence of an ${}_R M$-linear solution implies the existence of a scalar linear solution over the ring $R/\mathrm{Ann}(M)$. Hence, the statement of [16, Lemma II.6] is essentially the "only if" part of

Theorem 3. *A network is linearly solvable over ${}_R M$ if and only if it is scalar linearly solvable over $R/\mathrm{Ann}(M)$.*

Proof Idea: The proof of the "if" part is similar to the proof of [16, Lemma II.6] and uses the same ideas in the logically reverse direction. See [17, Theorem 3] for complete proof. □

B. Network Codes from Semi-Simple Abelian Group Algebras

In the rest of this paper we will assume that G is an Abelian group of *odd* order and $\mathbb{M}$ is an ideal in $\mathbb{F}_2[G]$.

The fact that $|G|$ is odd implies that $\mathbb{F}_2[G]$ is semi-simple. Several well known families of error correcting codes are ideals in semi-simple Abelian group algebras, such as BCH codes, punctured Reed-Muller codes, quadratic residue codes and bicyclic codes [21]–[24].

The transform domain treatment of Abelian codes in [25] provides an isomorphism of $\mathbb{F}_2[G]$ onto a direct product of finite fields using Discrete Fourier Transforms. This subsumes the spectral characterization [26] of cyclic codes. We know that [25, Theorem 1] there exists a ring isomorphism

$$\Phi:\ \mathbb{F}_2[G] \to \mathcal{R} \triangleq \mathbb{F}_{q_1} \times \mathbb{F}_{q_2} \times \cdots \times \mathbb{F}_{q_t} \tag{3}$$

where t is a positive integer and $q_1, \ldots, q_t$ are powers of 2. The ring $\mathcal{R}$ has t minimal ideals, the k^{th} minimal ideal is generated by $\theta_k = (0, \ldots, 0, 1, 0, \ldots, 0)$ where the only non-zero entry of θ_k occurs in the k^{th} position. The ideal generated by θ_k is $\langle \theta_k \rangle = \{0\} \times \cdots \times \{0\} \times \mathbb{F}_{q_k} \times \{0\} \times \cdots \times \{0\}$. Any ideal of $\mathcal{R}$ is a direct sum of the some of the minimal ideals, i.e., if J is an ideal of $\mathcal{R}$ then there exists a $T(J) \subset \{1, 2, \ldots, t\}$ such that $J = \oplus_{k \in T(J)} \langle \theta_k \rangle$. It is straightforward to show that

$$\mathrm{Ann}(J) = \oplus_{k \notin T(J)} \langle \theta_k \rangle, \quad \mathcal{R}/\mathrm{Ann}(J) \cong \textstyle\prod_{k \in T(J)} \mathbb{F}_{q_k}. \tag{4}$$

If $\mathbb{M}$ is an ideal in $\mathbb{F}_2[G]$ and $J = \Phi(\mathbb{M})$ is the image of $\mathbb{M}$ under (3), then we will use $T(\mathbb{M})$ to denote $T(J)$.

We are now ready to characterize the existence of network coding solutions over Abelian codes $\mathbb{M}$.

Lemma 2. *Let $\mathbb{M}$ be an ideal in the semi-simple commutative group ring $\mathbb{F}_2[G]$. A network has a linear solution over $\mathbb{M}$ if and only if it is scalar linearly solvable over each finite field $\mathbb{F}_{q_k}$, $k \in T(\mathbb{M})$.*

Proof. From Theorem 3, (3) and (4), a network is solvable over the $\mathbb{F}_2[G]$-module $\mathbb{M}$ if and only if the network has a scalar linear solution over $\mathbb{F}_2[G]/\mathrm{Ann}(\mathbb{M}) \cong \mathcal{R}/\Phi(\mathrm{Ann}(\mathbb{M})) \cong \prod_{k \in T(\mathbb{M})} \mathbb{F}_{q_k}$. From Lemma II.12 of [15] we know that a network is scalar linearly solvable over a finite direct product of finite rings if and only if it is scalar linearly solvable over each ring in the product. □

The finite fields in the decomposition (3) can be determined from the *conjugacy classes* of G [25]. We now recall this result from [25]. The conjugacy class C_g containing the group element $g \in G$ is $C_g = \{g, g^2, g^4, \ldots, g^{2^{\ell-1}}\}$ where $\ell = |C_g|$ is the smallest integer such that $g^{2^\ell} = g$, and is known as the *exponent* of C_g. The distinct conjugacy classes of G form a partition of G. The number finite fields t in the decomposition (3) is equal to the number of distinct conjugacy classes of G. Let $g_1, \ldots, g_t \in G$ be such that $C_{g_1}, \ldots, C_{g_t}$ are the distinct conjugacy classes. Then $G = C_{g_1} \cup \cdots \cup C_{g_t}$ and $\mathbb{F}_2[G] \cong \prod_{k=1}^t \mathbb{F}_{q_k}$ where $q_k = 2^{|C_{g_k}|}$ for each $k = 1, \ldots, t$.

C. Circular-Shift Linear Network Codes

Circular-shift network codes correspond to the case where $G = \{e, y, y^2, \ldots, y^{n-1}\}$, $y^n = e$, is a cyclic group. We represent the elements of group algebra $\mathbb{F}_2[G]$ as $\sum_{i=0}^{n-1} m_i y^i$ where $m_i \in \mathbb{F}_2$. Let the distinct conjugacy classes be those generated by the elements $y^{j_1}, \ldots, y^{j_t}$, i.e., $C_{y^{j_1}}, \ldots, C_{y^{j_t}}$ where $j_1, \ldots, j_t \in \{0, 1, \ldots, n-1\}$. Further, let ω be a primitive n^{th} root of unity in a suitable algebraic extension of $\mathbb{F}_2$. The map $\Phi(\sum_{i=0}^{n-1} m_i y^i) = (\hat{m}_1, \ldots, \hat{m}_t)$ where $\hat{m}_k = \sum_{i=0}^{n-1} m_i \omega^{i j_k}$ for $k = 1, \ldots, t$, is an isomorphism (3).

We will use the convention that $j_1 = 0$, i.e., $C_{y^{j_1}} = C_e = \{e\}$. The exponent of this conjugacy class is 1, and thus the first finite field in the decomposition (3) is $\mathbb{F}_{q_1} = \mathbb{F}_2$. The corresponding minimal ideal is $\langle \theta_1 \rangle = \mathbb{F}_2 \times \{0\} \times \cdots \times \{0\}$.

If $\mathbb{M}$ is such that $\Phi(\mathbb{M}) \supset \langle \theta_1 \rangle$ then $1 \in T(\mathbb{M})$. In this case, from Lemma 2, a network has a solution over $\mathbb{M}$ only if it is scalar linearly solvable over $\mathbb{F}_2$. Also, any other finite

field $\mathbb{F}_{q_k}$ in the decomposition (3) is a field extension of $\mathbb{F}_2$, i.e., there exists a ring homomorphism from $\mathbb{F}_2$ to $\mathbb{F}_{q_k}$. Hence, from Theorem 2, if a network is scalar linearly solvable over $\mathbb{F}_2$ then it is scalar linearly solvable over each $\mathbb{F}_{q_k}$, $k \in T(\mathbb{M})$. Using these observations with Lemma 2 we conclude that if $\mathbb{M}$ is such that $1 \in T(\mathbb{M})$ then a network is solvable over $\mathbb{M}$ if and only if it is scalar linearly solvable over $\mathbb{F}_2$.

Now, let $\mathbb{M}$ be such that $1 \notin T(\mathbb{M})$. This implies that for any $\sum_{i=0}^{n-1} m_i y^i \in \mathbb{M}$, the image $\Phi(\sum_{i=0}^{n-1} m_i y^i) = (\hat{m}_1, \hat{m}_2, \ldots, \hat{m}_t)$ satisfies $0 = \hat{m}_1 = \sum_{i=0}^{n-1} m_i$. Hence, every element of $\mathbb{M}$ has even weight. From Corollary 1 we deduce that any network code over $\mathbb{M}$ is of degree $(n-1)/2$. Hence, we have proved

Lemma 3. *Let G be a cyclic group of odd order n, and $\mathbb{M}$ be any ideal of $\mathbb{F}_2[G]$ such that $1 \notin T(\mathbb{M})$. Any network code over $\mathbb{M}$ is a degree $(n-1)/2$ network code.*

Let ℓ_0 be the multiplicative order of 2 modulo n. Then $C_y = \{y, y^2, \ldots, y^{2^{\ell_0-1}}\}$ and $|C_y| = \ell_0$. Assume, without loss of generality, that in the decomposition (3) $q_1 = 2$ and $q_2, \ldots, q_{t_0+1} = 2^{\ell_0}$, i.e., let t_0 denote the number of conjugacy classes with exponent equal to ℓ_0.

Lemma 4. *Let $\varphi(n) = |\{j \mid (j,n) = 1, 1 \le j \le n-1\}|$ be the Euler's totient function. Then $\ell_0 | \varphi(n)$ and $t_0 \ge \varphi(n)/\ell_0$.*

Proof Outline: The proof starts by showing $|C_{y^j}| = |C_y| = \ell_0$ if $(j,n) = 1$. And then we observe that $\{y^j \mid (j,n) = 1\}$ is closed under squaring. These results imply that $\{y^j \mid (j,n) = 1\}$ is a disjoint union of conjugacy classes each of size ℓ_0. The lemma then follows from the fact $|\{y^j \mid (j,n) = 1\}| = \varphi(n)$. See [17, Lemma 5] for full proof. □

Let $\mathbb{M} = \oplus_{k=2}^{t_0+1} \langle \theta_k \rangle$ be the direct sum of ideals corresponding to the t_0 conjugacy classes with exponent equal to ℓ_0. Since $1 \notin T(\mathbb{M})$, from Lemma 3 we deduce that any network code over $\mathbb{M}$ is of degree $(n-1)/2$. To compute the rate, note that $\log_2 |\mathbb{M}| = t_0 \ell_0$. Applying Lemma 4, we have $\log_2 |\mathbb{M}| \ge \varphi(n)$, and hence, the rate of any network code over $\mathbb{M}$ is $t_0 \ell_0 / n$ which is least $\varphi(n)/n$. Finally, we use Lemma 2 to see that a network has a solution over $\mathbb{M}$ if and only if it is scalar linearly solvable over $\mathbb{F}_{2^{\ell_0}}$. Hence, we have proved

Lemma 5. *Let ℓ_0 be the multiplicative order of 2 modulo n, and t_0 the number of ℓ_0-sized conjugacy classes of the cyclic group of order n. If a network has a scalar linear solution over $\mathbb{F}_{2^{\ell_0}}$ then it has a degree $(n-1)/2$ circular-shift network coding solution with rate $t_0 \ell_0 / n \ge \varphi(n)/n$.*

Lemma 5 improves upon the result in [12, Theorem 4], since the former applies to any network and the latter to only multicast networks. Our result also promises higher rate. When $n = 7$, Theorem 4 of [12] (see example in p. 2664) provides a rate $3/7$ network code, whereas Lemma 5 guarantees a rate $6/7$ code.

When n is prime with primitive root 2: In this case 2 is a primitive root modulo n. The cyclic group of order n has exactly two conjugacy classes $C_e = \{e\}$ and $C_y = \{y, y^2, \ldots, y^{n-1}\}$. Hence, $\mathbb{F}_2[G] \cong \mathbb{F}_2 \times \mathbb{F}_{2^{n-1}}$. Let $\mathbb{M}$ be the ideal $\Phi^{-1}(\{0\} \times \mathbb{F}_{2^{n-1}})$. From Lemma 3, a network code over $\mathbb{M}$ is of degree $(n-1)/2$, and its rate is $\log_2 |\mathbb{M}|/n = (n-1)/n$. Finally, from Lemma 2, a network has a solution over $\mathbb{M}$ if and only if it has a scalar linear solution over $\mathbb{F}_{2^{n-1}}$. This result generalizes [11, Theorem 4] from multicast networks to arbitrary networks.

Our next observation provides low-rate degree-1 codes.

Lemma 6. *Let $n = 2^{\ell_0} - 1$ for an integer ℓ_0. If a network has a scalar linear solution over $\mathbb{F}_{2^{\ell_0}}$ then it has a rate ℓ_0/n circular-shift network coding solution of degree 1.*

Proof. The conjugacy class C_y has exponent ℓ_0. Let $\langle \theta_2 \rangle$ be the ideal corresponding to C_y, and let $\mathbb{M}$ be the ideal $\Phi^{-1}(\langle \theta_2 \rangle)$. Then $\mathbb{M}$ is the simplex code of length n and its annihilator is the Hamming code. Clearly the rate of $\mathbb{M}$ is ℓ_0/n and the covering radius of the annihilator is 1. Also, $T(\mathbb{M}) = \{2\}$ and $q_2 = 2^{\ell_0}$. Then the result follows from Lemma 2. □

We end this section with an example of a family of ideals that provide a trade-off between rate and degree.

Example 2. Let $n = 15$. The conjugacy classes of the cyclic group of order 15 are $\{e\}$, $\{y, y^2, y^4, y^8\}$, $\{y^3, y^6, y^{12}, y^9\}$, $\{y^7, y^{14}, y^{13}, y^{11}\}$ and $\{y^5, y^{10}\}$. Let $\langle \theta_1 \rangle, \ldots, \langle \theta_5 \rangle$ be the minimal ideals corresponding to these conjugacy classes, respectively. Consider the below ideals $\mathbb{M}_1, \mathbb{M}_2, \mathbb{M}_3$ that provide decreasing value of degree at the cost of decreasing rates.

(i) $T(\mathbb{M}_1) = \{2, 3, 4\}$, i.e., $\Phi(\mathbb{M}_1) = \langle \theta_2 \rangle + \langle \theta_3 \rangle + \langle \theta_4 \rangle$. This code has rate $12/15$. Its annihilator is equivalent to the direct product of three length-5 repetition codes, and hence, $r_{\mathrm{cov}}(\mathrm{Ann}(\mathbb{M}_1)) = 6$. Thus, $\mathbb{M}_1$ yields degree 6 network codes.

(ii) $T(\mathbb{M}_2) = \{2, 3\}$. The annihilator of $\mathbb{M}_2$ is the $[15, 7]$ double-error correcting BCH code with covering radius 3; see [27, Table 10.1]. Thus, $\mathbb{M}_2$ provides rate $8/15$ network codes of degree 3.

(iii) $T(\mathbb{M}_3) = \{2\}$. The annihilator of $\mathbb{M}_3$ is the $[15, 11]$ Hamming code, which has covering radius 1. Network codes over $\mathbb{M}_3$ have rate $4/15$ and degree 1.

A network has a solution over $\mathbb{M}_1$, $\mathbb{M}_2$, $\mathbb{M}_3$ if and only if it has a scalar linear solution over $\mathbb{F}_{2^4}$. Thus, $\mathbb{M}_1, \mathbb{M}_2, \mathbb{M}_3$ achieve a rate-degree trade-off over the same class of solvable networks. □

IV. Conclusion

We identified an algebraic technique to design permute-and-add network codes by using the network coding framework of Connelly and Zeger and the matrix representation of group algebras. The natural ring theoretic flavour of our approach allowed us to obtain new results (such as Theorem 1, Corollary 1, Lemmas 2 and 6), and also generalize and strengthen some results known in the literature (Corollary 2 and Lemma 5). Our techniques also apply to non-cyclic Abelian groups of permutations, which yield network codes with a wider range of achievable rate and degree compared to circular-shift network codes (see [17, Sec IV-D] for an illustration).

REFERENCES

[1] R. Ahlswede, Ning Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[2] S.-Y. R. Li, R. W. Yeung, and Ning Cai, "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, 2003.

[3] R. Koetter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782–795, 2003.

[4] J. Cannons, R. Dougherty, C. Freiling, and K. Zeger, "Network routing capacity," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 777–788, 2006.

[5] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. M. G. M. Tolhuizen, "Polynomial time algorithms for multicast network code construction," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 1973–1982, 2005.

[6] J. Ebrahimi and C. Fragouli, "Algebraic algorithms for vector network coding," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 996–1007, 2011.

[7] S. Jaggi, Y. Cassuto, and M. Effros, "Low complexity encoding for network codes," in *2006 IEEE International Symposium on Information Theory*, 2006, pp. 40–44.

[8] M. Xiao, M. Medard, and T. Aulin, "A binary coding approach for combination networks and general erasure networks," in *2007 IEEE International Symposium on Information Theory*, 2007, pp. 786–790.

[9] A. Keshavarz-Haddad and M. A. Khojastepour, "Rotate-and-add coding: A novel algebraic network coding scheme," in *2010 IEEE Information Theory Workshop*, 2010, pp. 1–5.

[10] H. Hou, K. W. Shum, M. Chen, and H. Li, "BASIC Codes: Low-complexity regenerating codes for distributed storage systems," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3053–3069, 2016.

[11] H. Tang, Q. T. Sun, Z. Li, X. Yang, and K. Long, "Circular-shift linear network coding," *IEEE Transactions on Information Theory*, vol. 65, no. 1, pp. 65–80, 2019.

[12] Q. T. Sun, H. Tang, Z. Li, X. Yang, and K. Long, "Circular-shift linear network codes with arbitrary odd block lengths," *IEEE Transactions on Communications*, vol. 67, no. 4, pp. 2660–2672, 2019.

[13] H. Tang, Q. T. Sun, X. Yang, and K. Long, "On encoding and decoding of circular-shift linear network codes," *IEEE Communications Letters*, vol. 23, no. 5, pp. 777–780, 2019.

[14] K. W. Shum and H. Hou, "Network coding based on byte-wise circular shift and integer addition," in *2020 IEEE International Symposium on Information Theory (ISIT)*, 2020, pp. 1641–1645.

[15] J. Connelly and K. Zeger, "Linear Network Coding Over Rings Part I: Scalar Codes and Commutative Alphabets," *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 274–291, 2018.

[16] ——, "Linear Network Coding Over Rings Part II: Vector Codes and Non-Commutative Alphabets," *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 292–308, 2018.

[17] L. P. Natarajan and S. K. Joy, "Permute & Add Network Codes via Group Algebras," *arXiv e-prints arXiv:2102.01519*, available at https://arxiv.org/abs/2102.01519.

[18] J.-P. Serre, *Linear representations of finite groups*. Springer, 1977, vol. 42.

[19] N. Jacobson, *Basic Algebra I*. Dover Publications, Incorporated, 2009.

[20] I. N. Herstein, *Noncommutative Rings*. Mathematical Association of America, 1968.

[21] S. Berman, "Semisimple cyclic and Abelian codes. II," *Cybernetics*, vol. 3, no. 3, pp. 17–23, 1967.

[22] F. J. M. Williams, "Binary codes which are ideals in the group algebra of an abelian group," *The Bell System Technical Journal*, vol. 49, no. 6, pp. 987–1011, 1970.

[23] H. Imai, "A theory of two-dimensional cyclic codes," *Information and Control*, vol. 34, no. 1, pp. 1 – 21, 1977.

[24] A. Kelarev and P. Solé, "Error-correcting codes as ideals in group rings," *Contemporary Mathematics*, vol. 273, pp. 11–18, 2001.

[25] B. S. Rajan and M. U. Siddiqi, "Transform domain characterization of abelian codes," *IEEE Transactions on Information Theory*, vol. 38, no. 6, pp. 1817–1821, 1992.

[26] R. E. Blahut, *Algebraic codes for data transmission*. Cambridge University Press, 2003.

[27] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering codes*. Elsevier, 1997.