Properties of Network Polynomials

Javad B. Ebrahimi
EPFL, Lausanne
Email: javad.ebrahimi@epfl.ch

Christina Fragouli
EPFL, Lausanne
Email: christina.fragouli@epfl.ch

***Abstract*—It is well known that transfer polynomials play an important role in the network code design problem. In this paper we provide a graph theoretical description of the terms of such polynomials. We consider acyclic networks with arbitrary number of receivers and min-cut h between each source-receiver pair. We show that the associated polynomial can be described in terms of certain subgraphs of the network.**

I. Introduction

It is well known in the network coding literature that the problem of designing a linear network code that allows to multicast information from a source to a set of receivers over a specific network, can be reduced to the problem of assigning values to variables so that a multivariate polynomial becomes nonzero [2], [4]. Thus, inherently, each linear network coding instance over a network is mapped to a polynomial, which we will call *network polynomial*.

In this paper we try to understand how the structure of these polynomials relates to the underlying network graph. We show that every monomial of the network polynomial is associated with a subgraph of the network with certain properties. For networks with one receiver we show that there is, in fact, a bijection between the monomials of the network polynomial and subgraphs of the network that are minimal with respect to the min-cut property.

For the networks with two receivers, we classify the subgraphs which correspond to the monomials of the network polynomial.

Network polynomials play a significant role in network code design. In the seminal paper [2] it was shown that the existence of a network code over a graph relates to roots of such polynomials. The size of the network coding alphabet used also depends on algebraic properties of such polynomials [5], [6]. These polynomials arise not only in graphs, but also in deterministic networks [1], [3], [5]; In this paper as well, we provide a new method that relates alphabet size and code construction for special classes of networks to polynomial structure and properties. Thus, we believe that studying properties of such polynomials is interesting, not only from a theoretical point of view, but also because of possible applications.

The rest of this paper is organized as follows. Section II reviews the algebraic framework, using a line-graph perspective; Section III looks at transfer polynomials of a single receiver; Section IV looks at multiple receivers; Section V presents a specific application and Section VI concludes the paper.

II. Model and Background

In this section we describe the network model, and briefly review known results from [2], [4] from a line graph perspective; we use similar notation to [4].

a) Setup: We consider a directed acyclic graph $G = (V, E)$, where a source S would like to multicast information to N receivers R_1, …, R_N. We use the terms "graph" and "network" interchangeably. We are interested in scalar linear coding over a finite field $\mathbb{F}_q$, i.e., the source has h symbols $\{u_1, \ldots, u_h\}$ that she would like to send to all receivers, and intermediate network nodes are allowed to linearly combine their incoming symbols using coefficients from the field $\mathbb{F}_q$. The min-cut from the source to each receiver is greater or equal to h, i.e., there exist h edge-disjoint paths from the source to each receiver.

b) Line Graph: Unless otherwise specified, in this paper we will work with the line graph of the original network. Given a graph $G = (V, E)$, the associated line graph is defined as the graph $H = (V_L, E_L)$ whose vertex set V_L is the same as the edge set of the graph G, i.e., $V_L = E$. Two vertices $e, e' \in V_L$ are connected by an arc if and only if the starting point(head) of e' is the same as the ending point(tail) of e in the graph G.

Without loss of generality, we can assume that H has h nodes, known as *source nodes* [4], each of which has a symbol u_i from a finite field $\mathbb{F}_q$ to send to each receiver. Each receiver has also h associated *receiver nodes*, through which it receives information from the network. In the original graph G, the h source nodes in H can be thought of as h auxiliary edges, entering the source node and each bringing one of the symbols u_i; the h receivers nodes in H correspond in G to h incoming edges each receiver has.

Note that in the graph H, for each receiver, there exist h vertex disjoint paths, where each path starts from one source node and ends at one of the receiver nodes; these correspond to the h edge-disjoint paths from the source to the receiver that exist in G. We will come back to these paths in Section IV. Also note that if G is directed and acyclic, so is H [4].

Definition 2.1 (h-minimal subgraph): A subgraph L is called h-minimal with respect to the source S and the receivers R_1, R_2 if the min-cut from S to each of R_1, R_2 is at least h and no proper subgraph of L has this property.
For further notation and terminolofy about graphs, see [7].

c) Transfer and Network Polynomial: In linear network coding over $\mathbb{F}_q$, intermediate nodes in the network G linearly combine their received information using coding coefficient $\{x_k\}$ from the field $\mathbb{F}_q$. These coefficients are the unknown variables in the algebraic formulation of the network code design problem. In the line graph notation, we have one variable x_i associated with each edge of the graph H; thus we have $\nu \triangleq |E_L|$ such variables.

Let $X \in \mathbb{F}_q^h$ be a vector that collects the source symbols $\{u_1, \ldots, u_h\}$, and $Y \in \mathbb{F}_q^h$ a vector that collects the symbols receiver i observes, then $Y = \mathbf{A}(R)X$ where $\mathbf{A}(R)$ is the $h \times h$ transfer matrix from the source to the receiver R [2], [4]. The transfer matrix can be efficiently calculated, and captures the linear transformation that the network operations impose on the send source symbols.

Definition 2.2: The *transfer polynomial* f_i for a receiver R_i is defined as

$$p_i(x_1, \ldots, x_\nu) \triangleq \det(\mathbf{A}(R_i))$$

Definition 2.3: The *network polynomial* associated with a multicast network coding instance is the product of the transfer polynomials of all receivers, i.e.,

$$p(x_1, x_2, \ldots, x_\nu) \triangleq p_1(x_1, \ldots, x_\nu) \cdot \ldots \cdot p_N(x_1, \ldots, x_\nu) \quad (1)$$

d) Network Code Design: In the framework we discuss, the network code design problem asks to find an assignment of values to the unknown variables $\{x_i\}$ so that the network polynomial evaluates to a nonzero value. Indeed, in this case, the transfer polynomial to each receiver evaluates to a nonzero value; the transfer matrix to each receiver is full rank; and thus, each receiver can invert the transfer matrix and decode the source symbols. It is well known (see for example [2]) that such an assignment is always possible provided that the field size is larger than the number of receivers.

III. Transfer Polynomial

We now focus on a single receiver R_i. For simplicity, we will use $\mathbf{A}$ and p (instead of $\mathbf{A}(R_i)$ and p_i) for the transfer matrix and the transfer polynomial, respectively.

We will work with the line graph of the original network; thus, as mentioned in Section II, we assume that we have a set $\mathcal{S} = \{s_1, s_2, \ldots, s_h\}$ of h source nodes with in-degree 0 and a set $\mathcal{R} = \{r_1, r_2, \ldots, r_h\}$ of h receiver nodes. We also assume that there are h vertex disjoint paths from the elements of $\mathcal{S}$ to the elements of $\mathcal{R}$.

A. Monomials and Paths

As we discussed earlier, with every edge $e \in E$ of the line graph we have an associated variable x_e; thus with every path $P = e_{i_1}, e_{i_2}, \ldots, e_{i_k}$ we can associate the monomial

$$f(P) \triangleq x_{e_{i_1}} . x_{e_{i_2}} \cdot \ldots \cdot x_{e_{i_k}}.$$

Let $\mathcal{P}_{(i,j)}$ denote the set of all (s_i, r_j) paths, i.e., all paths that connect source node s_i to receiver node r_j. We then define

$$f_{(i,j)} \triangleq \sum_{P \in \mathcal{P}_{(i,j)}} f(P).$$

It is well known (and straightforward) that the entry (i,j) of the transfer matrix $\mathbf{A}$ is nothing but the polynomial $f_{(i,j)}$.

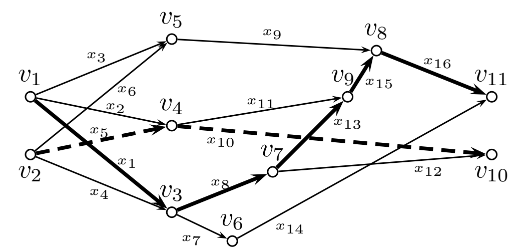

Fig. 1. An example of a network with $h = 2$. A DPQM is depicted with in the figure using bold edges and dashed edges. The term corresponding to this DPQM in the transfer polynomial is $x_1 x_8 x_{13} x_{15} x_{16} x_5 x_{10}$.

B. PQMs and DPQMs

We now define some new notation that will be useful in stating our results. Consider a permutation π of the set $\{1, 2, \ldots, h\}$ and denote $\pi(i)$ the ith element in the particular permutation (recall there are $h!$ possible permutations).

Definition 3.1 (PQM): A *Perfect Quasi-Matching* (PQM) is a set of h paths in which each path starts from a different node s_i and ends at a different node $r_{\pi(i)}$, for some permutation π, so that no two paths have the same starting or ending node. The (sgn) of a PQM is defined as the sign of π.

Definition 3.2 (DPQM): A PQM is called *Disjoint PQM* (DPQM), if the h paths are vertex-disjoint.

A DPQM corresponds to a set of edge-disjoint paths in the original graph.

C. Main Result

Our first result says that, each monomial that will appear in the transfer polynomial corresponds to a DPQM. In particular, each monomial in the transfer polynomial is of the form $f(P_1) \ldots f(P_h)$ where $P_1, \ldots, P_h$ are paths corresponding to a DPQM (i.e., edge-disjoint paths in the original graph). More formally:

Theorem 3.1:

$$p(x_1, \ldots, x_\nu) = \sum_{\pi} \sum_{\substack{P_i \in \mathcal{P}_{(i,\pi(i))} \\ P_i\text{'s form a DPQM}}} (-1)^{\text{sgn}(\pi)} \prod_{i=1}^{h} f(P_i)$$

Thus, one alternative way of finding the transfer polynomial, would be to find all DPQMs in the network, and sum the corresponding terms. Reversely, if we were given the transfer polynomial, simply by counting the monomials it has, we can learn how many DPQM's the network has towards this receiver; and we can identify for example intersection of DPQM's by identifying their common variables. Next we give an example, and in the rest of this section we prove Theorem 3.1.

Example 3.1: The network depicted in Figure 1 is the line graph of a network G with one source and one receiver and min-cut equal to 2. The nodes v_1, v_2 correspond to the receiver node of the graph and the nodes v_{10}, v_{11} are associated with the receiver node of the graph G. Let $x_{i,j}$ be the variable associated with the edge $v_i v_j$. Using the previous theorem, each monomial of the transfer polynomial of the receiver corresponds to a disjoint PQM between v_1, v_2 and v_{10}, v_{11}. Thus, the transfer polynomial is equal to:

$$\begin{aligned} f &= x_3x_9x_{16}x_5x_{10} + x_3x_9x_{16}x_4x_8x_{12} \\ &+ x_2x_{11}x_{15}x_{8,10}x_4x_8x_{12} + x_2x_{10}x_6x_9x_{16} \\ &+ x_2x_{10}x_4x_8x_{13}x_{15}x_{16} + x_2x_{10}x_4x_7x_{14} \\ &+ x_1x_8x_{13}x_{15}x_{16}x_5x_{10} + x_1x_7x_{14}x_5x_{10} \\ &+ x_1x_8x_{12}x_6x_9x_{16} + x_1x_8x_{12}x_5x_{11}x_{15}x_{16} \end{aligned}$$

D. Steps in proving Theorem 3.1

We start from the following lemma, which states that the only terms that can possibly appear as monomials in the transfer polynomial are of the form $f(P_1)\dots f(P_h)$ where $P_1, \dots, P_h$ are paths corresponding to a PQM.

Lemma 3.1:

$$p(x_1, \dots, x_\nu) = \sum_{\pi} \sum_{P_i \in \mathcal{P}_{(i,\pi(i))},\text{ for all } i} (-1)^{\text{sgn}(\pi)} \prod_{i=1}^{h} f(P_i)$$

Proof: The proof is straightforward and follows from expanding the determinant of the transfer matrix $\mathbf{A}(G)$. ■

Next, we need to prove that in fact only the terms corresponding to disjoint paths (that form a DPQM) will appear in the transfer polynomial; all other terms will cancel out. For this proof, we need to introduce first some notation.

Partial Order

Let $\prec_V$ be a partial order on the set of vertices of H such that $v \prec_V v'$ if and only if there exists a directed path from v to v'. This partial order can be extended to a total order on the set V. For simplicity, we use the same notation $\prec_V$ for the total order. Similarly, we can define the total order $\prec_E$ for the set of edges of G.

We can also define a partial order $\prec_P$ on the set of source-receiver paths defined as follows. $P_1 \prec_P P_2$ if $s_1 \prec_V s_2$ in which s_i is the starting point of the path P_i for $i = 1, 2$.

Let P_1, P_2 be two source-receiver paths with different end points. We say that P_1, P_2 are crossing paths if they share a common vertex. If P_1, P_2 are crossing path and v is a common vertex of P_1, P_2, we say $(v, \{P_1, P_2\})$ is a crossing pattern. Suppose that $(v, \{P_1, P_2\})$ is a crossing pattern and assume that $P_i = Q_iQ'_i$ for $i = 1, 2$ in which P_i is an (s_i, r_i) path, Q_i is an (s_i, v) path and Q'_i is an (v, r_i) path. By the dual of $(v, \{P_1, P_2\})$ pattern we refer to the crossing pattern $(v, \{Q_1Q'_2, Q_2Q'_1\})$. It is easy to observe that $Q_1Q'_2$ and $Q_2Q'_1$ are source-receiver paths that intersect at v and also it can be easily checked that the dual of the pattern $(v, \{Q_1Q'_2, Q_2Q'_1\})$ is $(v, \{P_1, P_2\})$. Furthermore, it is easy to see that the dual of each pattern can not be identical as the pattern.

Conclusion of the Proof

From Lemma 3.1, it suffices to show that the terms $(-1)^{\text{sgn}(\pi)} \prod_{i=1}^{h} f(P_i)$ cancel each other when the paths P_i are not pairwise vertex disjoint. We will show that we can pair up all the crossing PQM's into pairs so that both PQM's in a pair use the same set of edges but have opposite sgn's. As a result, their corresponding terms in the expansion of $P(G)$ will cancel each other.

We define the dual of a crossing PQM $\mathcal{P} = \{P_1, P_2, \dots, P_h\}$ as follows. Let $C = \{v_1, v_2, \dots, v_k\} \subset V$ be the set of all the vertices of the network that belong to more than one of the paths $P_i, i = 1, \dots, h$. Let v_1 be the minimum of the elements of C with respect to the order $\prec_V$. Let $P_1, P_2, \dots, P_l, l \geq 2$ be all the elements of $\mathcal{P}$ which pass trough v_1. Also, assume that P_1, P_2 are the smallest elements of $P_1, P_2, \dots, P_l$ with respect to the order $\prec_P$. Clearly $(v_1, \{P_1, P_2\})$ is a crossing pattern. Let $v_1, \{Q_1, A_2\}$ be the dual of this pattern. Now, we define the dual of $\mathcal{P}$ to be the following PQM:

$$\mathcal{P}' = \{Q_1, Q_2, P_3, P_4, \dots, P_h\}.$$

In the figure 2, Let $P_1 = v_1v_4v_{10}$ and $P_2 = v_2v_4v_9v_8v_{11}$. Then $(v_4, \{P_1, p_2\})$ is a crossing pattern.

Notice that:

1- $\mathcal{P}'$ is also a crossing PQM.
2- $\mathcal{P}'$ uses the same edges as of $\mathcal{P}$.
3- $\mathcal{P}' \neq \mathcal{P}$.
4- sgn($\mathcal{P}'$) = $-$ sgn($\mathcal{P}'$).
5- The dual of $\mathcal{P}'$ is $\mathcal{P}$.

The only nontrivial parts of the above is the last two parts. To see the last part, notice that if v_1 is the smallest crossing point of $\mathcal{P}$, it is also the smallest crossing point of $\mathcal{P}'$. Also, since P_1, P_2 are the two smallest elements of $\mathcal{P}$ and Q_1, Q_2 have the same set of the starting points of P_1, P_2, by definition of $\prec_P$, Q_1, Q_2 are the two smallest elements of $\mathcal{P}'$. Finally, since the dual of the dual of a crossing pattern is the original pattern, the dual of $\mathcal{P}'$ is $\mathcal{P}$.

For the part [5], notice that the end points of the paths of $\mathcal{P}'$ are matched the same way as the endpoints of the paths in $\mathcal{P}$ with one exception for the endpoints of the paths P_1, P_2 and Q_1, Q_2 which are matched differently.

IV. Network Polynomial

In the case of a single receiver the terms in the transfer polynomial corresponded to h disjoint paths, i.e., a subgraph of the network with some special properties. Similarly, in the case of N receivers, each term of the network polynomial now also corresponds to a subgraph, that satisfies some special properties.

A. Terms in the network polynomial

For simplicity we describe for the case of two receivers, R_1 and R_2. Consider an acyclic line network with one source set $\mathcal{S} = \{s_1, s_2, \dots, s_h\} \subset V$ and two receiver sets $\mathcal{R}_1 = \{r_1, r_2, \dots, r_h\}$ and $\mathcal{R}_2 = \{r'_1, r'_2, \dots, r'_h\}$. As discussed in Section II, the network polynomial can be calculated as

$$p(x_1, \dots, x_\nu) = \det(A(R_1)A(R_2)) = p_1(x_1, \dots)p_2(x_1, \dots).$$

As we already showed, each monomial of p_1 (and p_2) corresponds to a DPQM with respect to the set $\mathcal{S}$ and the set $\mathcal{R}_1$ ($\mathcal{R}_2$). Therefore, each monomial of p corresponds to a subgraph which is a union of two DPQM's, one with respect to the sets S, R and the other one with respect to the set S, R'. Notice that the converse of this statement is not necessarily true. This is due to the fact that one subgraph of the network can be decomposed as the union of two DPQM's in two different ways and therefore, in the network polynomial some terms might appear several time and they can possibly cancel each other. Thus, it is important to classify those subgraphs of the network that correspond to a monomial in the network polynomial.

We next attempt to extract properties that these subgraphs have; the following lemma summarizes some such easy properties.

Lemma 4.1 (Properties): Consider a subgraph L that corresponds to a term appearing in the network polynomial.

1) The edges of L can be decomposed into two DPQM's; one for each receiver.
2) Each vertex of L has in-degree 0,1 or 2. If it has in-degree 0, then it is a source node. If it has in-degree 1 and the its out-degree is 2, then its incoming edge must appear in both DPQM's.
3) Each vertex of L has out-degree 0,1 or 2. If it has out-degree 0, then it is a receiver node. If it has out-degree 1 and the its in-degree is 2, then its outgoing edge must appear in both DPQM's.
4) The mincut of each receiver on L is at least h.
5) The power of each variable in a monomial indicates whether the corresponding edge (in the original graph) is appears in one of the DPQM's or both.

Proof: Before we prove these properties, notice that each term of the network polynomial is product of two terms of transfer polynomials of the receivers.

1) This property is a direct implication of the previous sentence.
2) Each DPQM is a subgraph of the graph for which the in-degree and out-degree of each vertex is 0 or one. For the union of two DPQM's, the in-degree and out-degree of each vertex is 0,1 or 2. The second part of this property is also clear.
3) Similar to the previous property.
4) This property is a direct consequence of the first property.
5) Trivial.

■

Notice that these properties can be naturally extended for arbitrary number of receivers.

B. The case of two receivers

For the case of two receivers, we have a more concise characterization of these subgraphs.

Theorem 4.1 (Main theorem): In the expansion of the product of the transfer polynomials of the two receivers, each monomial appears either only once or even number of times. In particular, if the field $\mathbb{F}_q$ has characteristic 2, then the subgraphs corresponding the monomials of the network polynomial can be uniquely decomposable into two DPQM's.

Proof: The proof of this theorem is an immediate consequence of Theorem 3.1 ■

In order to prove the next theorem, we will need to define a class of the directed graphs which we call them "2-alternating colorable graphs".

Definition 4.1 (2-alternating colorable graphs): An acyclic directed graph K is called 2-alternating colorable if we can color its edges with two colors blue and red so that the following properties are satisfied.

i) Each vertex of K has in-degree 0,1 or 2. The vertices with in-degree 0 are called "head".
ii) Each vertex of K has out-degree 0,1 or 2. The vertices with out-degree 0 are called "tail". A vertex that is not head or tail is called an intermediate node.
iii) Each vertex of K has in-degree 1 if and only if it has out-degree 1.
iv) Each intermediate vertex has the same number of incoming and outgoing edges of each color.
v) Each head node has one outgoing edges from each color. Each tail node has one incoming edge from each color.

In the next theorem of this section, we will prove that a monomial of the network polynomial corresponds to a subgraph of the network which satisfies the properties in Lemma 4.1 and it does not contain a 2-alternating colorable subgraph.

Theorem 4.2: Suppose that H is an acyclic line-network with the source set $\mathcal{S}$ and the receiver sets $\mathcal{R}_1$, $\mathcal{R}_2$ each of which of min-cut h. Also, assume that the edges of H can be decomposed into two DPQM's, one for each receiver. The following statements are equivalent:

i) There exist at least two different ways for decomposing the edges of H into two DPQM's.
ii) H contains an induced 2-alternating colorable subgraph K such that no intermediate node of K has a neighbor in H other than its neighbors in K.
iii) There are even number of ways that H can be decomposed into two DPQM's.
iv) There is no term in the network polynomial corresponding to the edges of H.

Proof: First of all notice that if the edges of H can be decomposed into two DPQM's then we exactly know which edges will appear in both of DPQM's.

$i \Rightarrow ii$

Suppose that the edges of H can be decomposed into two DPQM's in at least two different ways. So, let us assume that in one way, $\mathcal{P}_1$ is a DPQM to R_1 and $\mathcal{P}_2$ is a DPQM to R_2. Suppose that in the other decomposition of H, $\mathcal{P}'_1$ is a DPQM to R_1 and $\mathcal{P}'_2$ is a DPQM to R_2. As we said before, the set of edges that participate in both $\mathcal{P}_1$ and $\mathcal{P}_2$ is the same set as those edges that are in $\mathcal{P}'_1$ and $\mathcal{P}'_2$. The other edges of H belong to exactly one of $\mathcal{P}_1$ or $\mathcal{P}_2$ and also exactly one of $\mathcal{P}'_1$ or $\mathcal{P}'_2$. Thus, we can partition the edges of H into the following five groups.

1) Edges that are in all the DPQM's $\mathcal{P}_1$,$\mathcal{P}_2$,$\mathcal{P}'_1$ and $\mathcal{P}'_2$.

2) Edges that are only in $\mathcal{P}_1$ and $\mathcal{P}'_1$.
3) Edges that are only in $\mathcal{P}_2$ and $\mathcal{P}'_2$.
4) Edges that are only in $\mathcal{P}_1$ and $\mathcal{P}'_2$. We call these edges, blue edges.
5) Edges that are only in $\mathcal{P}_2$ and $\mathcal{P}'_1$. We call these edges, red edges.

The edges of the first three groups are called neutral edges. Now we show that the red and the blue edges form a 2-alternating colorable subgraph K of H. According to the definition, we must verify 4 conditions. The first two conditions are trivial, based on the fact that K is a subgraph of H and H is the union of two DPQM's and therefore each vertex of H has in(out)-degree 0,1 or 2. To verify the third property, suppose that if a vertex v of K has an incoming edge e. Without loss of generality we may assume that this edge is red. This means that e belongs to $\mathcal{P}_2$ and $\mathcal{P}'_1$. $\mathcal{P}_2$ is a set of h disjoint paths from S to R_2. One of these paths uses the edge e. Lets assume that the next edge of this path is e'. Clearly, e' appears in $\mathcal{P}_2$. So, $e' \in E(H)$. First assume that e' is not a neutral edge. Thus, e' must appear in $\mathcal{P}'_1$ or in $\mathcal{P}'_2$. If e' belongs to $\mathcal{P}_1$, then by definition, e' is also a red edge and the third property of 2-alternating colorable graphs is also satisfied. Otherwise, e' appears in $\mathcal{P}'_2$. That means that e' belongs to one of the source-R_2 paths. Thus, there exists another edge which appears in $\mathcal{P}'_2$ and enters to the vertex v. This edge is different from e since e only appears in $\mathcal{P}_2$ and $\mathcal{P}'_1$. Let us call this edge e''. So, $e'' \in E(H)$ and therefore e'' appears in $\mathcal{P}_1$ or $\mathcal{P}_2$. As we know that e appears in $\mathcal{P}_2$ and $\mathcal{P}_2$ is a DPQM, e'' can not appear in $\mathcal{P}_2$, too. Therefore e'' should appear in $\mathcal{P}_1$. Therefore e'' is a blue edge. We can continue the argument and we similarly deduce that v must have another outgoing blue edge. This shows that either v has one incoming and one outgoing edges of the same color or it has one incoming and one outgoing edges from each of the two colors. Another possibility is that e' is a neutral edge. In this case, e' appears in $\mathcal{P}'_2$. So, there exists an edge f entering to v and belong to $\mathcal{P}'_2$. Obviously, f can not be an edge from $\mathcal{P}_2$ since e enters the same node v and belongs to the DPQM $\mathcal{P}_2$. So, f belongs to $\mathcal{P}_1$ and therefore f is a blue edge. Other possibilities can be similarly analyzed. It only remains to show that no intermediate node of K has a neighbor outside K. This is also easy to see because if v is an intermediate node of K and it has 4 neighbors in K, it can not have more neighbors in H since its total degree can not exceed 4. If v has total degree 2 in K then as we showed, both incoming and outgoing edges of v are of the same color and it is easy to see that in this case, v can not have neutral edges connected to it.

ii $\Rightarrow$ *iii*

Suppose that K is a 2-alternating colorable subgraph of H so that no intermediate node of K has a neighbor in H other than its neighbors in K. The main idea is to show that for every way of decomposing the edges of H into two DPQM's, we can define a dual decomposition and therefore we always have even number of ways of decomposing the edges of H into two DPQM's. We will do this job in two steps. In the first step, we illustrate how we can use a decomposition of H into two DPQM's to find a set of $2h$ paths from the source nodes to the receiver nodes. In the second step, we show that the constructed paths form another decomposition of H into DPQM's.

Step 1: Notice that $\mathcal{P}_1, \mathcal{P}_2$ define a natural 2-alternating coloring of K as follows. We color every edges of K that belongs to $\mathcal{P}_1$ with blue and those edges which belong to $\mathcal{P}_2$ with red. We show that no edge of K can be appeared in both $\mathcal{P}_1, \mathcal{P}_2$. In contrary, suppose that some edge of K belongs to both of DPQM's. Let e be such an edge which is minimal with respect to the order $\prec_E$. Let us assume that the head of the edge e is the vertex v. Since e is used in both DPQM's, v can not have another outgoing edge. By the definition of 2-alternating colorable graphs, v should also have precisely one incoming edge in the graph K. That means that v is not a head of K. Therefore, v as a vertex of H can not have any neighbor outside K. Therefore, v as a vertex of H has precisely one incoming edge. Moreover this edge belongs to K and also this edge must belong to both DPQM's, because of the definition of DPQM's. But this is a contradiction by the minimality of e. Therefore, the 2-coloring of the edges of K is well-defined. It is straightforward to check that this coloring satisfies all the properties of a 2-alternating coloring.

Now, we are ready to introduce the dual decomposition of $\mathcal{P}_1, \mathcal{P}_2$. We start from $\mathcal{P}_1, \mathcal{P}_2$, then we 2-alternating color the edges of K, as explained before. Each of the DPQM's $\mathcal{P}_1, \mathcal{P}_2$ consists of h vertex disjoint paths from the source to each receiver. We alter these paths as follows. We take one of the $2h$ paths, for example a path P_1 from $\mathcal{P}_1$, and we start traversing it until we reach a node of K for the first time. At this point, we are at a head v of K. By definition, v has two outgoing edges. One edge belongs to P_1 and the other belongs to a path P'_1 of $\mathcal{P}_2$. Instead of taking the edge of P_1, we keep traversing the other edge from P'_1 and we keep traversing along P'_1. Finally we arrive to a tail node v' of K. Again, by definition v' has two incoming edges. One from the path P'_1 and another edge from some path in $\mathcal{P}_1$, say path P_i. Then we continue along P_i until we reach a source node. Before we continue the proof, we must mention two points. The first point is that the vertex v' might not be a receiver node of R_2 because any receiver node has one incoming edges while tails of K have two incoming edges. So, every path from the source to the a receiver will be transformed to another path from the source to the same receiver but possibly another node of that receiver. It is also possible that we never touch the subgraph K. In this case the path P_1 remains unchanged. The second point is that if we reach the subgraph K and we exit from it, we will never meet K again. This is due to the fact that the only edges that connect K to H are incoming edges to the heads of K and outgoing edges from the tails of H.

Once we make the first source-receiver path, we start from another source-receiver path of the initial decomposition and we obtain the second source-destination path. We continue this procedure until we find $2h$ new source-receiver paths.

step 2: To complete the proof, we must check the following properties.

1) Each of the $2h$ receiver nodes receives one path from a source node.
2) No two paths to one receiver will cross.
3) The dual of the dual of a decomposition is the original decomposition.
4) No decomposition is its own dual.

The first property is easy to verify. In fact, we initially have $2h$ paths. They transform to another $2h$ paths and since the in-degree of each receiver node is 1, no two new paths enter to the same receiver node. So, they must enter to all the $2h$ paths.

For the second property, suppose that two paths P'_1, P'_2 which enter to two nodes of a receiver intersect at some vertex. Notice that the crossing point of these paths can not be inside K because those vertices of P'_1, P'_2 that belong to K belong to two paths of the DPQM $\mathcal{P}_2$ and those paths never cross. Similarly, P'_1, P'_2 can not cross outside K because outside K, P'_1, P'_2 are parts of paths of the DPQM $\mathcal{P}_1$ and the paths of a DPQM never cross.

The third property is clear when we use the same subnetwork K when want to find the dual of the dual decomposition. Since H might contain several 2-alternating colorable subnetwork for which intermediate nodes of K have no neighbors outside K, we should specify which subgraph we take. Once we fix K, according to the described way of making the dual of a decomposition, it is clear that the dual of a dual decomposition is the original decomposition.

Regarding the last property, notice that K is a non-empty subgraph of H. So, at least one of the $2h$ paths of the $\mathcal{P}_1, \mathcal{P}_2$ should pass through K. Obviously this path will be changed to another path. So, the dual of a decomposition has at least one path that is not in the original decomposition.

Thus, if H can be decomposed into two DPQM's in at least two different ways, then we can pair up the decompositions of H into DPQM's.

iii $\Rightarrow$ *iv*

Since we are working in a characteristic 2 field, the summation of even number of identical terms vanishes.

iv $\Rightarrow$ *i*

Since there is at least one decomposition of the edges of H into DPQM's but in the network polynomial, there is no term corresponding to the edges of H, there should be another decomposition of H into DPQM's to cancel the other one.

■

Theorem 4.3: If H is an h-minimal subgraph of G then the network polynomial has a unique monomial corresponding the edges of H.

Proof: In the network polynomial we set all the variables corresponding to the edges of G that are not in H, zero. The resulting polynomial is the network polynomial of the network H. Since we assume that H is h-minimal, there network coding problem for the network H can be solved. So, the resulting polynomial is non-zero. Thus, there exists at least one monomial whose terms correspond to some edges of H. On the other hand, since H is minimal, there is no monomial of the resulting polynomial whose variables correspond to a proper subset of the edges of H. Therefore, there exists a unique monomial corresponding to the edges of H.

■

Corollary 4.1: An h-minimal subgraph H of G is uniquely decomposable into DPQM's.

Proof: The statement of the corollary is a direct consequence of 4.2 and 4.3. ■

As a direct application of 4.3, we get an alternative proof for the following known result.

Corollary 4.2: The multicast network coding problem with 2 receivers can be solved over the binary field.

Proof: We take a minimal sub-network of the main network that has the same min-cut to each receiver as the original network. We set the variables corresponding the edges of this subnetwork to value 1 and any other variable to the value 0. ■

Example 4.1: Let G be the network in Figure 1. For every receiver, there are exactly two different set of disjoint PQM's. The transfer polynomial of the first receiver is equal to $x_1y_3a_1a_3p_1q_1 - x_3y_1a_1a_3p_1q_1 = a_1a_3p_1q_1(x_1y_3 - x_3y_1)$.

V. A Code-Design Application

In this section we give an example of why studying the structure the transfer and network polynomials can be useful. We look at a special case of network polynomials, that come from combination networks, and using a simple combinatorial argument, we provide an alternative code construction as well as an associated lower bound on the alphabet size[1] this construction uses, that matches the best known such bound.

Combination Network: A combination network with min-cut h is a layered network with 4 layers of nodes. The first layer consists of a single source s. The second layer has $m \geq h$ nodes. We label them as $v_1, v_2, \ldots, v_m$. The source s is connected to all v_i's. The third layer has m nodes $w_1, w_2, \ldots, w_m$. Each v_i is connected to w_i. The last layer consists of N receivers each of which has h in-neighbors from the nodes of the third layer. Without loss of generality we can assume that no two receivers have exactly the same set of in-neighbors. This is due to the fact that if some receivers have the same set of in-neighbors, we can keep one of them and drop the rest. Any network code solution for the resulting network can be naturally extended to a solution for the original network.

Network polynomial of combination network: The line graph of a combination network with $h = 2$ is a 4-layered network. The first layer has two source nodes s_1, s_2. The second layer consists of m nodes $v_1, v_2, \ldots, v_n$. For each $i = 1, 2,\ j = 1, 2, \ldots, n,\ s_i$ is connected to v_j. Let $x_i(y_i)$ be the variable associated with the edge $s_1, v_i(s_2, v_i)$. The third

[1]This translates to a sufficient condition on the field size for which the network coding problem can always be solved.

layer has also n nodes $w_1, w_2, \ldots, w_m$. Each v_i is connected to w_i. Let a_i be the variable associated with that edge. The last layer contains N pairs of receiver nodes. The i-the pair has 2 nodes r_i, t_i. Each pair has two in-neighbors from w_j's where one is connected to r_i and one is connected to t_i. Suppose that r_i is connected to $w_{f(i)}$ and t_i is connected to $w_{g(i)}$ in which f, g are two functions from the set $[N]$ to the set $[m]$, in which $[j] = \{1, 2, \ldots, j\}$. In Figure 2 and Example 4.1, we used p_i and q_i instead of $w_{f(i)}$ and $w_{g(i)}$ for simplicity.

Suppose that the variable associated to the edge $r_i, w_{f(i)}$ is p_i and the one associated to the edge $t_i, w_{g(i)}$ is q_i. As we saw in Example 4.1, the transfer polynomial of each receiver can be computed. Therefore, the network polynomial of G is equal to:

$$p = \prod_{i=1}^{N} a_{f(i)} a_{g(i)} p_i q_i (x_{1,f(i)} x_{2,g(i)} - x_{2,f(i)} x_{1,g(i)}) \qquad (2)$$

Figure 2 shows the line graph of a combination network with $h = 2, m = 4, N = 5$.

Alphabet Size: We use the results of the previous sections to prove the following theorem.

Theorem 5.1: For every combination network with N receivers and min-cut 2 to every receiver, there exists a network code over any field of size larger than $\sqrt{2N}$.

Proof: Let G be a combination network. The network polynomial of G is expressed in 2. We must find an assignment of the values to the variables so that I evaluates to a non-zero value. Set $a_i = p_i = q_1 = x_{1,g(i)} = x_{1,f(i)} = 1, z_i = x_{2,i}$ for all $i = 1, 2, \ldots, m$.

The network polynomial then becomes:

$$I = \prod_{i=1}^{N} (z_{f(i)} - z_{g(i)})$$

Thus, we only need to show that if the field size is larger than $\sqrt{2N}$, we can always assign values to z_i's such that $z_{f(i)} \neq z_{g(i)}$, for $i \in [m]$. Let $\mathbb{F}$ be a finite field of size larger than $\sqrt{2N}$. Each variable z_i appears in certain number of parenthesis. Without loss of generality suppose that z_1 is a variable that appears in the minimum number of parenthesis. Let's assume that z_1 appears in l_1 parenthesis.

We remove all the parenthesis containing z_1 from the product and again without loss of generality, we assume that z_2 is the least appeared variable among the remaining terms. Let's assume that z_2 appears in l_2 of the remaining parenthesis. We exclude all the terms with z_1, z_2 from the product and we repeat the procedure. What we end up is an ordering of the variables and N numbers $l_1, \ldots, l_N$. Let $l_k = \max\{l_1, \ldots, l_N\}$. We show that we can always find an assignment to the variables z_i from any field of size larger than l_k such that I is not zero. We assign values in to the variables based on the ordering we defined above, in the opposite direction. Namely, we first assign arbitrary value to z_N, then we chose an appropriate value for z_{N-1} and at the end we find a right value for z_1. At each step i we must make sure that we select a value for the variable i such that it is

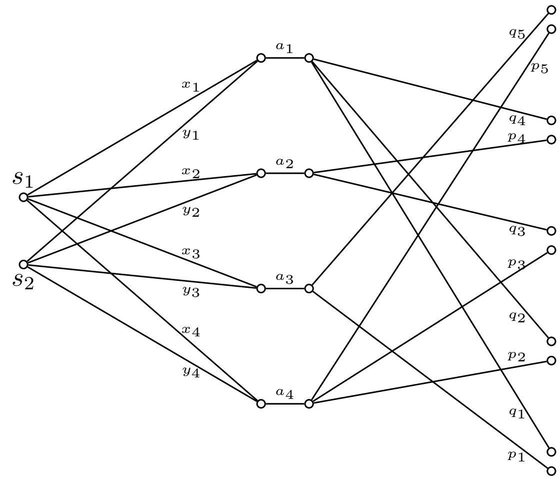

Fig. 2. An example of the line graph of a combination network.

different from the value of every other variable that appears with z_i in some parenthesis. Clearly, if the field size is larger than l_i, we have enough element in the field to select an appropriate value for z_i. Since l_k is the largest l_i, we can find an appropriate value for all the variables. Thus, it is enough to show that $l_k \leq \sqrt{2N}$. We prove this inequality using two inequalities.

i $l_k \leq m - k$
ii $l_k \leq 2N/(m - k)$

The first inequality holds because when we select the k-th variable, there are $m-k$ other variables left. Even if z_k appears with all the left variables, it will be appeared $m-k$ times. The second inequality holds because in the k-th step, each of the $m-k+1$ variables appear at least l_k times in the parenthesis. There are at most N parenthesis and each parenthesis has exactly two elements. Therefore, $l_k(m-k+1) \leq 2N$ and therefrom, we deduce the desired inequality. If we multiply both sides of the two inequalities, we can deduce that $l_k \leq \sqrt{2N}$. ∎

VI. Conclusions

In this paper, we etsablished relationships between the monomials that appear in the transfer and network polynomials to graph theoretical properties of the underlying network configuration. Several questions remain open, with most prominent a more exact characterization of the terms of the network polynomial for an arbitrary number of receivers.

References

[1] S. Avestimehr, S N. Diggavi and D N C. Tse, "A deterministic approach to wireless relay networks", *Proceedings of Allerton Conference on Communication, Control, and Computing*, Illinois, September 2007. See http://licos.epfl.ch/index.php?p=research_projWNC

[2] R. Koetter and M. Médard, "Beyond routing: an algebraic approach to network coding", *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782-796, October 2003.

[3] M. Kim, E. Erez, E. M. Yeh, M. Mdard, "Deterministic Network Model Revisited: An Algebraic Network Coding Approach", CoRRR, 2011.

[4] C. Fragouli and E. Soljanin, "Network coding: Fundamentals," *Foundations and Trends in Networking*, vol. 2, pp. 1–133, 2007.

[5] J. Ebrahimi and C. Fragouli, “Multicasting Algorithms for Deterministic Networks”, ITW, Cairo, January 2010.
[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] D. B. West, “Introduction to Graph Theory”, *Prentice Hall*, 2001.