From Secret Key Agreement to Matroidal Undirected Network

Chung Chan
Institute of Network Coding
The Chinese University of Hong Kong
Email: cchan@inc.cuhk.edu.hk, chungc@alum.mit.edu

***Abstract*—An undirected network link model is formulated, generalizing the usual undirected graphical model. The optimal direction for multicasting can be found in polynomial time with respect to the size of the network, despite the exponential number of possible directions. A more general problem is considered where certain function of a distributed source is to be computed at multiple nodes. The converse results are derived, not from the usual cut-set bound but through the related problem of secret key agreement and secure source coding by public discussion. A unifying model of partly directed network is also formulated, covering both the directed and undirected networks as special cases.**

***Index Terms*—Secret key agreement, undirected network coding, matroid, polymatroid, function computation**

I. Introduction

The problem of undirected network coding was first studied in [2]. The network consists of point-to-point communication links, where information can flow in two different directions, up to a total rate below the capacity of the link. Independent messages are generated at a source node and then multicast to a set of sink nodes. This is done by choosing the directions of the links and performing coding at the source and intermediate nodes. Although the number of possible directions is exponential in the number of undirected links, efficient polynomial-time algorithm exists for computing the optimal direction [3]. Given the optimal direction, the network coding scheme can also be obtained in polynomial time [4]. There is also a symmetry in the undirectedness of the network that allows the same code to be used for different choices of the source from the same multicast group [5].

The purpose of this work is to identify the more general structure that makes this undirected network coding problem polynomially solvable. It is motivated by the previous work in [6], [7], which pointed out a common notion of mutual dependence underlying the undirected network coding problem and the seemingly different problem of secret key agreement [8]. More precisely, the capacities of the two problems are the same and can be computed in polynomial time by exploiting the underlying structure called matroid [9]. This structure also leads to an information-theoretically appealing characterization of the capacity, which can be viewed as a natural generalization of Shannon's mutual information to the multivariate case and the combinatorial notion of partition connectivity [9] originated from the tree packing problem. A similar divergence upper bound on the capacity was first pointed out in [8], and the connection with steiner-tree packing was also observed independently by [2] and [10] for the network coding and secrecy problems respectively. However, the bound is not tight in general as shown by the minimal counter-example in [11] and the connection with steiner-tree packing is not exact. The identity in [7] provides a way to resolve this disparity and better understand the connection between the different problems.

The main result of this work is a generalization of the graphical undirected network model referred to as the matroidal undirected network. It can be viewed as the counterpart of the deterministic network model in [12] since the network may contain undirected broadcast links, interference links, and more general finite linear channels. It is also inspired by the more abstract view of a network as a matroid or linking system in [13], [14], for which the max-flow min-cut theorem takes on a more general form. In addition to studying the problem of multicasting independent messages in the previous work, we will also consider multicasting a distributed source or function of the source just like [15], [16] for the directed network. By relating the problem to the secure source coding problem in [17], [18], polynomial-time solutions or partial solutions can be obtained by exploiting the underlying matroidal structure. The concept can also be extended to a network with its direction partially fixed, with some directed and undirected links. This creates a continuum between the directed and undirected network models.

II. Motivation

The connection from the secret key agreement problem to the undirected network coding problem is motivated by a notion of multivariate correlation that appears to be a natural generalization of Shannon's mutual information. Let us introduce this informally using the secret agreement game [6] played by a group of people. One person is chosen as the wiretapper while others are the users. Each player are given a piece of paper they can write on but they cannot show it to anyone. The users win if they all put down the same thing that is different from what the wiretapper put down. The users are also allowed to discuss in public as long as what they is clearly heard by the wiretapper. Is there a winning strategy for the users? If there is just one user, he can simply put down something random since the wiretapper probably cannot guess

This work was partially supported by a grant from the University Grants Committee of the Hong Kong Special Administrative Region, China (Project No. AoE/E-02/08).

it. This does not work if there are more users because they need to agree on the same thing. If they do not discuss about what they want to write, it is unlikely that they can agree on the same thing. But if they describe too clearly about what they want to write, it is likely that the wiretapper guess it too. Is it useful to discuss at all?

The answer is affirmative if the users observe some correlated private events prior to playing the game. For example, suppose the users all like to play basketball but the wiretapper does not. Then, the users can put down the winning team of an important match as the secret. If any user forgets about the match, other users may remind them by naming a few players in the winning team. Assuming that the wiretapper does not follow any basketball game, he will not be able to guess it. If the secret agreement game is played repeatedly, how many times can the user win? Intuitively, the closer the users are to each other, the more secret they can generate. Can we say in a more concrete mathematical framework that the amount of winning is the correlation among the private observations of the users?

The secret key agreement problem in [8] provides such a framework. It consists of a finite set V of users, a subset A of at least two users are called active. Each user $i \in V$ observes privately a discrete memoryless source Z_i that is correlated according to some joint distribution P_{Z_V} with $\mathsf{Z}_V := (\mathsf{Z}_i : i \in V)$ denoting the entire multiple source. The users can discuss in public noiselessly and with unlimited rate until the active users can agree on some uniformly random key that is kept secret to a wiretapper who listens to the entire public discussion. The maximum secret key rate, called the secrecy capacity, is characterized in [8] by a linear program that is upper bounded by a divergence expression as follows.

$$H(\mathsf{Z}_V) - \min_{z_V} z(V) \leq \min_{\mathcal{P}} \frac{D(P_{\mathsf{Z}_V} \| \prod_{C\in\mathcal{P}} P_{\mathsf{Z}_C})}{|\mathcal{P}| - 1}$$

where $H(\cdot)$ and $D(\cdot\|\cdot)$ denote the entropy and divergence respectively [19]. The L.H.S. is the secrecy capacity with $z_V := (z_i : i \in V)$ being the public discussion rate tuple subject to the linear Slepian-Wolf constraints that

$$z(B) := \sum_{i\in B} z_i \geq H(\mathsf{Z}_B|\mathsf{Z}_{B^c}) \qquad \forall B \subseteq V : B \not\supseteq A$$

The R.H.S. is the divergence upper bound with $\mathcal{P}$ being a partition of V into at least two parts such that each part contains at least an element in A. In the two-user case, the divergence bound is simply the Shannon's mutual information $I(\mathsf{Z}_1 \wedge \mathsf{Z}_2) := D(P_{\mathsf{Z}_1\mathsf{Z}_2} \| P_{\mathsf{Z}_1} P_{\mathsf{Z}_2})$. It is a theoretically-appealing measure of correlation because it is, roughly speaking, a normalized distance between the joint distribution and the set of product distributions obtained from the different ways of breaking the correlation. Indeed, the bound is tight [11] when $A = V$, confirming this notion of multivariate correlation for Z_V. However, when $A \subsetneq V$, we also have a minimal counter-example for which the bound is loose. An interesting question is whether we can modify the bound slightly to make it tight.

The tightness of the divergence bound when $A = V$ was also observed in [10] but in the special source model called the pairwise independent network, where the correlation of the source is captured by a dependency graph $G = (V, E, \theta)$ where V and E are the vertex and edge sets, and $\theta : E \mapsto \binom{V}{2}$ is the edge function. More precisely, the nodes in the graph correspond to the users, and each edge $e \in E$ in the graph corresponds to an independent random bit Y_e observed by the incident nodes in $\theta(e)$. The divergence bound evaluates to

$$\min_{\mathcal{P}} \frac{|\delta_G(\mathcal{P})|}{|\mathcal{P}| - 1}$$

where $\delta_G(\mathcal{P})$ is the set of edges that crosses between two different parts in $\mathcal{P}$. In combinatorics, this quantity is the partition connectivity of G. By Tutte and Nash-Williams theorem [9], it is the amount of (possibly different) spanning trees one can pack (fractionally) in the graph if we regard an edge in the graph as a container for an edge of a spanning tree. The fact that it equals the secrecy capacity when $A = V$ is that each spanning tree corresponds to a way of sharing a secret key bit for all the users [10]. For the general case $A \subsetneq V$, [10] extended this idea to pack steiner trees that span the nodes in A. This approach attains at last half of the secrecy capacity but is not optimal in general. The number of steiner trees can be strictly smaller than the secrecy capacity, for example, in the butterfly network in [3]. It was unclear whether the capacity equals the divergence bound for pairwise independent network. Since a counter-example was not known, the equality was conjectured in [20]. The counter-example in [11] is not a pairwise independent network and so does not apply to this special case. Nevertheless, the conjecture is unlikely because of the following reason. The divergence bound, referred to as the steiner strength, was proven to be NP-complete in [3]. The secrecy capacity, however, can be solved in polynomial time by the ellipsoid method [7] because the separation problem corresponds to submodular function minimizations which are solvable in polynomial time [21]. Equality of the expressions implies that P = NP in complexity theory, which seems unlikely.

Interestingly, the same situation happens in the undirected network coding problem [2]. Consider G as a network where each edge corresponds to an independent undirected link that allows information to flow in both directions up a total amount of one bit. A source node $s \in A$ tries to multicast a message to every users in A, referred to as the multicast group. It was shown that the capacity of the network, like the secrecy capacity for pairwise independent network, is upper bounded by the steiner strength. In the broadcast case when $A = V$, the bound is again tight because the partition connectivity is the number of spanning trees that can be packed in G, and each spanning tree corresponds to a way of routing one bit of information to every node. Similarly, for $A \subsetneq V$, the routing solution corresponds to packing steiner trees, which can attain at least half of the capacity but is suboptimal in general. It is again unlikely that the capcity is equal to the steiner strength because the capacity can be computed in polynomial time but computing the steiner strength is NP-complete [3]. There seems to be a mapping between the results of secret key agreement and undirected network coding. Is it possible that the capacities for the two problems are the same? Can we relate the two problems somehow?

If the answer is affirmative, then there may also be a way to view the secrecy capacity for a more general source model as the capacity of a more general undirected network. This appears to be the case. In [22], [23], the notion of partition connectivity is extended to hypergraphs $H = (V, E, \phi)$, which is a generalization of a graph with edge function $\phi : V \mapsto 2^V \setminus \{\emptyset\}$, i.e. an edge can cover more than two nodes. More precisely, it is shown that a hypergraph can be decomposed (fractionally) into connected sub-hypergraphs up to an amount equal to

$$\min_{\mathcal{P}} \frac{\sum_{e\in E}[d_H(e,\mathcal{P})-1]}{|\mathcal{P}|-1}$$

where $d_H(e, \mathcal{P})$ is the number of parts in $\mathcal{P}$ that overlaps $\phi(e)$. Just like the pairwise independent network, this is a special case of the divergence bound when each edge $e \in E$ corresponds to an independent random bit observed by the incident nodes in $\phi(e)$, and so it is the secrecy capacity when $A = V$. It is also the capacity of the corresponding network coding problem [6] by viewing each edge $e \in E$ as an undirected broadcast link where one of the incident node in $\phi(e)$ can broadcast one bit of information to the remaining incident nodes. Note that the partition connectivity for hypergraphs above looks rather different from the original expression for graphs. A more natural generalization would be to use the original expression with $\delta_H(e)$ defined as the set of hyperedges overlapping at least two parts in $\mathcal{P}$. Unfortunately, this yields a different quantity that is not the solution to the problem of packing connected sub-hypergraphs. The question then is whether this quantity has other meaningful interpretation, perhaps equal to the capacity of a different generalization of the undirected network coding problem. This turns out to be the case. In [6], it was shown to be the secrecy capacity for $A = V$ when each edge $e \in E$ corresponds to a random bit vector $(\mathsf{Y}_i^e : i \in \phi(e))$ with Y_i^e observed by $i \in \phi(e)$. The random vector has its components sum to 0 and all its proper subvectors uniformly random. The capacity was also shown to be that of the undirected network coding problem by viewing each edge e as an undirected interference edge where an incident node $i \in \phi(e)$ can be selected as the receiver to observe the output bit $\mathsf{Y} = \sum_{j\in\phi(e)\setminus\{i\}} \mathsf{X}_j$ with X_j being an input bit from user j. It became evident that the result of [22], [23] can be extended further using a more general source model for the secret key agreement problem, which potentially gives a more general undirected network model. But two questions remain: Are the capacities of the secret key agreement and undirected network coding problem the same even for $A \subsetneq V$? If so, can they be expressed in a form similar to the divergence bound?

In the case of directed network coding, the original graphical network has also be extended to network with broadcast links, interference links, and more general finite linear network [12]. It turns out that a further generalization is possible using the abstract mathematical structure called matroid [14]. A natural idea then is to generalize the undirected network using the structure of a matroid. A matroid (M, ρ) [9] can be defined by a finite ground set M and a rank function $\rho : 2^M \mapsto \mathbb{Z}_+$, which satisfies $\rho(B') \le \rho(B) \le |B|$ for all $B' \subseteq B \subseteq M$, and the submodularity property that

$$\rho(B_1) + \rho(B_2) \ge \rho(B_1 \cap B_2) + \rho(B_1 \cup B_2)$$

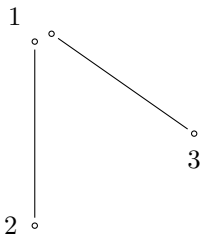
for all $B_1, B_2 \subseteq M$. This property is also satisfied by the entropy function $h(B) := H(\mathsf{Z}_B)$, which can be also be understood as the non-negativity of (conditional) mutual information $I(\mathsf{Z}_{B_1} \wedge \mathsf{Z}_{B_2}|\mathsf{Z}_{B_3}) \ge 0$ for $B_i \subseteq M$ [19]. It is essentially the property used in [11] to prove the tightness of the divergence bound when $A = V$, and so it is not too surprising to see a generalization of the result using this property. In [14], the general directed network model in [12] is identified with the linking system (or bi-matroid) in [13]. The connection between a matroid and a linking system is a notion called the base of a matroid, which is defined as the subset $X \in M$ with full rank $\rho(X) = |X| = \rho(M)$. Suppose $M = X \sqcup Y$ is the disjoint union of X and Y where X is a base of the matroid (M, ρ). Then, (X, Y, λ) defines a linking system where $\lambda : 2^X \times 2^Y \mapsto \mathbb{Z}_+$ is the linking function

$$\lambda(X', Y') = \rho(Y' \cup (X \setminus X')) - |X \setminus X'|$$

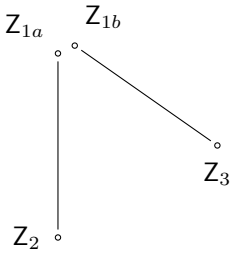
for all $X' \subseteq X$ and $Y' \subseteq Y$. In [14], X is identified as the set of input variables of a directed network and Y the output variables. $\lambda(X', Y')$ generalizes the notion of the maximum information flow from nodes controlling X' to nodes observing Y'. e.g. set $\rho(B) = 1$ for all $\emptyset \ne B \subseteq M$ and $\rho(\emptyset) = 0$. Any element, say $x \in M$, is a base since $\rho(\{x\}) = r(M) = 1 = |x|$. With $X = \{x\}$ and $Y = M \setminus \{x\}$, the linking function is $\lambda(x, Y') = 1$ for every $\emptyset \ne Y' \subseteq Y$. This represents a broadcast channel, where there can be at most one bit of information flow from the input variable to every non-empty subset of the output variables. The insight here is to view a directed network more generally as a matroid with a base of the matroid fixed as the set of input variables.

Naturally then, an undirected network can also be viewed as a matroid but with the freedom of choosing different bases of the matroid as the set of input variables. Each choice of a base corresponds to a different direction of the network. This idea was successfully used in [6] to generalize some results of [23] on the partition connectivity for hypergraphs. This also helped discover a way to turn the secret key agreement problem into the undirected network coding problem, where a solution to the latter also solves the prior. Finally, the matroidal structure was used in [7] to prove that the capacities for the secret key agreement problem and the undirected network coding problem are equal in general for all $A \subseteq V$. There is also an equivalent expression in the form of partition connectivity.

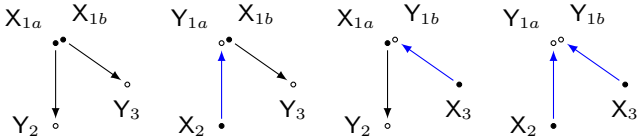
It turns out that the secret key agreement problem can be further generalized to secure source coding in [17], [18], where the goal is to compute a secret source as securely as possible instead of agreeing on a secret key. It is natural to think that the results there can also be translated into solutions of certain undirected network problem. This is the motivation of the current work. In the sequel, we will describe the model more precisely and introduce the problem of multicasting information over a general undirected network. Interested readers can also refer to the paper in [1], which contains the detailed proofs and extensions of the results.



(a) 1-bit undirected links between user 1 and 2, and between 1 and 3.

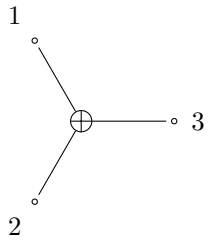


(b) $Z_{1a} = Z_2$, $Z_{1b} = Z_3$ independent and uniformly random.

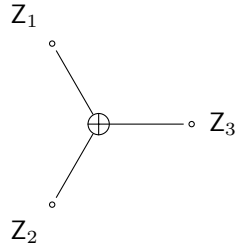


(c) Inputs denoted by X_i's and outputs by Y_i's.

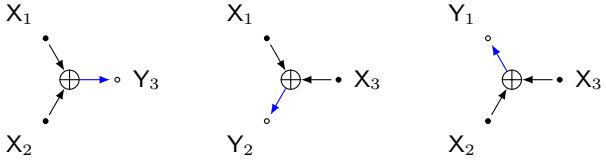
Fig. 1. A graphical undirected network: (a) undirected network; (b) emulated source; (c) possible directions.



(a) 1-bit undirected interference link among user 1, 2 and 3.



(b) $Z_1 \oplus Z_2 \oplus Z_3 = 0$ and (Z_i, Z_j) uniformly random for any $i \neq j$.



(c) $Y_k = X_i \oplus X_j$ with different permutations (i, j, k) of $(1, 2, 3)$.

Fig. 2. A matroid undirected network: (a) undirected network; (b) emulated source; (c) possible directions.

III. System Model

A. Matroidal undirected finite linear network

The key idea is to define an undirected network *not* by the interconnections of a graph but by the more general statistical dependence of a distributed source. To illustrate this, consider the graphical network in Fig. 1(a), which consists of three users and two undirected links. One of the links is between user 1 and 2 and the other is between user 1 and 3. There are altogether $2^2 = 4$ different ways to direct the network as shown in Fig. 1(b). Consider the first direction in Fig. 1(b). If we set the input symbols (X_{1a}, X_{1b}) to the independent and uniformly random variables (Z_{1a}, Z_{1b}), then the statistics of the inputs and outputs are captured by the distributed source shown in Fig. 1(c) with $(Y_2, Y_3) = (Z_2, Z_3)$ as the output symbols. If we instead choose the second direction in Fig. 1(b), but assign the input symbols (X_2, X_{1b}) again to the independent and uniformly random variables (Z_2, Z_{1b}), we have the same source in Fig. 1(c). It is easy to see that the statistics of the channel inputs and outputs are always captured by the same distributed source regardless of the choice of the direction. The source obtained this way by sending independent and uniformly random inputs over the network is called the *emulated source*. Indeed, the emulated source completely characterizes the undirected network in the sense that all the possible directions can be obtained from the source. To do so, we simply need to identify a maximal subset of uniformly random source components, referred to as a *base* of the emulated source. For example, (Z_{1a}, Z_{1b}) is a base and it corresponds to the first directed network in Fig. 1(c) with (X_{1a}, X_{1b}) as the inputs. (Z_2, Z_{1b}), (Z_{1a}, Z_3) and (Z_2, Z_3) are the remaining bases, each of which corresponds to one of the remaining directions of the network. In general, we can use an emulated source to characterize the graphical network model in [2] where undirected links are represented by edges in a multigraph. The emulated source is obtained by choosing independent uniformly random input symbols for the network with an arbitrary direction. The set of possible bases of the emulated source then corresponds to the set of possible ways to direct the network. We call this kind of undirected network *matroidal* because the emulated source form a matroid [9] with the rank function being the entropy function [19] of the source. This is along the same idea as in [13] where a channel viewed more generally as a linking system can be regarded as a matroid with a fixed base being the set of input variables.

Matroidal undirected network is a more general concept than the graphical network. It covers, for example, the network in Fig. 2(a) with an undirected interference edge. There are three possible directions as shown in Fig. 1(c). In the first configuration, user 1 and 2 choose the input bits X_1 and X_2 respectively, while user 3 observes the mod-2 sum $Y_3 = X_1 \oplus X_2$. With X_1 and X_2 chosen uniformly randomly and independently, the channel turns into the emulated source in Fig. 2(b). There are three possible choices of the bases, namely (Z_1, Z_2), (Z_1, Z_3) and (Z_2, Z_3). Each of them corresponds to a different direction in Fig. 2(c). The network is characterized by the emulated source, and so it is matroidal. Similarly, an undirected broadcast link among the three users can be represented by the emulated source $Z_1 = Z_2 = Z_3$ being an uniformly random bit. Any Z_i for $i = 1, 2, 3$ is a base and can therefore be chosen as the input of the link.

We will consider more generally a finite linear undirected network, of which the interference and broadcast links are special cases. Denote the finite field of order q by $\mathbb{F}_q$ and have all logarithms taken with base q for convenience. Let $V := [m] := \{1, \ldots, m\}$ be the finite set of users in the network. User $i \in V$ chooses the channel input $\dot{\mathbf{x}}_i$ as a column vector of elements in $\mathbb{F}_q$. After the entire input vector $\dot{\mathbf{x}}_V := [\dot{\mathbf{x}}_1^\intercal \ \cdots \ \dot{\mathbf{x}}_m^\intercal]^\intercal$ is specified, user $i \in V$ observes the output vector

$$\dot{\mathbf{z}}_i := \boldsymbol{H}_i \dot{\mathbf{x}}_V \qquad i \in V \tag{1}$$

where $\boldsymbol{H}_i$ is a (transfer) matrix with entries in $\mathbb{F}_q$. We will impose the additional requirement that $\dot{\mathbf{x}}_i$ is a subvector of $\dot{\mathbf{z}}_i$,

i.e. $\dot{\mathbf{x}}_i \subseteq \dot{\mathbf{z}}_i$. This does not lose generality as user i observes his channel input $\mathbf{x}_i$ trivially. If the inputs of a finite linear network are generated uniformly randomly and independently, then the channel outputs form a finite linear source. More formally, a source $\mathsf{Z}_V \coloneqq (\mathsf{Z}_i : i \in V)$ is called finite linear if the component source Z_i for user $i \in V$ can be written as a vector $\mathbf{z}_i$ over $\mathbb{F}_q$ satisfying

$$\mathbf{z}_i = \boldsymbol{H}_i \mathbf{x}_V \qquad i \in V \tag{2}$$

for some uniformly random subvector $\mathbf{x}_V$ of $\mathbf{z}_V$, i.e.

$$\mathbf{x}_i \subseteq \mathbf{z}_i \qquad \forall i \in V \tag{3a}$$

$$H(\mathbf{x}_V) = \ell(\mathbf{x}_V) = H(\mathbf{z}_V) \tag{3b}$$

where $\ell(\mathbf{x}_V)$ denotes the length of $\mathbf{x}_V$, and $H(\cdot)$ is the entropy [19] with all logarithms taken base q. $\mathbf{x}_V$ satisfying (3) is a base of Z_V. It is a perfect compression of the source because $\mathbf{x}_V \subseteq \mathbf{z}_V$ and $H(\mathbf{x}_V) = H(\mathbf{z}_V)$ means that there is a bijection between $\mathbf{x}_V$ and $\mathbf{z}_V$, while $H(\mathbf{x}_V) = \ell(\mathbf{x}_V)$ means that $\mathbf{x}_V$ cannot be compressed further. The set of all possible bases of Z_V is denoted as $\mathscr{B}(\mathsf{Z}_V)$. The transfer matrix $\boldsymbol{H}_V \coloneqq [\,\boldsymbol{H}_1^\intercal \ \cdots \ \boldsymbol{H}_m^\intercal\,]^\intercal$ is called a representation of Z_V. Each representation can be viewed as a directed finite linear network and every base satisfying (3) has a corresponding representation. For example, if $\bar{\mathbf{x}}_V$ is another base satisfying (3), then it is a subvector of $\mathbf{z}_V$ by (3a) and so it can be written as $\bar{\mathbf{x}}_V = \boldsymbol{M}\mathbf{z}_V$ for some boolean matrix $\boldsymbol{M}$. Since $\mathbf{z}_V = \boldsymbol{H}_V \mathbf{x}_V$ by (2), we have $\bar{\mathbf{x}}_V = \boldsymbol{M}\boldsymbol{H}_V \mathbf{x}_V$ and so the two bases are related linearly. The matrix $\boldsymbol{M}\boldsymbol{H}_V$ must be invertible since the bases are uniformly distributed and have the same length by (3b). Thus, $\mathbf{x}_V = (\boldsymbol{M}\boldsymbol{H}_V)^{-1}\bar{\mathbf{x}}_V$ and so we can write $\mathbf{z}_i = \boldsymbol{H}_i(\boldsymbol{M}\boldsymbol{H}_V)^{-1}\bar{\mathbf{x}}_V$ for all $i \in V$. $\boldsymbol{H}_V(\boldsymbol{M}\boldsymbol{H}_V)^{-1}$ is therefore the representation of Z_V corresponding to $\bar{\mathbf{x}}_V$. The set of all bases then corresponds to a collection of finite linear networks, which defines the undirected finite linear network.

B. Multicasting over the undirected network

We consider the problem of multicasting correlated sources or some function of the sources like [15], [16] but over a matroidal undirected finite linear network characterized by a finite linear source Z_V as described in §III-A. Let $\mathsf{U}_V \coloneqq (\mathsf{U}_i : i \in V)$ be the discrete memoryless multiple source where the source component U_i is observed privately by user $i \in V$. A subset $A \subseteq V$ of $|A| \geq 1$ user are called the sink nodes or active users. They are required to recover some single-letter function G of the source U_V by a block coding scheme. A positive integer $n \in \mathbb{P}$ is chosen as the block length. U_V and Z_V are extended n times into the i.i.d. sequences $\mathsf{U}_V^n \coloneqq (\mathsf{U}_{Vt} : t \in [n])$ and similarly Z_V^n, with Z_{Vt} represented by the vector $\mathbf{z}_{Vt}$ over $\mathbb{F}_q$. Each user $i \in V$ first observes the entire sequence U_i^n and then transmits over the undirected network as follows.

Encoding At time t from 1 to n, user $i \in V$ specifies the direction $\mathbf{x}_{it} \subseteq \mathbf{z}_{it}$ and the corresponding channel input $\dot{\mathbf{x}}_{it}$ with $\ell(\dot{\mathbf{x}}_{it}) = \ell(\mathbf{x}_{it})$ as a function of his private source U_i^n and his previous channel outputs denoted by $\dot{\mathbf{z}}_{i[t-1]}$. An encoding error occurs if the direction is invalid, i.e. $\mathbf{x}_V \notin \mathscr{B}(\mathsf{Z}_V)$. Otherwise, the channel return to user $i \in V$ his output $\dot{\mathbf{z}}_{it} \coloneqq \boldsymbol{H}_{it}\dot{\mathbf{x}}_{Vt}$ at time t, where $\boldsymbol{H}_{Vt}$ is the representation of Z_{Vt} corresponding to the base $\mathbf{x}_{Vt}$, i.e. $\mathbf{z}_{it} \coloneqq \boldsymbol{H}_{it}\mathbf{x}_{Vt}$ for all $i \in V$.

Decoding After time n, each active user $j \in A$ attempts to recover G^n as a function $\hat{\mathsf{G}}_j$ of his private source U_j^n and his entire channel output sequence $\dot{\mathbf{z}}_{i[n]}$. A decoding error occurs if $\mathsf{G}^n \neq \hat{\mathsf{G}}_j$ for any $j \in A$.

Let ε_n be the probability of encoding or decoding error, i.e.

$$\varepsilon_n \coloneqq \Pr\left\{\exists t \in [n], \mathbf{x}_{Vt} \notin \mathscr{B}(\mathsf{Z}_V) \text{ or } \exists j \in A, \mathsf{G}^n \neq \hat{\mathsf{G}}_j\right\} \tag{4}$$

G^n is said to be transmissible to A if ε_n decays to zero, i.e. $\limsup_{n\to\infty} \varepsilon_n = 0$. We are interested to find a computable necessary condition for transmissibility, and in particular, a sufficient condition for omniscience case where $\mathsf{G} = \mathsf{U}_V$.

Another case of interest is when the users want to send independent messages instead of correlated memoryless sources. Let W_i be the message from user $i \in V$ and $\hat{\mathsf{W}}_j$ of the entire message W_V by user $j \in A$. The encoding and decoding proceed in the same way as before with U_i^n, G^n and $\hat{\mathsf{G}}_j$ replaced by W_i, W_V and $\hat{\mathsf{W}}_j$ respectively. ε_n is also defined as in (4) with the corresponding modifications. Each W_i takes values from a finite set W_i that is growing exponentially in n. The data rate is defined as

$$R_i \coloneqq \limsup_{n\to\infty} \frac{\log|W_i|}{n} \tag{5}$$

The rate tuple $R_V \coloneqq (R_i : i \in V)$ is said to be achievable if $\limsup_{n\to\infty} \varepsilon_n = 0$ assuming the messages are uniformly distributed. The maximum throughput or simply the capacity of the network is defined as the maximum achievable sum rate

$$\sup R(V) = \sup \limsup_{n\to\infty} \sum_{i\in V} \frac{\log|W_i|}{n} \tag{6}$$

where the supremums on the left and right are taken over all achievable rate vectors and block codes respectively.

IV. Main Results

We first derive a necessary condition for transmissibility. Such converse results for network coding are often derived using the cut-set bound. It is rather tricky to apply the same technique here because the directions of the network can vary in time and adapt to the correlated sources. We will obtain the desired condition in a different way through the closely related problem of secure source coding by public discussion [24]. It turns out that if G is transmissible over the network, it is also securely computable by public discussion. Thus, the necessary condition for computing G securely is also a necessary condition for transmitting G.

The secure source coding problem involves a wiretapper in addition to the set of users, a subset of which is also identified as the active users. The users observe some private correlated sources as before. They want to discuss in public until some given function of the source, called the secret source, can be computed by the active users but not the wiretapper. Unlike

the original network coding problem where the communication is over a given undirected network, there is no restriction on the public discussion. The users can broadcast messages about their private sources to all other users noiselessly in multiple rounds and with unlimited rates. The only catch is that the public messages and discussion scheme are also known to the wiretapper. The secret source is said to be securely computable if the error probability in recovering the secret source by the active users and the amount of information of the secret source leaked to the wiretapper can be made to decay to zero. This problem was first proposed in [24] as an extension to the secret key agreement problem in [8]. It was further extended in [18], [25] in the study of imperfect secrecy, the achievable exponents and the admissible choices of key functions.

More precisely, for the secure source coding problem, we set $(\mathsf{U}_V, \mathsf{Z}_V)$ as the multiple source, where U_V is independent of Z_V, and $(\mathsf{U}_i, \mathsf{Z}_i)$ is the component source observed privately by user $i \in V$. G is the secret source to be computed by the active users in A after public discussion. We want to argue that G is securely computable if it is transmissible to A using a block code in §III-B. Consider the following public discussion scheme for block length n. At time t from 1 to n, user $i \in V$ broadcasts the public message

$$\mathbf{f}_{it} := \mathbf{x}_{it} + \dot{\mathbf{x}}_{it} \tag{7}$$

where $\mathbf{x}_{Vt}$ is the base for Z_{Vt} and $\dot{\mathbf{x}}_{it}$ is the corresponding channel input for the solution in the original network coding problem. $\dot{\mathbf{x}}_{it}$ has to be computed from U_i^n and the previous channel outputs $\dot{\mathbf{z}}_{i[t-1]}$. However, there is no undirected channel in the secure source coding problem that can generate the channel outputs. Instead, the user simulates such channel using the public messages by computing

$$\begin{aligned}\boldsymbol{H}_{it}\mathbf{f}_{it} - \mathbf{z}_{it} &= \boldsymbol{H}_{it}(\mathbf{x}_{it} + \dot{\mathbf{x}}_{it}) - \boldsymbol{H}_{it}\mathbf{x}_{it} \\ &= \boldsymbol{H}_{it}\dot{\mathbf{x}}_{it} = \dot{\mathbf{z}}_{it}\end{aligned}$$

where $\boldsymbol{H}_{Vt}$ is the representation of Z_{Vt} corresponding to the base $\mathbf{x}_{Vt}$. After time n, user $j \in A$ can compute the estimate $\hat{\mathsf{G}}_j$ of G^n from U_j^n and $\dot{\mathbf{z}}_{i[n]}$. The overall error probability is ϵ_n, which decays to zero by the assumption that G is transmissible. It remains to argue that the public discussion reveals no information about G^n. From (24), $\mathbf{f}_{V[n]}$ is uniformly distributed because $\mathbf{x}_{V[n]}$ is not only uniformly distributed by (3b) but also independent of $\dot{\mathbf{x}}_{V[n]}$ since $\dot{\mathbf{x}}_{V[n]}$ is a function of U_V^n and the channel output $\dot{\mathbf{z}}_{V[n]}$, which is ultimately a function of U_V^n. Since $\mathbf{f}_{V[n]}$ is uniformly distributed regardless of the realization of U_V^n, we have U_V^n independent of $\mathbf{f}_{V[n]}$. Hence, G is securely computable and so the necessary condition in [24] and [18, Theorem 7] for G to be securely computable is also the necessary condition for G to be transmissible.

Theorem 1 *A function G of U_V is transmissible to $A \subseteq V$: $|A| \geq 1$ over an undirected finite linear network Z_V only if*

$$H(\mathsf{G}) = H(\mathsf{U}_V) + H(\mathsf{Z}_V) - \min_{z_V} z(V) \tag{8}$$

with $z_V := (z_i \in \mathbb{R} : i \in V)$ subject to the linear constraints

$$z(B) \geq H(\mathsf{U}_B|\mathsf{U}_{B^c}) + H(\mathsf{Z}_B|\mathsf{Z}_{B^c}) \quad \forall B \subseteq V : B \not\supseteq A \tag{9a}$$

$$z(B) \geq H(\mathsf{U}_B|\mathsf{U}_{B^c}\mathsf{G}) + H(\mathsf{Z}_B|\mathsf{Z}_{B^c}) \; \forall B \subseteq V : B \supseteq A \tag{9b}$$

where $z(B) := \sum_{i \in B} z_i$ and B^c denotes $V \setminus B$. The optimal z_V can be computed in polynomial time with respect to the size $|V| = m$ of the network, assuming that $H(\mathsf{U}_B)$ and $H(\mathsf{Z}_B)$ can be evaluated in polynomial time for $B \subseteq V$. □

PROOF For the secure source coding problem in [18], the R.H.S. of (8) is a linear program (LP) that characterizes the maximum amount of information about G that can be kept secret from the wiretapper under the requirement that G is recoverable by all active users after public discussion. Intuitively, it should be equal to $H(\mathsf{G})$ for G to be securely computable since no information about G should be leaked to the wiretapper. For the secret key agreement problem in [25], the R.H.S. of (8) is the maximum amount of secret key, called the secrecy capacity, that can be agreed upon by the active users after public discussion, and that is restricted to be a function of G. Once again, it should be equal to $H(\mathsf{G})$ if G is securely computable since all the randomness of G can be used for the secret key. With the previous argument that G being transmissible implies it is securely computable, this is the desired necessary condition.

The polynomial time complexity in computing the optimal z_V is not straightforward because the number of constraints in (9) is exponential in m. The idea is to exploit the underlying matroidal structure by solving the LP using the ellipsoid method [9]. The complexity of the ellipsoid method is equivalent to that of the separation oracle, which determines whether a solution is feasible. From (9), z_V is feasible iff for all $j \in A$

$$0 \leq \min_{B \subseteq V : j \notin B} [z(B) - H(\mathsf{U}_B|\mathsf{U}_{B^c}) - H(\mathsf{Z}_B|\mathsf{Z}_{B^c})] \quad \text{, and}$$

$$0 \leq \min_{B \subseteq V : A \subseteq B} [z(B) - H(\mathsf{U}_B|\mathsf{U}_{B^c}\mathsf{G}) - H(\mathsf{Z}_B|\mathsf{Z}_{B^c})]$$

These are submodular function minimizations over lattice families, and so can be solved in polynomial time [9]. More precisely, the first constraint set $\{B \subseteq V : j \notin B\}$ is a lattice family because, for every B_1 and B_2 in the family, $B_1 \cap B_2$ and $B_1 \cup B_2$ are also in the family. The first objective function $f(B) := z(B) - H(\mathsf{U}_B|\mathsf{U}_{B^c}) - H(\mathsf{Z}_B|\mathsf{Z}_{B^c})$ is submodular because $f(B_1) + f(B_2) \geq f(B_1 \cap B_2) + f(B_1 \cup B_2)$ using the fact that entropy function is submodular [19]. The same argument applies to the last minimization. Since there are only $|A| + 1 \leq m + 1$ submodular function minimizations, the overall complexity is polynomial in m as desired. ■

The necessary condition is not sufficient in general. Some examples are given in [1]. The problem of function computation is difficult even for the directed networks [16]. In the omniscience case $\mathsf{G} = \mathsf{U}_V$, however, closely matching necessary and sufficient conditions have been derived for directed networks using the cut-set bound and random coding scheme [15]. It turns out that the necessary condition above can also be expressed in a similar form of the cut-set bound below, and so a random coding scheme can also give a closely matching sufficient condition for undirected networks.

Theorem 2 *U_V is transmissible to A over a matroidal undirected finite linear network Z_V only if*

$$H(\mathsf{Z}_V) = \min_{z_V} z(V) \tag{10}$$

with z_V subject to the linear constraints

$$z(B) \geq H(\mathsf{U}_B|\mathsf{U}_{B^c}) + H(\mathsf{Z}_B|\mathsf{Z}_{B^c}) \ \forall B \subseteq V : B \not\supseteq A \tag{11a}$$
$$z(B) \geq H(\mathsf{Z}_B|\mathsf{Z}_{B^c}) \qquad \forall B \subseteq V : B \supseteq A \tag{11b}$$

which holds only if (and if)

$$0 = \max_{x_V \in \mathcal{B}} \min_{B \subseteq V : B \not\supseteq A} [H(\mathsf{Z}_{B^c}) - x(B^c) - H(\mathsf{U}_B|\mathsf{U}_{B^c})] \tag{12}$$

with $\mathcal{B}$ being the set of x_V satisfying

$$x(B) \leq H(\mathsf{Z}_B) \quad \forall B \subsetneq V \tag{13a}$$
$$x(V) = H(\mathsf{Z}_V) \tag{13b}$$

$x_V = z_V$ is an optimal solution to (13) if z_V is an optimal solution satisfying (10). □

(12) is in the form of the cut-set bound. To see this, consider some subset $B \subseteq V : B \not\supseteq A$. Since the source U_V needs to be recovered by some users in B^c, namely the active users in $A \setminus B \neq \emptyset$, there must be an information flow of rate at least $H(\mathsf{U}_B|\mathsf{U}_{B^c})$ collectively from B to B^c. Suppose, for simplicity, that $\mathbf{x}_{Vt} \in \mathscr{B}(\mathsf{Z}_V)$ is chosen as the direction for time t prior to observing any channel outputs. Then, using some standard information-theoretic argument, it can be argued that the network supports a flow rate of at most

$$\frac{1}{n} \sum_{t \in [n]} I(\mathbf{x}_{Bt} \wedge \mathsf{Z}_{B^c}|\mathbf{x}_{B^c t}) = H(\mathsf{Z}_{B^c}) - x(B^c) \tag{14}$$

where $I(\cdot)$ denotes Shannon's mutual information [19], $x_i \coloneqq \frac{1}{n}\sum_{t\in[n]} \ell(\mathbf{x}_{it})$, and the last equality is by (3). Furthermore, it can be shown [9] that the set of all possible x_V forms the base $\mathcal{B}$ of a polymatroid. (12) simply asserts that there is a way to direct the network according to some $x_V \in \mathcal{B}$ such that any subset B^c of users containing an active user in A can obtain information at the required rate $H(\mathsf{U}_B|\mathsf{U}_{B^c}) \leq H(\mathsf{Z}_{B^c}) - x(B^c)$. The formal proof of Theorem 2 is given in [1] using the identity in [7]. The following closely matching sufficient condition is also derived using the random coding scheme by adapting the error analysis in [12] to the current undirected network model.

Theorem 3 *U_V is transmissible to A if*

$$0 < \max_{x_V \in \mathcal{B}} \min_{B \subseteq V : \emptyset \neq B \not\supseteq A} [H(\mathsf{Z}_{B^c}) - x(B^c) - H(\mathsf{U}_B|\mathsf{U}_{B^c})] \tag{15}$$

(15) is necessary if $<$ is replaced by $\leq$ as it becomes (12). □

As detailed in [1], the optimal direction of the network can be obtained from the optimal x_V to (15), which again can be computed in polynomial time. In the case of multicasting independent messages, the sufficient and necessary conditions match precisely and give the achievable rate region below.

Theorem 4 *The set of achievable R_V for the undirected network Z_V is the set of non-negative tuples defined by*

$$\mathcal{G} \coloneqq \{x_V - z_V \geq \mathbf{0} : x_V \in \mathcal{B}, z_V \in \mathcal{Q}\} \tag{16}$$

where $\mathcal{B}$ is defined by (13), and $\mathcal{Q}$ is the set of z_V satisfying

$$z(B) \geq H(\mathsf{Z}_B|\mathsf{Z}_{B^c}) \quad \forall B \subseteq V : B \not\supseteq A \tag{17}$$

The capacity or maximum achievable sum rate $R(V)$ is

$$C \coloneqq H(\mathsf{Z}_V) - \min_{z_V \in \mathcal{Q}} z(V) \tag{18}$$

The projection of $\mathcal{G}$ onto the coordinates in A is

$$\{y_A : y_V \in \mathcal{G}\} = \{y_A \geq \mathbf{0} : y(A) \leq C\} \tag{19}$$

which is completely characterized by C. □

The capacity has the alternative form of partition connectivity in [7]. It can again be computed using the ellipsoid method in polynomial time and so as the projection (19) of $\mathcal{G}$ onto A.

V. Partly Directed Network

It is possible to apply the previous results to other undirected network model where the matroidal structure can be identified. Consider, in particular, adding some directed links to a matroidal undirected network. The resulting network is no longer covered by the previous model because its direction is partially fixed. However, the set of possible directions inherits the matroidal structure from the undirected part of the network, and so, by exploiting this structure, the direction of the network can potentially be optimized efficiently as before. In this section, we will define a more general partly directed network model and show how to adapt the previous results to this case by exploiting the matroidal structure.

A matroidal partly directed finite linear network is characterized by a finite linear source Z_V over some finite field $\mathbb{F}_q$ in the same way as the undirected network described in §III. However, the direction $\mathbf{x}_V \in \mathscr{B}(\mathsf{Z}_V)$ of the network consists of two components, i.e. $\mathbf{x}_i = [\mathbf{x}'_i \ \mathbf{x}''_i]^\mathsf{T}$ for $i \in V$, where one of the component $\mathbf{x}'_V$ is fixed while the other $\mathbf{x}''_V$ can be chosen by the system. If $\mathbf{x}'_V$ is empty, then $\mathbf{x}''_V \in \mathscr{B}(\mathsf{Z}_V)$ and so we have the original matroidal undirected network. If $\mathbf{x}''_V$ is empty instead, then $\mathbf{x}'_V \in \mathscr{B}(\mathsf{Z}_V)$ and we have a directed finite linear network. Another special case is the combination of an undirected network Z''_V and a directed network Z'_V with direction $\mathbf{x}'_V \in \mathscr{B}(\mathsf{Z}'_V)$, where Z'_V and Z''_V are independent. The resulting network is characterized by the partial direction $\mathbf{x}'_V$ and the emulated source Z_V with $\mathsf{Z}_i = (\mathsf{Z}'_i, \mathsf{Z}''_i)$ for $i \in V$.

The requirement that $\mathbf{x}_V \in \mathscr{B}(\mathsf{Z}_V)$ limits the possible values of $\mathbf{x}'_V$ and $\mathbf{x}''_V$. Let $\mathscr{P}(\mathsf{Z}_V)$ denote the set of possible partial directions $\mathbf{x}'_V$, and $\mathscr{B}(\mathsf{Z}_V|\mathbf{x}'_V)$ denote the set of possible directions $\mathbf{x}''_V$ that completes $\mathbf{x}'_V$. These two sets can be characterized more explicitly from (3). More precisely, (3a) means that $\mathbf{x}'_i$ and $\mathbf{x}'_i$ are vectors of elements from Z_i, while (3b) means that $H(\mathbf{x}'_V) + H(\mathbf{x}''_V|\mathbf{x}'_V) = \ell(\mathbf{x}'_V) + \ell(\mathbf{x}''_V) = H(\mathsf{Z}_V)$. Thus, the inequalities $H(\mathbf{x}'_V) \leq \ell(\mathbf{x}'_V)$ and $H(\mathbf{x}''_V|\mathbf{x}'_V) \leq \ell(\mathbf{x}''_V)$ must be satisfied with equalities. We also have $\ell(\mathbf{x}''_V) = H(\mathsf{Z}_V) - \ell(\mathbf{x}'_V) = H(\mathsf{Z}_V|\mathbf{x}'_V)$. In summary,

$$\mathbf{x}'_V \in \mathscr{P}(\mathsf{Z}_V) \iff \begin{cases} \mathbf{x}'_i \subseteq \mathbf{z}_i & \forall i \in V \quad (20a) \\ H(\mathbf{x}'_V) = \ell(\mathbf{x}'_V) & (20b) \end{cases}$$

$$\mathsf{x}''_V \in \mathscr{B}(\mathsf{Z}_V|\mathsf{x}'_V) \Longleftrightarrow \begin{cases} \mathsf{x}''_i \subseteq \mathsf{z}_i & \forall i \in V \quad \textbf{(21a)} \\ H(\mathsf{x}''_V) = \ell(\mathsf{x}''_V) = H(\mathsf{z}_V|\mathsf{x}'_V) & \textbf{(21b)} \end{cases}$$

where z_i for $i \in V$ is the vector of all elements in Z_i over $\mathbb{F}_q$.

The block code over a partly undirected network can be defined in the same way as in §III-B. For simplicity, however, we will consider a restricted model where the choice of the direction cannot adapt to the correlated sources nor the channel outputs. In other words, the direction $\mathsf{x}''_{Vt} \in \mathscr{B}(\mathsf{Z}_V|\mathsf{x}'_V)$ for time $t \in [n]$ is chosen before observing the source U_V. This restriction will weaken but also simplify the converse part by ruling out the more complicated adaptation schemes. In particular, we will use the cut-set bound to establish the converse that is analogous to the one established previously through the secrecy problem.

The necessary condition in Theorem 1 directly applies to the partly directed network because G is transmissible over an undirected network if it is transmissible under the restricted model with the direction of the network fixed partly. The condition can be improved, however, since it does not take into account the additional restriction on the choice of direction. Consider some subset $B \subseteq V : B \not\supseteq A$. There is at least one active user in B^c because $B \not\supseteq A$. For this user to recover the function G of the multiple source U_V over a partly directed network Z_V with partial direction $\mathsf{x}'_V \in \mathscr{P}(\mathsf{Z}_V)$, there should be altogether a flow of information at rate at least $H(\mathsf{G}|\mathsf{U}_{B^c})$ from B to B^c. Suppose x_{Vt} is the direction of the network at time $t \in [n]$ with $\mathsf{x}_{it} = [\mathsf{x}'_{it}\ \mathsf{x}''_{it}]^\mathsf{T}$ for all $i \in V$ and some $\mathsf{x}''_{Vt} \in \mathscr{B}(\mathsf{Z}_V|\mathsf{x}'_V)$. As mentioned before, the network supports a flow upper bounded by (14), which can be written as $H(\mathsf{Z}_{B^c}|\mathsf{x}'_V) - x''(B^c)$ where $x''_i := \frac{1}{n}\sum_{t\in[n]} \ell(\mathsf{x}''_{it})$. From (21), it can be shown [9] that the set of possible x''_V forms the base $\mathscr{B}'$ of a polymatroid, namely, the set of x''_V satisfying

$$x''(B) \le H(\mathsf{Z}_B|\mathsf{x}'_V) \quad \forall B \subsetneq V \qquad \textbf{(22a)}$$
$$x''(V) = H(\mathsf{Z}_V|\mathsf{x}'_V) \qquad \textbf{(22b)}$$

Thus, a necessary condition for G to be transmissible to A is

$$0 \le \max_{x''_V \in \mathscr{B}'} \min_{B\subseteq V:\emptyset\neq B\not\supseteq A} [H(\mathsf{Z}_{B^c}|\mathsf{x}'_{B^c}) - x''(B^c) - H(\mathsf{G}|\mathsf{U}_{B^c})] \qquad \textbf{(23)}$$

which simply states that there exists some way to direct the remaining part of the network such that it supports the required flow for G to be transmissible.

It is not clear whether this condition in the form of a cut-set bound can be evaluated efficiently since the minimization is over exponentially many choices of B but the expression to minimize may not be a submodular function of B.[1] We want to weaken the condition slightly so that it becomes easily computable while still taking into account the restriction on the choice of direction. This can be done using the insight from Theorem 2 that equates an easily computable condition to some form of the cut-set bound. Indeed, we will present the result as follows in a form that appears as a generalization of Theorem 2.

Theorem 5 *G is transmissible to A over a partly directed finite linear network Z_V with partial direction $\mathsf{x}'_V \in \mathscr{P}(\mathsf{Z}_V)$ only if (23) holds. With $\tilde{V} := V \cup \{m+1\}$, $\tilde{A} := A \cup \{m+1\}$, $\mathsf{U}_{m+1} := \mathsf{G}$, $\mathsf{Z}_{m+1} := \mathsf{x}'_V$ and $\mathsf{x}'_{m+1} := \emptyset$, define $f : 2^{\tilde{V}} \mapsto \mathbb{R}$ with*

$$f(\tilde{B}) := H(\mathsf{U}_{\tilde{B}}) + H(\mathsf{Z}_{\tilde{B}}) - \ell(\mathsf{x}'_{\tilde{B}}) \qquad \forall \tilde{B} \subseteq \tilde{V} \qquad \textbf{(24)}$$

which is submodular with $f(\emptyset) = 0$. Then, (23) holds only if

$$f(V|\{m+1\}) = \min_{z_V} z(V) \qquad \textbf{(25)}$$

with z_V subject to the linear constraints

$$z(B) \ge f(B) \qquad \forall B \not\supseteq A \qquad \textbf{(26a)}$$
$$z(B) \ge f(B|\{m+1\}) \qquad \forall B \supseteq A \qquad \textbf{(26b)}$$

which holds only if (and if)

$$f(\{m+1\}) = \max_{x_V} \min_{B\subseteq V:B\not\supseteq A} [f(B^c) - x(B^c)] \qquad \textbf{(27)}$$

with $B^c := V \setminus B$ and x_V satisfying

$$x(B) \le f(B|\{m+1\}) \qquad \forall B \subsetneq V \qquad \textbf{(28a)}$$
$$x(V) = f(V|\{m+1\}) \qquad \textbf{(28b)}$$

$x_V = z_V$ is an optimal solution to (28) if z_V is an optimal solution satisfying (25). □

The necessary condition (25) can be computed in polynomial time if $f(B)$ can be. This can be done by the ellipsoid method as described in the proof of Theorem 1 using the submodularity of f. (27) is therefore the desired form of the cut-set bound that is weaker than (23) but can be efficiently computed through (25). Note that if we have $\mathsf{G} = \mathsf{U}_V$ and $\mathsf{x}'_V = \emptyset$, then (25) and (27) above becomes (10) and (12) in Theorem 2 respectively. The equivalence between (25) and (27) can be argued following the proof of Theorem 2 using only the fact that f is submodular with $f(\emptyset) = 0$. See [1] for the complete proof.

The cut-set bounds (23) and (27) become equivalent in the special case when $\mathsf{G} = \mathsf{U}_V$, i.e. the entire correlated sources need to be recovered by every active user. In other words, (23) can be computed efficiently without any weakening. To show the equivalence, note that for all $B \subseteq V$,

$$f(B) = H(\mathsf{U}_B) + H(\mathsf{Z}_B|\mathsf{x}'_B)$$
$$f(B \cup \{m+1\}) = H(\mathsf{U}_V) + H(\mathsf{Z}_B|\mathsf{x}'_V)$$

Substituting this into (27), we have

$$H(\mathsf{U}_V) \le \max_{x_V} \min_{B\subseteq V:\emptyset\neq B\not\supseteq A} [H(\mathsf{U}_{B^c}) + H(\mathsf{Z}_{B^c}|\mathsf{x}'_{B^c}) - x(B^c)]$$

This is equivalent to (23) as desired with $H(\mathsf{G}|\mathsf{U}_{B^c}) = H(\mathsf{U}_V) - H(\mathsf{U}_B^c)$ and $x_V = x''_V$, which is valid because the constraints (22) on $x''_V \in \mathscr{B}'$ are identical to the constraints (28) on x_V with $f(B|\{m+1\}) = H(\mathsf{Z}_B|\mathsf{x}'_V)$. Indeed, not only can (23) efficiently be computed, it is also nearly tight using the same random coding argument as in the proof of Theorem 2, but with the direction specified by $\mathsf{x}_{it} := [\mathsf{x}'_i\ \mathsf{x}''_{it}]$

[1] In particular, $-H(\mathsf{G}|\mathsf{U}_{B^c})$ may not be submodular in B. As a counter-example, consider $\mathsf{G} = \mathsf{U}_1 \oplus \mathsf{U}_2$ with U_1 and U_2 uniform and independent. Then, $-H(\mathsf{G}|\mathsf{U}_1) - H(\mathsf{G}|\mathsf{U}_2) = -2 < -1 = -H(\mathsf{G}|\mathsf{U}_1, \mathsf{U}_2) - H(\mathsf{G})$.

for user $i \in V$ and time $t \in [n]$. In summary, we have the following theorem.

Theorem 6 *U_V is transmissible to A only if*

$$0 \le \max_{x''_V \in \mathcal{B}'} \min_{B \subseteq V : \emptyset \ne B \not\supseteq A} [H(\mathsf{Z}_{B^c}|\mathbf{x}'_{B^c}) - x''(B^c) - H(\mathsf{U}_B|\mathsf{U}_{B^c})] \quad (29)$$

where $\mathcal{B}'$ is defined in (22). If (29) is satisfied with strict inequality, U_V is transmissible. □

Consider now the case when each user $i \in V$ wants to multicast an independent message at rate R_i to the active users in A. Using the same argument as for Theorem 4, the achievable rate region can be obtained by replacing $H(\mathsf{U}_B|\mathsf{U}_{B^c})$ with $R(B)$ in the condition (29) in Theorem 6 for the transmissibility of the correlated sources U_V. i.e. R_V is achievable iff

$$0 \le \max_{x''_V \in \mathcal{B}'} \min_{B \subseteq V : \emptyset \ne B \not\supseteq A} [H(\mathsf{Z}_{B^c}|\mathbf{x}'_{B^c}) - x''(B^c) - R(B)] \quad (30)$$

We can rewrite $H(\mathsf{Z}_{B^c}|\mathbf{x}'_{B^c}) - x''(B^c)$ as $H(\mathsf{Z}_{B^c}) - x(B^c)$ with $x_i := \ell(\mathbf{x}'_i) + x''_i$ for $i \in V$. Then, following the proof of Theorem 4, we can obtain the achievable rate region below.

Theorem 7 *The set of achievable R_V for the partly directed network Z_V with partial direction $\mathbf{x}'_V \in \mathscr{P}(\mathsf{Z}_V)$ is*

$$\mathcal{G}' := \{x_V - z_V \ge \mathbf{0} : x_V = x'_V + x''_V, x''_V \in \mathcal{B}', z_V \in \mathcal{Q}\} \quad (31)$$

where $x'_i := \ell(\mathbf{x}'_i)$ for $i \in V$, and $\mathcal{Q}$ is defined in (17). □

The capacity $C' := \max_{R_V \in \mathcal{G}'} R(V)$ is upper bounded by (18) because of the additional restriction on the choice of direction. It can also be computed in polynomial time by the ellipsoid method because the condition (30) for R_V to be achievable can be. This is because (30) is obtained from (27) with $H(\mathsf{U}_B)$ replaced by $R(B)$, which is obviously polynomially computable, and so is $f(\tilde{B})$.[2]

The earlier result (19) may not extend here, however. i.e. it may not be possible to attain the capacity with just one active user transmitting an independent message. For instance, consider a two-user network with two directed one-bit links pointing in opposite direction between the two users. With all users active, the capacity is 2 bits but each user can transmit at most 1 bit. In other words, the presence of fixed directed links impose additional restriction on the rate allocation, even among the active users.

VI. Conclusion

The undirected network coding problem is related to the secret key agreement problem by the process of source emulation which turns the network into a source. The source characterizes the undirected network because the choice of the bases of the source corresponds to a possible direction of the network. In other words, the interconnections of an undirected network can be described as the correlation of its emulated source. The graphical network can then be generalized by a more general source model the correlation of which may not be captured by a graph, but can be captured by the more general structure of a matroid. We found that the source emulation process can be reversed by public discussion in the sense that the emulated source can be turned into a effective secure channel if we use the base of the source to encrypt secret inputs by the one-time pad. As a consequence, a secrecy problem can be solved as a network coding problem, by supporting a hidden flow of information underneath the public discussion using the correlation among the components of the emulated source. The capacities of the two problems are equal and lead to a common notion of multivariate correlation that appears to be a natural generalization of Shannon's mutual information and the combinatorial notion of partition connectivity. Some more general results in secure source coding are also applicable to the undirected network coding problem. In particular, it leads to a computable sufficient condition for multicasting some single-letter function of a distributed source, with a closely matching sufficient condition or an exact solutions in the omniscience case when the function is the entire source, and when independent messages are multicasted instead of the distributed source. The idea of viewing an undirected network more abstractly as a matroid also leads to a more general network model with the direction partially fixed. The same matroidal structure allows for polynomial time solutions or partial solutions to different multicast problems.

The polynomial time complexity described here relies on the use of ellipsoid method, which translates the linear programming problem of interest to the separating problem that involves submodular function minimizations, which can be solved in polynomial time [21]. This method, however, is not considered practical and therefore only serves as an initial pointer to the search of potentially more practical solutions like the ones given in [3] for the graphical undirected network. The relationship between the secrecy and the undirected network coding problems is also not very symmetrical. Some results in the secure source coding problem do not yet have a counterpart in the undirected network coding problem. Examples are the achievable secrecy exponents in [18], [25], [26]. Although matroidal undirected network is a very general concept, practical coding appears to be possible only in the special case when the network is finite linear. The identity proven in [7] relating the capacities of the secrecy and network coding problems, however, do not rely on such linearity, and is therefore more general. It is not clear whether such generality has further practical significance. Nevertheless, the matroidal framework has given many fruitful research directions. For example, a linear perfect secret key agreement is proposed in [27] using the generalized max-flow min-cut theorem for the linking systems. The block length required to attain the capacity is upper bounded by [28] using again the submodularity of entropy and an integer programming technique called the total dual integrality, which is also well-known in matroid theory. It is optimistic that further discovery of the theory of information for the secrecy problem can enhance our understanding of other related problems.

[2] The other terms in $f(\tilde{B})$ involving $\mathsf{Z}_{\tilde{B}}$ and $\mathbf{x}'_{\tilde{B}}$ corresponds to computing the rank of a submatrix of $\boldsymbol{H}_V$ in (2), which can be done by the Gaussian elimination.

References

[1] C. Chan, publications. http://chungc.net63.net/pub, http://goo.gl/4YZLT.

[2] Z. Li and B. Li, "Network coding in undirected networks," in *Proceedings of 38th Annual Conference on Information Sciences and Systems (CISS)*, 2004.

[3] Z. Li, B. Li, and L. C. Lau, "On achieving maximum multicast throughput in undirected networks," *Information Theory, IEEE Transactions on*, vol. 52, no. 6, pp. 2467 – 2485, jun. 2006.

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

[5] J. Goseling, C. Fragouli, and S. N. Diggavi, "Network coding for undirected information exchange," *IEEE Communications Letters*, vol. 13, no. 1, January 2009.

[6] C. Chan, "Generating secret in a network," Ph.D. dissertation, Massachusetts Institute of Technology, 2010, see [1].

[7] ——, "The hidden flow of information," in *2011 IEEE International Symposium on Information Theory Proceedings (ISIT2011)*, St. Petersburg, Russia, Jul. 2011, see [1].

[8] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Transactions on Information Theory*, vol. 50, no. 12, Dec 2004.

[9] A. Schrijver, *Combinatorial Optimization: Polyhedra and Efficiency*. Springer, 2002.

[10] C. Y. S. Nitinawarat and A. Reznik, "Secret key generation for a pairwise independent network model," in *IEEE International Symposium on Information Theory, 2008. ISIT 2008.*, July 2008, pp. 1015–1019.

[11] C. Chan and L. Zheng, "Mutual dependence for secret key agreement," in *Proceedings of 44th Annual Conference on Information Sciences and Systems*, 2010, see [1].

[12] A. S. Avestimehr, S. N. Diggavi, and D. N. C. Tse, "Wireless network information flow: A deterministic approach," *CoRR*, vol. abs/cs/0906.5394, 2009.

[13] A. Schrijver, "Matroids and linking systems," *Journal of Combinatorial Theory, Series B*, vol. 26, no. 3, pp. 349 – 369, 1979.

[14] M. Goemans, S. Iwata, and R. Zenklusen, "An algorithmic framework for wireless information flow," in *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, 30 2009-oct. 2 2009, pp. 294 –300.

[15] T. S. Han, "Multicasting multiple correlated sources to multiple sinks over a noisy channel network," *Information Theory, IEEE Transactions on*, vol. 57, no. 1, pp. 4 –13, jan. 2011.

[16] R. Appuswamy, M. Franceschetti, N. Karamchandani, and K. Zeger, "Network coding for computing: Cut-set bounds," *IEEE Transactions of Information Theory*, vol. 57, no. 2, pp. 1015–1030, Feb 2011.

[17] H. Tyagi, P. Narayan, and P. Gupta, "When is a function securely computable?" *CoRR*, vol. abs/1007.2945, 2010.

[18] C. Chan, "Multiterminal secure source coding for a common secret source," in *Forty-Ninth Annual Allerton Conference on Communication, Control, and Computing*, Allerton Retreat Center, Monticello, Illinois, sept 2011.

[19] R. W. Yeung, *Information Theory and Network Coding*. Springer, 2008.

[20] C. Ye and A. Reznik, "Group secret key generation algorithms," in *IEEE International Symposium on Information Theory, 2007.*, June 2007, pp. 2596–2600.

[21] M. Grötschel, L. Lovász, and A. Schrijver, "The ellipsoid method and its consequences in combinatorial optimization," *Combinatorica*, vol. 1, pp. 169–197, 1981, 10.1007/BF02579273.

[22] A. Frank, T. Király, and M. Kriesell, "On decomposing a hypergraph into k-connected sub-hypergraphs," *Discrete Applied Mathematics*, vol. 131, no. 2, pp. 373–383, September 2003.

[23] J. Bang-Jensen and S. Thomassé, "Decompositions and orientations of hypergraphs," Preprint no. 10, Department of Mathematics and Computer Science, University of Southern Denmark, May 2001.

[24] H. Tyagi, P. Narayan, and P. Gupta, "Secure computing," in *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, june 2010, pp. 2612 –2616.

[25] C. Chan, "Agreement of a restricted secret key," see [1].

[26] ——, "Universal secure network coding by secret key agreement," see [1].

[27] ——, "Linear perfect secret key agreement," in *2011 IEEE Information Theory Workshop Proceedings (ITW2011)*, Paraty, Brazil, Oct. 2011, see [1].

[28] ——, "Delay of linear perfect secret key agreement," see [1].