AN ALGEBRAIC POLYPHASE APPROACH TO WIRELESS NETWORK CODING*

Ketan Rajawat, Tairan Wang and Georgios B. Giannakis

Dept. of ECE, University of Minnesota, Minneapolis, MN 55455 USA
Emails: {ketan, wang0822, georgios}@umn.edu

ABSTRACT

Network coding has been shown to improve throughput, minimize delay and economize the energy requirements in wireless networks. This paper presents an algebraic polyphase approach to the wireless linear network coding problem. By modeling wireless nodes as consisting of linear periodic time varying filters, the model incorporates realistic constraints including omni directionality of transmissions, half-duplex operation and interference effects. A rank criterion is introduced, which together with the transmission constraints, constitutes the necessary and sufficient conditions for the existence of a wireless network code.

***Index Terms*—** Network coding, linear period time varying (LPTV) filters, wireless networks.

1. INTRODUCTION

Network coding (NC) is a packet-level coding technique that generalizes the classical routing paradigm [1]. Based on linear superposition of incoming packets at nodes, linear NC achieves multicast capacity in single-source wired networks [2]. Recent efforts focus on extending extending NC beyond traditional wired networks to areas such as distributed storage, peer-to-peer file sharing and wireless networks [3].

Wireless NC promises high data rates, robustness to channel fading and efficient energy utilization over conventional routing deployments [4, 5]. However, unlike the relatively simple wired NC designs, the wireless regime is considerably more challenging and fundamentally different. For example, on one hand, wireless antennas are mostly omni directional and thus all nodes are expected to enjoy a broadcast advantage. On the other hand, wireless nodes with single transceivers cannot transmit and receive at the same time (half-duplex constraint); and transmissions from different nodes must be scheduled properly to avoid interference at the destination nodes. Thus, the formulation and results from wired NC do not readily extend to the wireless scenarios. As mentioned in [6], the algebraic formulation of wired NC in [7] is primarily link-based, whereas for wireless NC, a node-based formulation makes more sense.

Most wireless network codes developed so far make use of random NC [8, 9]. While random coding does render the networks robust to link failures, it requires a large alphabet size and tends to waste resources. A deterministic approach to wireless NC adhering to realistic constraints was first proposed in [6].

* Work in this paper was prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U. S. Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative Agreement DAAD19-01-2-0011. The U. S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.

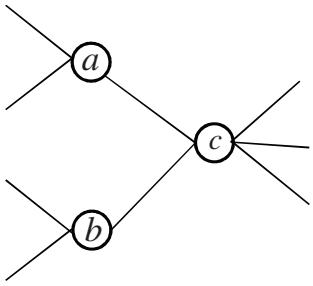

Fig. 1. Part of a network showing nodes a, b and c.

The present paper develops an algebraic formulation of linear wireless NC. The main result asserts that by modeling nodes as consisting of linear periodic time varying (LPTV) filters, it is possible to develop a matrix transfer function that relates source messages to those received at the sinks. This allows one to obtain concrete algebraic conditions for unique decodability of the source messages. Coupled with the wireless constraints mentioned earlier, these constitute the necessary and sufficient conditions on the existence of linear wireless NC. Those in turn guide the design of optimal linear wireless NCs through purely algebraic methods, paralleling those pioneered for error control channel codes.

2. PRELIMINARIES

Consider a wireless communication network represented by a directed graph $\mathcal{G} = (V, E)$, with V denoting the set of nodes and E the set of edges. Because of the broadcast nature of the wireless interface, each node is possibly connected to several other nodes. Thus, the set E consists of tuples (v_1, v_2) denoting the two nodes that the edge connects. Similar to [7], lower case alphabets will denote the nodes and numbers will represent the edges.

In network multicasting, each source $s \in S$ ($S \subset V$) transmits a message comprising a collection of ω_s symbols (or data units) drawn from GF(p^m) for some prime number p and positive integer m. Messages from source s are intended for the sink nodes $T_s \in V \setminus s$, that is the sinks for s can be any nodes in V except s itself. The network operates in a time slotted fashion, where the duration of each slot depends on the medium access control (MAC) protocol. Aiming to model a wireless network in a realistic manner, we adopt the following assumptions:

(A1) *Each node can transmit or receive error free only one symbol per time slot;*

(A2) *Each node adheres to a half-duplex constraint; and*

(A3) *At any node, simultaneous reception from two transmitting nodes is not allowed.*

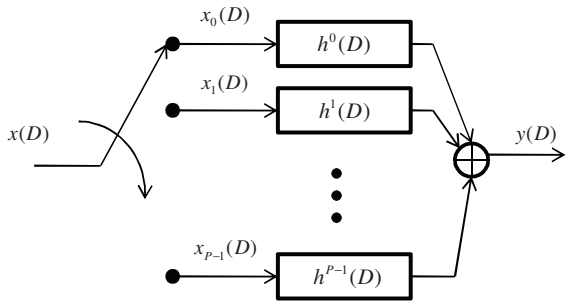

Fig. 2. An LPTV filter as a switched array of LTI filters.

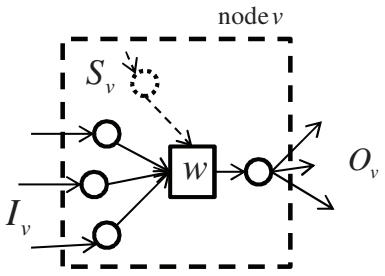

Fig. 3. Model of a single wireless node.

The half-duplex constraint (A2) prevents any node from transmitting and receiving in the same time slot. Any interfering signals present at a node during transmissions are simply ignored. This allows adjacent nodes to transmit simultaneously as long as their intended receivers are distinct so that (A3) is not violated. In addition to (A3), it is assumed that there is no interference between non-connected nodes. This latter assumption will be relaxed to include a more general interference model.

Existing wireless NC apporaches satisfy (A2) and (A3) at the MAC layer while coding is performed at the network layer. In contrast here (A2) and (A3) are included in NC design itself which effects the overall throughput by restricting operation of the nodes to non-conflicting schedules [6].

Under (A2) and (A3), each node will be shown to behave in a periodic manner. In the molecule network depicted in Fig. 1, node c must receive from a and b in two time slots and transmit (broadcast) their linear combination in the next slot. Thus, the period P of node c's transmissions, and hence of the entire network, is at least three. Note that depending on the connectivity, the period of the network could even be larger than the degree of any of the nodes. Further, each node is constrained to operate (transmit, receive or remain idle) at the period of the network.

3. WIRELESS NETWORKS AS LPTV SYSTEMS

Since wireless nodes operate periodically, they can be described as consisting of LPTV filters. Fig. 2 shows a commutator model of a generic LPTV filter. Let the polynomial $x(D) := \sum_n x(n)D^n$ represent the sequence of symbols $x(n)$. An LPTV filter with period P, input $x(D)$ and output $y(D)$ is succinctly described by the following matrix-vector equation [10, Chap. 4]

$$\mathbf{y} = \mathbf{H}\mathbf{x} \tag{1}$$

where the i-th entry of the $P \times 1$ vector $\mathbf{x}$ is given by

$$x_i(D) = D^i \sum x(nP+i)D^{nP}, \quad i = 0, 1, \ldots, P-1 \tag{2}$$

and likewise for $\mathbf{y}$. The polynomial $x_i(D)$ represents the i-th polyphase component of $x(n)$. The input $x(D)$ is deinterleaved into P components (phases), $x_i(D)$, and acted upon by P linear time-invariant (LTI) filters. The transfer matrix of the multi-input multi-output relation (1) is

$$\mathbf{H} = \begin{bmatrix} h_0^0(D) & h_{P-1}^1(D) & \ldots & h_1^{P-1}(D) \\ h_1^0(D) & h_0^1(D) & \ldots & h_2^{P-1}(D) \\ \vdots & & \ddots & \vdots \\ h_{P-1}^0(D) & h_{P-2}^1(D) & \ldots & h_0^{P-1}(D) \end{bmatrix} \tag{3}$$

where $h_j^i(D)$ denotes the j-th polyphase component of the filter $h^i(D)$. Equivalently, the (i,j)-th entry of $\mathbf{H}$ is

$$[\mathbf{H}]_{ij} = h_{(i-j)_P}^j(D) \tag{4}$$

where $(i-j)_P := (i-j) \bmod P$.

In the rest of the section, we will rely on the polyphase description (1) to construct a transfer matrix that relates the source messages and the output at the sink through the linear network coding operations taking place at the nodes. This is the counterpart of the transfer matrix developed in [7] except that here it will be in the polyphase domain to account for the wireless regime. As before, the subscripts will denote the corresponding polyphase components.

3.1. A Single Node

Consider a generic wireless transceiver v modeled as in Fig. 3. The node consists of LPTV filters at the receiving and transmitting ends (denoted by circles) and a buffer represented by a box, that stores the P phases of incoming signals. Let I_v denote the set of potential transmitters to v; and $\mathbf{x}_a$ the polyphase decomposition (polydec) of the message transmitted by a node $a \in I_v$. Depending on whether a effects v at the i-th time slot, the received message $w_{v_a i}(D) = h_{v_a i} x_{ai}(D)$ where $h_{v_a i} \in \{0, 1\}$. Collecting $\{h_{v_a i}\}_{i=0}^{P-1}$ in a diagonal matrix, the received signal can be expressed as $\mathbf{w}_{v_a} = \mathbf{H}_{v_a}\mathbf{x}_a$, where

$$\mathbf{H}_{v_a} = \text{diag}(h_{v_a 0}, h_{v_a 1}, \ldots, h_{v_a P-1}). \tag{5}$$

Let S_v be the set of imaginary sources generating messages s_σ (for all $\sigma \in S_v$) endogenous to node v (denoted by dotted lines in Fig. 3). The received signal $\mathbf{w}_v$ is formed by the superposition of endogenous and exogenous messages

$$\mathbf{w}_v = \sum_{a \in I_v} \mathbf{H}_{v_a}\mathbf{x}_a + \sum_{\sigma \in S_v} \mathbf{H}_{v_\sigma}\mathbf{s}_\sigma \tag{6}$$

where $\mathbf{H}_{v_\sigma}$ corresponds to the source σ. For linear NC, the output signal again consists of a linear combination of the elements of the $\mathbf{w}_v$ vector. If the LTI scaling filter for the i-th phase is $h_v^i(D)$, the polydec representation of the output $\mathbf{x}_v$ can be expressed as

$$\mathbf{x}_v = \mathbf{H}_v\mathbf{w}_v \tag{7}$$

where $\mathbf{H}_v$ is constructed from $h_v^i(D)$ similar to (3). The memory in each node v is assumed limited so that the maximum degree of $h_v^i(D)$ is $P-1$. This also simplifies the system design since $[\mathbf{H}_v]_{ij}$ is a scalar multiple of $D^{(i-j)_P}$. Finally, combining (6) and (7) yields

$$\mathbf{x}_v = \mathbf{H}_v \left(\sum_{a \in I_v} \mathbf{H}_{v_a}\mathbf{x}_a + \sum_{\sigma \in S_v} \mathbf{H}_{v_\sigma}\mathbf{s}_\sigma \right). \tag{8}$$

Equation (8) holds subject to the following constraints: (a) node v can only receive from one node at a time; (b) v cannot transmit and receive at the same time; and (c) adjascent nodes must schedule their transmissions so that they do not interfere at the receiving node. These can be expressed analytically as

$$h_{v_a i} h_{v_b i} = 0 \qquad \forall\, a, b \in I_v \text{ and } a \neq b \tag{9a}$$

$$h^j_{v(i-j)_P}(D) h_{v_a i} = 0 \qquad \forall\, a \in I_v \tag{9b}$$

$$h^j_{a(i-j)_P}(D) h_{v_b i} = 0 \qquad \forall\, a, b \in I_v \text{ and } a \neq b \tag{9c}$$

for each $i, j \in \{0, 1, \ldots, P-1\}$.

Under the wireless-embracing constraints (A1)-(A3), equations (8) and (9a)-(9c) describe the input-output relationship per node.

Remark 1 Interestingly, it is straightforward to incorporate the more realistic double-disk interference model [11] in this formulation. Indeed, if there exists a set of nodes $I(v) \supseteq I_v$, which may possibly interfere with reception at v, it suffices to change $a \in I_v$ in (9c) to $a \in I(v)$.

Remark 2 When v is only a single-source node, (9a)-(9c) are not in effect. Further, one can eliminate $\mathbf{H}_{v_\sigma}$ since its effect can be included in $\mathbf{H}_v$ and the output becomes

$$\mathbf{y}_v = \mathbf{H}_v \mathbf{s}. \tag{10}$$

Similarly, when v is a sink node, it constructs the vector

$$\mathbf{y}_v = \mathbf{H}_v \left(\sum_{a \in I_v} \mathbf{H}_{v_a} \mathbf{x}_a \right). \tag{11}$$

Here the entries of $\mathbf{H}_v$ have no transmit constraints but the entries of $\mathbf{H}_{v_a}$ for $a \in I_v$ are still constrained by (9a). Similar to [7], sink nodes are assumed, without loss of generality, to have no endogenous sources.

3.2. Single-Source Network Coding

Using the per-node LPTV model of the previous subsection it becomes possible to construct a transfer function between the source messages and the output at the sink. Consider a network $\mathcal{G}$ with source s and a given sink t (there may be other sinks but the transfer function for each must be constructed separately). Let $\mathbf{x}$ be the super vector formed by stacking all polydec outputs $\{\mathbf{x}_v, v \in V \setminus s\}$. Also let the polydec of source messages be stacked in the vector $\mathbf{s}$. With these notational conventions, it follows that

$$\mathbf{x} = \mathbf{F}\mathbf{x} + \mathbf{A}\mathbf{s} \tag{12}$$

where $\mathbf{F}$ is the adjacency matrix consisting of $P \times P$ submatrices,

$$\mathbf{F}_{ij} = \begin{cases} \mathbf{H}_i \mathbf{H}_{i_j} & \text{if } j \in I_i \text{ where } i, j \in V \setminus s \\ 0 & \text{otherwise} \end{cases} \tag{13}$$

and $\mathbf{A} = \mathbf{H}_s$. Then at any sink t, the message $\mathbf{s}$ can be recovered from $\mathbf{y} := \mathbf{x}_t = \mathbf{B}\mathbf{x}$, where $\mathbf{y}$ is the polydec of the recovered message and $\mathbf{B}$ is the corresponding extraction matrix. The matrix $\mathbf{F}$ turns out to be nilpotent and $\mathbf{x}$ can be eliminated to yield

$$\mathbf{y} = \mathbf{B}(\mathbf{I} - \mathbf{F})^{-1} \mathbf{A}\mathbf{s}. \tag{14}$$

Given $\mathbf{y}$, successful recovery of the message $\mathbf{s}$ thus depends on the structure of the transfer matrix $\boldsymbol{\mathcal{H}} = \mathbf{B}(\mathbf{I} - \mathbf{F})^{-1}\mathbf{A}$. In this model, $\mathbf{s}$ is assumed to be a continuous stream of messages at the sources. However, not all polyphase components of $\mathbf{s}$ are actually injected into the network because there are time slots during which the source is actually silent (thus allowing adjacent nodes to transmit). Thus, if the source transmits for ω_s time slots per period (and remains silent for the rest of the slots), the $P \times P$ system of equations (14) simplifies to the $P \times \omega_s$ system

$$\mathbf{y} = \boldsymbol{\mathcal{H}}_m \mathbf{s}_m \tag{15}$$

where the $\mathbf{s}_m$ stands for the source message part and $\boldsymbol{\mathcal{H}}_m$ is constructed by removing from $\boldsymbol{\mathcal{H}}$ the columns corresponding to zero entries in $\mathbf{s}$. Obviously, the ω_s polyphases are recoverable if and only if $\boldsymbol{\mathcal{H}}_m$ is full rank. We have thus established that:

Proposition 1 *Constraints* (9a)-(9c) *and full rank of* $\boldsymbol{\mathcal{H}}_m$ *are the necessary and sufficient conditions for the unique decodability of a source message in a single-source wireless network code.*

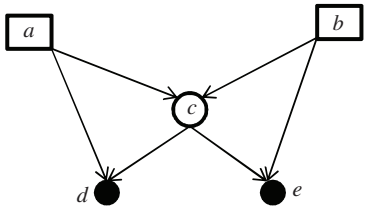

Fig. 4. A simple butterfly network with sources a and b and sinks d and e.

3.3. Multi-Source Network Coding

The multi-source LPTV setup is a simple extension of the single-source formulation. In fact, for each sink, we still have the transfer equation in (14) except that $\mathbf{s}$ is formed by stacking the polydec of different source messages. However messages from only a subset of source may be required at a given sink. Since the sink has no means of distinguishing the required messages from interference, one must ensure that the corresponding entries of $\boldsymbol{\mathcal{H}}$ are zero [7].

If $\mathbf{s}_M$ ($\mathbf{s}_I$) denotes the message (interference) part of $\mathbf{s}$ at a sink t, the input-output relationship at t can be written as

$$\mathbf{y} = \begin{bmatrix} \boldsymbol{\mathcal{H}}_1 & \boldsymbol{\mathcal{H}}_2 \end{bmatrix} \begin{bmatrix} \mathbf{s}_M \\ \mathbf{s}_I \end{bmatrix}. \tag{16}$$

where $\mathbf{s}_M$ has size $\omega_{st} \times 1$. As before, $\boldsymbol{\mathcal{H}}_{1m}$ and $\boldsymbol{\mathcal{H}}_{2m}$ are constructed by removing the columns corresponding to the zero entries of $\mathbf{s}_M$ and $\mathbf{s}_I$, respectively. The conditions for zero interference and recoverability of $\mathbf{s}_M$ become

$$\text{rank}(\boldsymbol{\mathcal{H}}_{1m}) = \omega_{st} \tag{17a}$$

and

$$\boldsymbol{\mathcal{H}}_{2m} = \mathbf{0} \tag{17b}$$

respectively, for some values $h_{ik} \in GF(p^m)$. Hence,

Proposition 2 *Constraints* (9a)-(9c) *and* (17a)-(17b) *constitute the necessary and sufficient conditions for the unique decodability of source messages in a a multi-source wireless network code.*

4. AN EXAMPLE

We now consider an example to illustrate the formulation. Consider the simple butterfly network with two source nodes depicted in Fig. 4. Source nodes a and b are connected to one imaginary source

stream each, while the sinks d and e require messages from both sources.

The period of the network is at least three since the node c takes at least two time slots to receive from nodes a and b, and another time slot to transmit (in general $P \geq \max_{v \in V \setminus S} I_v + 1$). Selecting $P = 3$, we wish to check if a solution exists. The signals transmitted by nodes a, b and c are, respectively

$$\begin{aligned}\mathbf{x}_a &= \mathbf{H}_a \mathbf{s}_a \\ \mathbf{x}_b &= \mathbf{H}_b \mathbf{s}_b \\ \mathbf{x}_c &= \mathbf{H}_c (\mathbf{H}_{c_a} \mathbf{x}_a + \mathbf{H}_{c_b} \mathbf{x}_b)\end{aligned}$$

where $\mathbf{H}_a$, $\mathbf{H}_b$ and $\mathbf{H}_c$ are constructed from the LTI filters $h_a^i(D)$, $h_b^i(D)$ and $h_c^i(D)$ for $i = 0, 1$ and 2; while $\mathbf{H}_{c_a} := \text{diag}\,(h_{c_a 0}, h_{c_a 1}, h_{c_a 2})$ and $\mathbf{H}_{c_b} := \text{diag}(h_{c_b 0}, h_{c_b 1}, h_{c_b 2})$. Sinks d and e output,

$$\mathbf{x}_d = \mathbf{H}_d \left(\mathbf{H}_{d_a} \mathbf{x}_a + \mathbf{H}_{d_c} \mathbf{x}_c\right) \tag{18}$$

$$\mathbf{x}_e = \mathbf{H}_e \left(\mathbf{H}_{d_b} \mathbf{x}_a + \mathbf{H}_{d_c} \mathbf{x}_c\right) \tag{19}$$

where the transfer matrices are constructed as before. We can now construct the system transfer function for node d as

$$\boldsymbol{\mathcal{H}} = \mathbf{H}_d \left[\left(\mathbf{H}_{d_a} + \mathbf{H}_{d_c} \mathbf{H}_c \mathbf{H}_{c_a}\right) \mathbf{H}_a \quad \mathbf{H}_{d_c} \mathbf{H}_c \mathbf{H}_{c_b} \mathbf{H}_b\right]. \tag{20}$$

Constraints (9a)-(9c) specialize to

$$\begin{aligned} h_{c_a i} h_{c_b i} &= 0 \qquad h_{e_b i} h_{e_c i} = 0 \qquad h_{d_a i} h_{d_c i} = 0 \\ h^j_{a(i-j)_2} h_{c_b i} &= 0 \quad h^j_{b(i-j)_2} h_{c_a i} = 0 \quad h^j_{c(i-j)_2} h_{c_b i} = 0 \\ h^j_{c(i-j)_2} h_{d_a i} &= 0 \quad h^j_{a(i-j)_2} h_{d_c i} = 0 \quad h^j_{c(i-j)_2} h_{c_a i} = 0 \\ h^j_{b(i-j)_2} h_{e_c i} &= 0 \quad h^j_{c(i-j)_2} h_{e_b i} = 0 \qquad \forall\, i, j = 0, 1, 2 \end{aligned} \tag{21}$$

where terms such as $h^j_{v(i-j)_2}$ are scalar multiples of $D^{(i-j)_2}$.

The first step towards finding a network code is to obtain a feasible set of variables that satisfy all the constraints. Since each constraint involves two variables each and is homogeneous, it can be readily converted into a single Boolean equation. This is accomplished by replacing each variable x by its indicator variable $\mathbb{1}(x)$, which is non zero if and only if x is non zero. Taking the Boolean OR of all the resulting monomials and equating to zero yields a Boolean equation which can be solved using standard methods; see e.g., [12] and references therein.

Next, for each solution found, variable x becomes zero whenever $\mathbb{1}(x) = 0$, but remains indeterminate otherwise. Since terms such as $h_{c_a i} \in \{0, 1\}$, they can be directly replaced by the corresponding value of their indicator functions. Finally, substitution into the transfer function $\boldsymbol{\mathcal{H}}$ results in a set of polynomial equations that can be solved using standard methods from algebraic geometry. Thus, one possible solution of (21) yields

$$\begin{aligned}[\mathbf{H}_a]_{00} = [\mathbf{H}_{c_a}]_{00} = [\mathbf{H}_{d_a}]_{00} &= 1 \\ [\mathbf{H}_b]_{11} = [\mathbf{H}_{c_b}]_{11} = [\mathbf{H}_{e_b}]_{11} &= 1 \\ [\mathbf{H}_{d_c}]_{22} = [\mathbf{H}_{e_c}]_{22} &= 1 \\ [\mathbf{H}_c]_{20} = D^2 \text{ and } [\mathbf{H}_c]_{21} &= D\end{aligned}$$

with all other entries being zero. The resultant network transfer matrix is

$$\boldsymbol{\mathcal{H}} = \mathbf{H}_d \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ D^2 & 0 & 0 & 0 & D & 0 \end{bmatrix}. \tag{22}$$

It is now possible to choose $\mathbf{H}_d$ such that each of the polyphase components of $\mathbf{y}$ becomes a separate message vector; e.g.,

$$\mathbf{H}_d = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ D^2 & 0 & 1 \end{bmatrix} \tag{23}$$

yields

$$\boldsymbol{\mathcal{H}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & D & 0 \end{bmatrix}. \tag{24}$$

The components of the sink vector become

$$\mathbf{y}_d = \begin{bmatrix} s_{a0}(D) \\ 0 \\ D s_{b1}(D) \end{bmatrix} \tag{25}$$

where as usual $s_{ai}(D)$ denotes the i-th polyphase component of the source vector from node a. Construction of $\mathbf{H}_e$ for sink e can also be performed similarly. In general, we might need to eliminate some columns of $\boldsymbol{\mathcal{H}}$ to obtain $\boldsymbol{\mathcal{H}}_m$, and then express the rank conditions as a set of polynomial equations [13]. Any solution to this set of equations is then a valid network coding solution.

5. REFERENCES

[1] R. W. Yeung and N. Cai, *Network Coding Theory*. Now Publishers Inc, 2006.

[2] S.-Y. Li, R. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, 2003.

[3] P. Chou and Y. Wu, "Network coding for the Internet and wireless networks," *IEEE Signal Process. Mag.*, vol. 24, no. 5, pp. 77–85, 2007.

[4] S. Deb, M. Effros, T. Ho, D. R. Karger, R. Kötter, D. S. Lun, M. Médard, and N. Ratnakar, "Network coding for wireless applications: A brief tutorial," in *Proc. of Intl. Workshop on Wireless Ad-hoc Networks*, London, UK, May 2005.

[5] Y. Wu, P. Chou, and S.-Y. Kung, "Minimum-energy multicast in mobile ad hoc networks using network coding," *IEEE Trans. Commun.*, vol. 53, no. 11, pp. 1906–1918, Nov. 2005.

[6] Y. Sagduyu and A. Ephremides, "On joint MAC and network coding in wireless ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3697–3713, 2007.

[7] R. Kötter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, pp. 782–795, 2003.

[8] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft, "XORs in the air: Practical wireless network coding," *IEEE/ACM Trans. Netw.*, vol. 16, pp. 497–510, 2008.

[9] D. Lun, M. Médard, and R. Kötter, "Efficient operation of wireless packet networks using network coding," in *Proc. of Intl. Workshop on Convergent Technologies*, Oulu, Finland, June 2005.

[10] P. P. Vaidyanathan, *Multirate Systems and Filter Banks*. Upper Saddle River, NJ, USA: Prentice-Hall Inc., 1993.

[11] M. Cheng, S. Huang, X. Huang, and W. Wu, "New graph model for channel assignment in ad hoc wireless networks," *IEE Proc.-Commun.*, vol. 152, pp. 1039–1046, Dec. 2005.

[12] M. Keinanen, "Techniques for solving Boolean equation systems," Ph.D. dissertation, Helsinki University of Technology, 2006. [Online]. Available: http://lib.tkk.fi/Diss/2006/isbn9512285460/isbn9512285460.pdf

[13] R. Cramer, E. Kiltz, and C. Padró, "A note on secure computation of the moore-penrose pseudo-inverse and its application to secure linear algebra," in *Proc. of 27th Annual IACR CRYPTO*, Santa Barbara, CA, USA, August 2007.