LINEAR PHYSICAL LAYER NETWORK CODING FOR MULTIHOP WIRELESS NETWORKS

Alister Burr and Dong Fang

University of York, U.K.
{alister.burr,dong.fang}@york.ac.uk

ABSTRACT

We consider linear network coding functions that can be employed at the relays in wireless physical layer network coding, applied to a general multi-hop network topology. We introduce a general model of such a network, and discuss the algebraic basis of linear functions, deriving conditions for unambiguous decodability of the source data at the destination. We consider the use of integer rings, integer fields, binary extension fields and the ring of binary matrices as potential algebraic constructs, and show that the ring constructs provide more flexibility. We use the two-way relay channel and a network containing two sources and two relays to illustrate the concept and to demonstrate the effect of fading of the wireless channels. We show the capacity benefits of the more flexible rings.

Index Terms— Physical layer network coding (PNC), linear algebra, rings.

1. INTRODUCTION

Physical layer network coding has significant advantages in wireless multi-hop networks, where multiple relay nodes are provided to assist multiple source nodes to transfer data to one or more destinations. It allows a node to exploit as far as possible all signals that it receives simultaneously, rather than treating most as interference. Rather than decoding each incoming data stream separately, a node detects and forwards some function of the incoming data streams.

For a number of reasons linear functions form an appealing class of functions to use for this purpose. This paper will explore the range of algebraic frameworks which might be used in these linear functions. Traditionally it has been assumed that a finite field will be used – one objective of this paper is to show that rings may also be used, and that these allow greater flexibility and lead to better performance. We will determine for the first time in abstract terms some general properties that are required of the function and its coefficients, and consider some alternative forms the function and its algebraic basis may take. We note however that linear functions are not the only approach one could take: see [1], [2]. These functions are of course more general, but are more complex to apply.

Specifically we will first consider the requirements upon the functions in order to allow unambiguous decoding of the required source symbols at the final destination, working from the forwarded function values. Secondly, we will consider the effect of the wireless channel, and how the relative phase and amplitude state of incoming wireless channels at a given node degrade the capability of that node to decode the result of some given function.

Note that in this paper we will address as general a network topology as possible, in which multiple source nodes communicate with multiple destinations via multiple layers of relays. We then use the two way relay channel (TWRC) as an example to illustrate the general principles.

Conventional, network layer, network coding (NC) uses linear functions based on Galois fields ([3]). More recently, with the emergence of compute-and-forward [4], there has been considerable work on network coding functions based on rings, and especially rings over Gaussian and Eisenstein integers [5], [6], because of their consonance with the nested lattice structures [7] used in compute-and-forward. In this paper we also focus on functions based on rings, for reasons we will explain below, but we take a more abstract and general approach, allowing an arbitrary mapping between the transmitted signals and the network code symbols. Hence its applicability is not limited to compute-and-forward, but can be applied to general physical layer network coding schemes.

In the next section we describe the general system model we will consider, including also a general description of the linear network coding functions applied at each node. We assume, as mentioned above, that data from at least one of multiple sources in the network is to be decoded at at least one destination node. We consider this requirement for unambiguous decodability, and give some conditions for the coefficients of the linear functions that ensure that it is possible.

We then consider some possible algebraic frameworks for the symbols and the coefficients, focussing in particular on two: rings over the integers modulo some arbitrary integ-

The work described in this paper is funded in part by European Commission FP7 programme, contract no. 318177 (DIWINE), and in part by U.K. EPSRC, grant no. EP-K040006, and was also carried out in collaboration under COST Action IC1004.

er q, and binary matrices. We note that these generalise in different ways the more restricted framework of fields respectively based on the integers modulo prime q, and based on binary extension fields. Next we consider the specific network topology mentioned above: the TWRC. For each algebraic framework, we show the constraints imposed by the requirement for unambiguous decodability.

Finally we consider the effects of the channel fading parameters on the incoming channels to a given relay node. This introduces a further requirement on the mapping function: that the resulting network coded symbol can be decoded from the received signal at the node. We discuss, giving some examples, how choice of mapping function can optimise performance, and evaluate this in terms of the equivocation between the received signal and the corresponding network coded symbol. This leads to an evaluation of outage probability in the case of these two topologies, after which we conclude the paper.

2. SYSTEM MODEL

The system model is shown in **Figure 1**. K sources, S_1 to S_K, are connected via P layers of relays to one destination (or more – however only one is considered here). The p^{th} layer contains $L(p)$ relays, $R_1^{(p)}$ to $R_{L(p)}^{(p)}$. We assume that relay $R_l^{(p)}$ is connected to relays $R_m^{(p-1)}, m \in \mathcal{C}_l^{(p)}$, where $\mathcal{C}_l^{(p)}$ denotes the connection set of $R_l^{(p)}$, in the sense that these are the relays from which exploitable signals are received. We will treat smaller components received from other relays as noise. Of course $R_l^{(1)}$ is connected to $S_m, m \in \mathcal{C}_l^{(1)}$. To comply with the duplex constraint we assume that each layer of relays does not transmit simultaneously with the previous one. Note that we assume here that relays receive signals only from the immediately preceding layer of relays. However to increase the generality of the model we will allow the connection set for the destination D to include relays from previous layers and indeed some sources. Thus D is connected to $R_m^{(p)}, (m,p) \in \mathcal{C}^D, p \in 0 \ldots P, m \in 1 \ldots L(p)$ where, for notational convenience, $R_m^{(0)}$ is taken to refer to S_m.

The representative symbol transmitted from $R_l^{(p)}$ is denoted $s_l^{(p)}$, and that from source S_l is $s_l^{(0)}$, or just s_l. Relay $R_l^{(p)}$ attempts to decode, and then forward, the function $f_l^{(p)}\left(\left\{s_m^{(p-1)} : m \in \mathcal{C}_l^{(p)}\right\}\right)$ of the symbols received from its connection set in the previous layer.

As we have already emphasised, this function is linear, in the sense that it can be written:

$$f_l^{(p)}\left(s_{m_1}^{(p-1)}, s_{m_2}^{(p-1)}, \ldots s_{m_{|\mathcal{C}|}}^{(p-1)}\right) = a_{lm_1}^{(p-1)} \odot s_{m_1}^{(p-1)} \oplus a_{lm_2}^{(p-1)} \odot s_{m_2}^{(p-1)} \ldots \oplus a_{lm_{|\mathcal{C}|}}^{(p-1)} s_{m_{|\mathcal{C}|}}^{(p-1)} \quad (1)$$

where $m_1, m_2, \ldots m_{|\mathcal{C}|} \in \mathcal{C}_l^{(p)}$, and $a_{m_1}^{(p-1)}, a_{m_2}^{(p-1)}, \ldots a_{m_{|\mathcal{C}|}}^{(p-1)}$ are the coefficients of the function. $\odot$ and $\oplus$ denote two operations, which we refer to as 'multiplication' and 'addition' respectively.

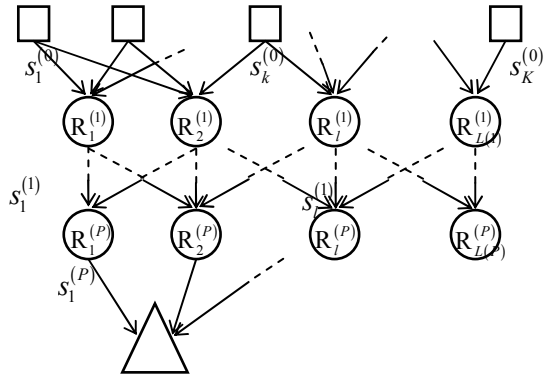

Figure 1 System model

We have not yet committed ourselves as to the nature of the symbols, the coefficients and the operations, but it is already clear that they must be drawn from an algebraic framework at least as rich as a ring, if only because two operations are defined. Other required properties of this ring will become clear as we proceed, but we will note at this point that we may allow the input symbols, the coefficients and the output symbol to be drawn from different subsets of the ring members. We denote the subset of source symbols as $\mathcal{S}$ (assuming here for simplicity that all sources use the same alphabet), with cardinality $|\mathcal{S}| = M \le q$. The subset containing the result of the function, denoted $\mathcal{S}_f$, has cardinality $|\mathcal{S}_f| = N, M \le N \le q$.

We can clearly describe the relationship between the vector of symbols transmitted from layer p-1 and those decoded at layer p in terms of a matrix:

$$\mathbf{s}^{(p)} = \mathbf{A}^{(p)} \mathbf{s}^{(p-1)} \quad (2)$$

where the element on the l^{th} row and m^{th} column of $\mathbf{A}^{(p)}$, relating the output of the m^{th} relay of the p^{th} layer to that of the l^{th} relay of the $(p\text{-}1)^{\text{th}}$ layer, is $a_{lm}^{(p)}$. $a_{lm}^{(p)}$ can be non-zero only if the latter relay is in the connection set of the former, $R_l^{(p-1)} \in \mathcal{C}_m^{(p)}$.

Hence the relation between the original source symbols and the symbols decoded and forwarded by the p^{th} layer of relays can be written as:

$$\mathbf{s}^{(p)} = \mathbf{A}^{(p)} \mathbf{A}^{(p-1)} \ldots \mathbf{A}^{(1)} \mathbf{s}^{(0)} = \mathbf{B}^{(p)} \mathbf{s} \quad (3)$$

We assume that the destination is able to detect the outputs of all relays (and sources, if applicable) within its connection set, and will write these as a vector $\mathbf{s}^D = \left\{s_m^{(p)}, (m,p) \in \mathcal{C}^D\right\}$, the length of which, $Q = |\mathcal{C}^D|$.

This also can be related to the vector of original source symbols as $\mathbf{s}^D = \mathbf{B}\mathbf{s}$.

We will assume, without loss of generality, that the destination wishes to decode s_1, and has no interest in the other source symbols. (There may be other destinations which wish to decode the other sources).

3. ALGEBRAIC FRAMEWORKS

In this section we consider the requirements that unambiguous decodability places on the network coding functions f, on the algebraic frameworks in which they operate, and on the coefficients of the functions.

Consider the set $\mathcal{S}^D$ of all symbol vectors $\mathbf{s}^D$ in the connection set of the destination. This can be partitioned into $|\mathcal{S}_1|$ subsets, corresponding to different values of s_1. For unambiguous decodability of s_1, these subsets must be distinct, that is:

$$\mathbf{B}\begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_Q \end{bmatrix} \neq \mathbf{B}\begin{bmatrix} s_1' \\ s_2' \\ \vdots \\ s_Q' \end{bmatrix}, \forall s_1 \neq s_1', s_2, s_2', \ldots s_Q, s_Q' \qquad (4)$$

We can show that unambiguous decodability is guaranteed if:

1. the first column of $\mathbf{B}$, $\mathbf{B}_{(1)}$, is not zero;
2. the non-zero elements of $\mathbf{B}_{(1)}$ are not zero divisors over the set of source symbols $\mathcal{S}$, and are uniquely invertible;
3. $\mathbf{B}_{(1)}$ is linearly independent of the remaining columns of $\mathbf{B}$.

Note that this applies to the elements of the composite matrix $\mathbf{B}$, not to the coefficients of the functions at individual relays. We will consider below how this requirement affects the mapping function coefficients for some specific network topologies. However first we consider some possible algebraic rings and fields which might be used for the coefficients.

3.1. Ring of integers modulo-q

The first case we consider is the ring of integers modulo-q, $\mathcal{R}(q) = \{0,1 \ldots q-1\}$, in which both addition, $\oplus$, and multiplication, $\odot$, are taken modulo-q. The set of source symbols $\mathcal{S} = \{0,1 \ldots M-1\}$.

In this case we note that only the subset of $\mathcal{R}(q)$ which is relatively prime to q are not zero divisors over the complete ring. These elements are also the only ones that are uniquely invertible. Hence for unambiguous decodability of s_1 only these should appear as elements in $\mathbf{B}_{(1)}$.

Note that if q is prime, the ring is a field, and all non-zero elements are invertible, and none are zero divisors. In this case any element may be chosen as a function coefficient. Moreover if all functions within the network are based on this arithmetic, then all elements of matrix $\mathbf{B}$ as well as matrices $\mathbf{A}$ are invertible, and therefore condition (2) above is necessarily fulfilled.

3.2. Binary extension field

We consider next the binary extension field $GF(q)$, whose cardinality is a power of 2, because of the advantages of using a field, and because this cardinality is more convenient than a prime number. We write $q = 2^r$. Here the elements are polynomials of order up to r-1 with binary coefficients. Addition is modulo-2 addition of the coefficients, and multiplication is polynomial multiplication modulo some irreducible polynomial of order r. **Table 1** lists the non-zero elements of $GF(4)$, giving them also in binary form and as powers of a primitive element t.

α^0	1	10	[1 0; 0 1]
α^1	t	01	[0 1; 1 1]
α^2	$t^2 \bmod (1+t+t^2) = 1+t$	11	[1 1; 1 0]
$\alpha^3 = \alpha^0$	$(t+t^2) \bmod (1+t+t^2) = 1$	10	

Table 1 Elements of $GF(4)$

This field can also be represented in the form of binary $r \times r$ matrices, whose rows are the binary representation of an element, in the form given in **Table 1**, followed by the next r-1 powers of α in binary form. They are given in this form in the last column of **Table 1**. Addition and multiplication are then modulo-2 addition and multiplication of the matrices. It will be noted that all the non-zero matrices in **Table 1** are full rank, and therefore invertible, and also that none are zero divisors.

3.3. Ring of binary matrices

This representation of binary extension fields includes only a small subset of possible $r \times r$ binary matrices, and in fact does not include all the full rank $r \times r$ binary matrices. This inspires an extension to a larger set of matrices.

Consider the set of all $r \times r$ binary matrices, in which addition is element by element modulo-2, and multiplication is matrix multiplication, again using modulo-2 arithmetic. This is a ring in which addition is again element-by-element addition modulo-2, and multiplication is matrix multiplication using modulo-2 arithmetic. The additive identity is the all zeros matrix; the multiplicative identity is the identity matrix. Not all non-zero ring elements have inverses, since

some matrices are singular, and some elements are zero divisors. Hence this is not a field.

Note however, as mentioned, that there are some full rank $r \times r$ matrices which do not occur in the field. These are also not zero divisors. Hence this ring can be used provided the three conditions above are fulfilled. It will provide a much larger range of functions which can be used at the relays, which may have advantages when used in WPNC. We will use the notation $\mathbf{A}_{lm}^{(p)}$ to refer to the coefficient of $s_m^{(p-1)}$ in the function at $R_l^{(p)}$.

However the set of data symbols is limited to cardinality 2^r, whereas the set of matrices has total size 2^{r^2}. Hence the set of inputs to the functions must be limited to a subset of the matrices. Here we arbitrarily choose matrices in which the first column is an r-tuple representing the data symbol, while the remaining columns are zero. Note that multiplication of one of these matrices by any square matrix results in another matrix of the same form, and hence this subset is closed on such multiplication. Similarly it is closed upon addition within the subset.

In this case the matrix **B** is constituted of $r \times r$ matrices, and hence can be rewritten as a composite binary matrix, which we will call **C**. The three requirements for unambiguous decodability that we stated in section 3 above then reduce to the requirement that the first r columns of **C** are linearly independent of the remaining columns. We will also define the matrix $\mathbf{C}_l^{(p)} = \left[\mathbf{A}_{lm_1}^{(p)} \ \ldots \ \mathbf{A}_{lm_{|\mathcal{C}|}}^{(p)} \right]$ to denote the relationship between the stacked binary vector of the r-tuples from the nodes in the connection set of $R_l^{(p)}$ and its output r-tuple.

4. EXAMPLE: TWO-WAY RELAY CHANNEL

We use the simplest possible example topology to illustrate our general network model and the applications of our proposed algebraic frameworks: the two-way relay channel.

Figure 2 illustrates the two way relay channel, in which two terminals exchange information via a relay. Here we are interested only in the information from the first terminal, S_1, and its reception at the second terminal, D_1. The connection set of D_1 includes the relay, labelled $R_1^{(1)}$ in accordance with our general network model, and also S_2, since it is collocated in the same terminal.

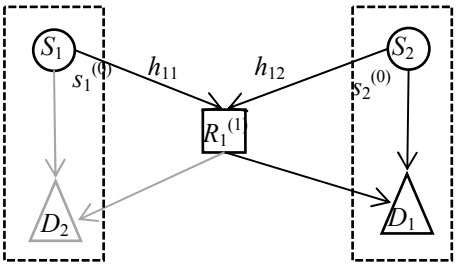

Figure 2 Two-way relay channel

In accordance with (2) and (3), but bearing in mind that this is a single layer network with only one relay, we can write:

$$s_1^{(1)} = \mathbf{A}_1^{(1)} \mathbf{s}^{(0)} = \begin{bmatrix} a_{11}^{(1)} & a_{12}^{(1)} \end{bmatrix} \begin{bmatrix} s_1^{(0)} \\ s_2^{(0)} \end{bmatrix} \tag{5}$$

The vector of symbols $\mathbf{s}^D$ at the connection set of the destination is:

$$\mathbf{s}^D = \begin{bmatrix} s_1^{(1)} \\ s_2^{(0)} \end{bmatrix} = \mathbf{B}\mathbf{s} = \begin{bmatrix} a_{11}^{(1)} & a_{12}^{(1)} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} s_1^{(0)} \\ s_2^{(0)} \end{bmatrix} \tag{6}$$

Since the first column of **B** is necessarily linearly independent of the second, the only requirement here is that the coefficient $a_{11}{}^{(1)}$ is invertible and not a zero divisor. (Of course unambiguous decodability of s_2 will place the same requirement on $a_{12}{}^{(1)}$).

5. EFFECT OF FADING

We next consider the effect of fading on the channels between the sources and the relay, which we describe for the TWRC in terms of the channel coefficients h_1 and h_2, as illustrated in **Figure 2**. This also provides a good illustration of the effect of fading at a given relay in a more general network topology.

The constellation at the relay in the TWRC has in general cardinality M^2. (In the more general topology the channel at a given relay with connection set $\mathcal{C}$ has cardinality $M^{|\mathcal{C}|}$.) Its shape is determined by the *relative fade coefficient* $h_{re} = h_2 / h_1$. The task of the relay is to decode the result of the function $f_1^{(1)}$ directly from the received signal. The result of the function defines a partition of this constellation into N subsets: the mutual information between the received signal and the network coded symbols is, at least asymptotically, determined by the minimum distance between points in this constellation in different subsets. This mutual information in turn limits the rate at which the network coded data can be received.

Hence the relay function should be chosen to maximize this mutual information, depending on the relative fade coefficient. This will be achieved if the closest points in the constellation belong to the same subset. Hence in general we must choose relay function coefficients throughout the network first to ensure unambiguous decodability at the destination, and second to maximize the mutual information at each relay, by ensuring (as far as possible within the decodability requirement) that the closest points in the composite constellation at the relay belong to the subset corresponding to the same output symbol from the function.

Note that if we use the ring of binary matrices, and represent the relay function using the matrix $\mathbf{C}_l^{(p)}$, then each row of the matrix defines a binary partition of the constellation. Thus rows of the matrix can be chosen to maximize minimum distance at each level of the partition.

6. PERFORMANCE

We measure performance in terms of the mutual information discussed in the previous section between the received signal y at a relay and its output function result f, where:

$$y = h_1 x_1 + h_2 x_2 + n = y_0(s_1, s_2) + n \quad (7)$$

in which the x's are the transmitted signals corresponding to the symbols at the nodes in the relay's connection set. Then the mutual information:

$$I(F;Y) = H(F) - H(F|Y) \quad (8)$$

where:

$$H(F|Y) = \sum_{f \in S_f} P(f) \int_{y \in \mathbb{C}} p(y|f) \log_2 \left(\frac{p(y)}{p(y|f)P(f)} \right) dy \quad (9)$$

$$P(f) = \sum_{s_1, s_2 : f = f(s_1, s_2)} P(s_1) P(s_2) \quad (10)$$

$$p(y) = \frac{1}{M^2} \sum_{s_1, s_2} p_{\mathcal{N}} \left(\frac{y - y_0(s_1, s_2)}{\sigma} \right) \quad (11)$$

$$p(y|f) = \sum_{s_1, s_2 : f = f(s_1, s_2)} p_{\mathcal{N}} \left(\frac{y - y_0(s_1, s_2)}{\sigma} \right) \quad (12)$$

and $p_{\mathcal{N}}$ denotes the complex normal distribution, with σ being the standard deviation per dimension of the noise.

For a given code rate R_c at the source nodes we may then determine the outage probability:

$$P_{out} = \int_{h_{re} \in \mathbb{C}} p(h_{re}) \mathcal{U}\left(I(F;Y) < R_c H(F) \right) dh_{re} \quad (13)$$

where $\mathcal{U}(z > z_t)$ takes the value 1 for $z > z_t$, 0 otherwise. We evaluate this using Monte Carlo integration, assuming that the function coefficients are chosen to maximize mutual information for a given relative fade coefficient, while fulfilling the requirements identified above for unambiguous decodabililty.

Figure 3 shows the results using functions with coefficients drawn from $\mathcal{R}(4)$, $\mathcal{R}(5)$, $GF(4)$, and the ring of 2×2 matrices. $\mathcal{R}(5)$ (which of course is in fact a field) is included because for the TWRC this is the only framework that can ensure that all closely spaced points fall in the same subset. However we note that because of the increased flexibility it provides, the ring of binary matrices outperforms all the other frameworks.

CONCLUSIONS

We have introduced a general model of a network using physical layer network coding, and of linear functions which might be used for network code mapping in the relays, from an abstract algebraic point of view. We determine criteria on these functions and their coefficients in order to ensure unambiguous decodability of a source at the destination. We generalize the more conventional approaches based on fields to rings of binary matrices, and consider also the effect of fading. The primary contribution of the paper is to show that compared to the finite fields conventionally used, these rings provide increased flexibility and hence can improve outage performance.

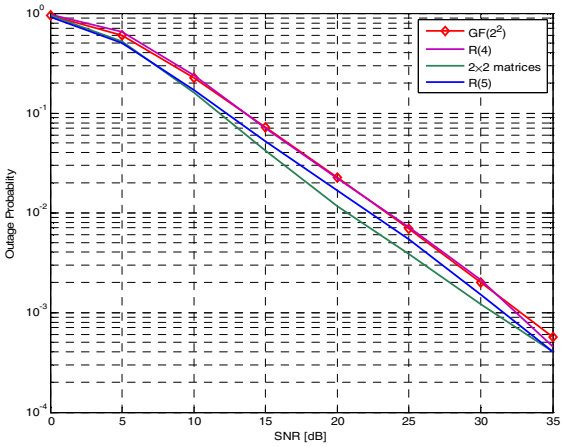

Figure 3 Outage probability using various algebraic frameworks

References

[1] T. Koike-Akino, P. Popovski and V. Tarokh, "Optimized constellations for two-way wireless relaying with physical network coding," *IEEE Journal on Selected Areas in Communications,* vol. 27, no. 5, pp. 773-787, 2009.

[2] V. Namboodiri, V. Muralidharan and B. Rajan, "Wireless bidirectional relaying and Latin Squares," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2012.

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

[4] B. Nazer and M. Gastpar, "Compute-and-Forward: Harnessing Interference Through Structured Codes," *IEEE Transactions on Information Theory,* vol. 57, no. 10, pp. 6463 - 6486, 2011.

[5] C. Feng, D. Silva and F. Kschischang, "An Algebraic Approach to Physical-Layer Network Coding," *IEEE Transactions on Information Theory,* vol. 59, no. 10, pp. 6258 - 6260, 2013.

[6] Q. Sun, J. Yuan, T. Huang and K. Shum, "Lattice Network Codes Based on Eisenstein Integers," *IEEE Transactions on Communicaions,* vol. 61, no. 7, pp. 2713 - 2725, 2013.

[7] U. Erez and R. Zamir, "Achieving 1/2 log (1+SNR) on the AWGN channel with lattice encoding and decoding," *IEEE Transactions on Information Theory,* vol. 50, no. 10, pp. 2293 - 2314, 2004.