A Class of Non-Linearly Solvable Networks

Joseph Connelly and Kenneth Zeger

***Abstract*—For each integer $m \geq 2$, a network is constructed which is solvable over an alphabet of size m but is not solvable over any smaller alphabets. If m is composite, then the network has no vector linear solution over any module alphabet. The network's capacity is shown to equal one, and when m is composite, its linear capacity is bounded away from one for all finite-field alphabets.**

I. INTRODUCTION

A *network* will refer to a finite, directed, acyclic multigraph, some of whose nodes are *sources* or *receivers*. Source nodes generate vectors of *messages*, where each message is an arbitrary element of a fixed, finite set of size at least 2, called an *alphabet*. Each outgoing edge of a network node carries a vector of alphabet elements, called *edge symbols*. Each receiver node has *demands*, which are message vectors the receiver wishes to obtain, and *decoding functions*, which map the receiver's inputs to alphabet vectors in an attempt to satisfy the receiver's demands.

A (k, n) *fractional code over an alphabet* $\mathcal{A}$ is an assignment of edge functions to all edges in a network and an assignment of decoding functions to all receiver nodes in the network, such that each source generates k components of $\mathcal{A}$ and each edge carries n components of $\mathcal{A}$. A (k, n) *solution over* $\mathcal{A}$ is a (k, n) code over $\mathcal{A}$ such that each receiver's decoding functions can recover all of its demands from its inputs

We focus attention on linear codes where the alphabets are modules. A module is a generalization of a vector space where the scalars are from a ring rather than a field. Special cases of linear codes over modules include linear codes over groups, rings, and fields. A (k, n) *linear code over an* R*-module* G has edges and decoding functions of the form

$$\sum_i M_i x_i + \sum_j M'_j y_j$$

where $x_i \in G^k$ are the messages originating at the node, $y_j \in G^n$ are the node's incoming edge symbols, M_i are $n \times k$ matrices, M'_j are $n \times n$ matrices whose entries are constant values in R, and multiplication of elements of R by elements of G is the action of the module.

A network is defined to be

- *solvable over* $\mathcal{A}$ if a $(1, 1)$ solution over $\mathcal{A}$ exists,
- *scalar linearly solvable over* $\mathcal{A}$ if there exists a $(1, 1)$ linear solution over $\mathcal{A}$, and
- *vector linearly solvable over* $\mathcal{A}$ if there exists a (k, k) linear solution over $\mathcal{A}$, for some $k \geq 1$.

A network is *solvable*, (respectively, *vector linearly solvable*) if it is solvable (respectively, vector linearly solvable) over some alphabet. The *capacity* of a network is:

$$\sup\{k/n : \exists \text{ a } (k, n) \text{ solution over some } \mathcal{A}\}.$$

The *linear capacity* over an alphabet is similarly defined.

One decade ago, it was demonstrated in [4] that there can exist a network which is solvable but not vector linearly solvable over any finite-field alphabet. To date, the network given in [4] is the only known example of such a network. In fact, the network was shown to not be vector linearly solvable over very general algebraic types of alphabets and was shown to have linear capacity bounded below its capacity for all finite field alphabets. As a result, the network has been described as "diabolical" by Kschischang [6][1] and Koetter [5].

The diabolical network has been utilized in numerous extensions and applications of network coding, such as by Krishnan and Rajan [7] for network error correction, and by Rai and Dey [8] for multicasting the sum of messages, to construct networks with equivalent solvability properties, hence showing that linear codes are insufficient for each problem. Blasiak, Kleinberg, and Lubetzky [1] used index codes to create networks where there is a polynomial separation between linear and nonlinear network coding rates. Chan and Grant [2] showed a duality between entropy functions and network coding problems, which allowed for an alternative proof of the insufficiency of linear network codes.

This work was supported by the National Science Foundation.

J. Connelly and K. Zeger are with the Department of Electrical and Computer Engineering, University of California, San Diego, La Jolla, CA 92093-0407 (j2connelly@ucsd.edu and zeger@ucsd.edu).

This paper appeared in the proceedings of the IEEE International Symposium on Information Theory (ISIT), held in Barcelona, Spain July 2016.

[1] The terminology was apparently attributed by F. Kschischang to M. Sudan.

We present an infinite class of solvable networks which are not vector linearly solvable. We denote each such network as $\mathcal{N}_4$, and we construct $\mathcal{N}_4$ from several intermediate networks denoted by $\mathcal{N}_1, \mathcal{N}_2, \mathcal{N}_3$, all of which are constructed from network building block B. Specifically, for each positive composite number m, we describe how to construct a network $\mathcal{N}_4$ which has a non-linear solution over an alphabet of size m, yet has no vector linear solution over any module alphabet. In addition, such a network is not solvable over any alphabet whose size is less than m. We omit the proofs throughout this paper due to length constraints. The full version of this paper is available in [3].

Definition I.1. Let G be an R-module. We will say that G is a *standard R-module* if

1) R acts faithfully on G; that is if $r, s \in R$ are such that $r \cdot g = s \cdot g$ for all $g \in G$, then $r = s$,
2) R has a multiplicative identity,
3) R is finite, and
4) If $r \in R$ has a multiplicative left (respectively, right) inverse, then it has a two-sided inverse, which will be denoted r^{-1}.

For any finite ring R with identity and positive integer k, the set $M_k(R)$ of $k \times k$ matrices over R with matrix addition and multiplication is a ring and R^k is a standard $M_k(R)$-module. In fact, a $(1,1)$ linear code over the $M_k(R)$-module R^k is equivalent to a (k,k) linear code over R.

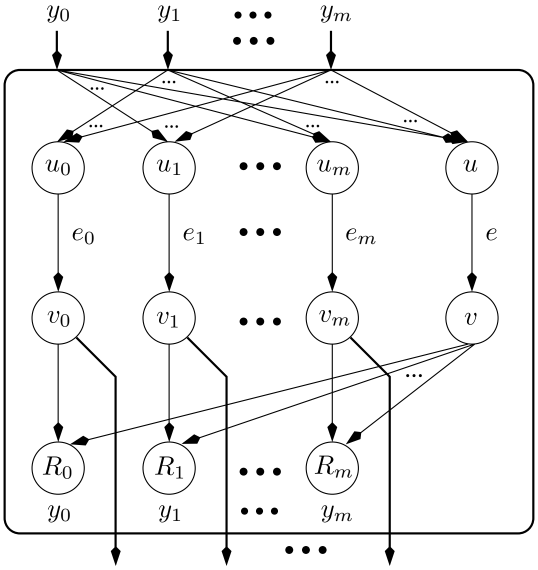

Fig. 1. The network building block $B(m)$ has message inputs $y_0, y_1, \ldots, y_m$ (from unspecified source nodes) and $m+1$ output edges.

Lemma I.2. *If a network is not scalar linearly solvable over any standard R-module, then it is not vector linearly solvable over any R-module.*

For each $m \geq 2$, the network building block $B(m)$ is defined in Figure 1 and is used to build each of the intermediate networks. The node u within $B(m)$ has an incoming edge from every message. For each i, the node u_i has an incoming edge from every message except the ith. The node v_i has a single incoming edge from node u_i, so without loss of generality, we may assume both outgoing edges of v_i carry the symbol e_i. Similarly, we may assume each of the outgoing edges of the node v carries the symbol e.

II. The network $\mathcal{N}_1(m)$

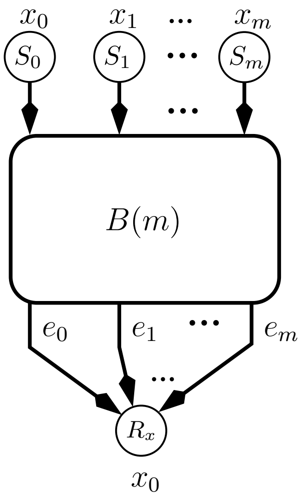

Fig. 2. The network $\mathcal{N}_1(m)$ is constructed from a $B(m)$ block together with source nodes $S_0, S_1, \ldots, S_m$ and an additional receiver R_x. For each i, the source node S_i generates the message x_i and is the ith input to $B(m)$. The additional receiver receives all of the output edges of $B(m)$ and demands x_0.

For each $m \geq 2$, network $\mathcal{N}_1(m)$ is defined in Figure 2. The special case $m = 2$ corresponds to the non-Fano network with a relabeling of messages and nodes. Lemmas II.1, II.2, and II.4, respectively, characterize $\mathcal{N}_1(m)$'s solvability, linear solvability, and capacity.

Lemma II.1. *For each $m \geq 2$, if network $\mathcal{N}_1(m)$ is solvable over alphabet $\mathcal{A}$, then m and $|\mathcal{A}|$ are relatively prime.*

Lemma II.2. *Let $m \geq 2$, and let G be a standard R-module. Then $\mathcal{N}_1(m)$ is scalar linearly solvable over G if and only if* $\mathsf{char}(R)$ *is relatively prime to m.*

Corollary II.3. *Let $m, n \geq 2$. Network $\mathcal{N}_1(m)$ is scalar linearly solvable over the ring $\mathbf{Z}_n$ if and only if m and n are relatively prime.*

Lemma II.4. *For each $m \geq 2$, network $\mathcal{N}_1(m)$ has:*

(a) *capacity equal to 1,*
(b) *linear capacity equal to 1 for any finite-field alphabet whose characteristic does not divide m, and*
(c) *linear capacity equal to $1 - \frac{1}{2m+2}$ for any finite-field alphabet whose characteristic divides m.*

III. The network $\mathcal{N}_2(m, w)$

For each $m \geq 2$ and $w \geq 1$, network $\mathcal{N}_2(m, w)$ is defined in Figure 3. We note that networks $\mathcal{N}_2(m, 1)$ and $\mathcal{N}_1(m+1)$ have similar structure, but in $\mathcal{N}_1(m+1)$ each of the output edges of $B(m+1)$ is connected to R_x, and in $\mathcal{N}_2(m, 1)$ all but one of the output edges of $B(m+1)$ are connected to R_z. This disconnected edge causes the difference in solvability properties of the two networks. The special case of $m = 2$ and $w = 1$ yields a network with solvability properties similar to the Fano network. Lemmas III.1, III.2, III.3, and III.4 characterize network $\mathcal{N}_2(m, w)$'s solvability, linear solvability, and capacity.

Lemma III.1. *For each $m \geq 2$ and $w \geq 1$, network $\mathcal{N}_2(m, w)$ is solvable over an alphabet of size mw. The solution is non-linear if and only if $w \geq 2$.*

Lemma III.2. *For each $m \geq 2$ and $w \geq 1$, if network $\mathcal{N}_2(m, w)$ is solvable over alphabet $\mathcal{A}$, then m and $|\mathcal{A}|$ are not relatively prime.*

Lemmas III.1 and III.2 provide a partial characterization of the alphabet sizes over which $\mathcal{N}_2(m, w)$ is solvable.

Lemma III.3. *Let $m \geq 2$ and $w \geq 1$, and let G be a standard R-module. Then $\mathcal{N}_2(m, w)$ is scalar linearly solvable over G if and only if $\mathsf{char}(R)$ divides m.*

Lemma III.4. *For each $m \geq 2$ and $w \geq 1$, network $\mathcal{N}_2(m, w)$ has*

(a) *capacity equal to 1,*
(b) *linear capacity equal to 1 for any finite-field alphabet whose characteristic divides m, and*
(c) *linear capacity upper bounded by $1 - \frac{1}{2mw+2w+1}$ for any finite-field alphabet whose characteristic does not divide m.*

Improving these upper-bounds on the linear capacities and/or finding codes at these rates are left as open problems. These problems appear to be non-trivial, and such improvements are unrelated to the main results of this paper.

IV. The network $\mathcal{N}_3(m, n)$

For each $m, n \geq 2$, network $\mathcal{N}_3(m, n)$ is defined in Figure 4. We note that networks $\mathcal{N}_3(m+1, m+1)$ and $\mathcal{N}_2(m, 2)$ have similar structure, except for the disconnected edge to R_z. Corollary IV.4 and Lemmas IV.2, IV.3, and IV.5 characterize network $\mathcal{N}(m, n)$'s solvability, linear solvability, and capacity.

Lemma IV.1. *Let $m, n \geq 2$ and $\alpha, s \geq 1$ such that s is relatively prime to m. Then network $\mathcal{N}_3(m, sm^{\alpha})$ is non-linearly solvable over an alphabet of size $m^{\alpha+1}$.*

Lemma IV.2. *Let $m, n \geq 2$. If network $\mathcal{N}_3(m, n)$ is solvable over alphabet $\mathcal{A}$ and $|\mathcal{A}|$ divides n, then m and $|\mathcal{A}|$ are relatively prime.*

Lemma IV.3. *Let $m, n \geq 2$, and let G be a standard R-module. Then $\mathcal{N}_3(m, n)$ is scalar linearly solvable over G if and only if $\mathsf{gcd}(\mathsf{char}(R), m, n) = 1$.*

The proof of Corollary IV.4 uses a Cartesian product code and Lemmas IV.1 and IV.3 to show $\mathcal{N}_3$ has non-linear solutions over more alphabet sizes.

Corollary IV.4. *Let $m, n \geq 2$ and $\alpha, s, t \geq 1$ such that s and t are relatively prime to m. Then network $\mathcal{N}_3(m, m^{\alpha})$ is solvable over an alphabet of size $tm^{\alpha+1}$.*

Lemma IV.5. *Let $m, n \geq 2$. Then $\mathcal{N}_3(m, n)$ has*
(a) capacity equal to 1,
(b) linear capacity equal to 1 for any finite-field alphabet whose characteristic is relatively prime to m or n, and
(c) linear capacity equal to $1 - \frac{1}{2m+2n+3}$ for any finite-field alphabet whose characteristic divides m and n.

V. The network $\mathcal{N}_4(m)$

A *disjoint union* of networks refers to a new network formed by combining existing networks with disjoint sets of nodes, edges, sources, and receivers. For each $m \geq 2$ with prime factorization $m = p_1^{\gamma_1} \cdots p_\omega^{\gamma_\omega}$, we construct network $\mathcal{N}_4(m)$ as the following disjoint union of networks $\mathcal{N}_1$, $\mathcal{N}_2$, and $\mathcal{N}_3$:

$$\begin{aligned} \mathcal{N}_4(m) = & \left(\bigcup_{\substack{\text{prime } q \\ q \nmid m \\ q < f(m)}} \mathcal{N}_1(q) \right) \\ & \cup \left(\bigcup_{i=1}^{\omega} \mathcal{N}_2\left(p_i^{\gamma_i},\ (m/p_i^{\gamma_i})\right) \right) \\ & \cup \left(\bigcup_{\substack{i=1 \\ \gamma_i > 1}}^{\omega} \mathcal{N}_3\left(p_i,\ g(m,i)\right) \right) \end{aligned}$$

where for each $i = 1, \dots, \omega$,

$$\begin{aligned} f(m) &= p_1^{\gamma_1 - 1} \cdots p_\omega^{\gamma_\omega - 1} \\ \mu(m,i) &= \min\ \{\alpha \geq 0\ :\ p_i^\alpha \geq f(m)\} \\ g(m,i) &= p_i^{\gamma_i - 1} \prod_{\substack{j=1 \\ j \neq i}}^{\omega} p_j^{\mu(m,j)}. \end{aligned}$$

In the disjoint union of networks which defines $\mathcal{N}_4(m)$, there is a $\mathcal{N}_1$ network for each prime number which is less than $p_1^{\gamma_1-1} \cdots p_\omega^{\gamma_\omega-1}$ and does not divide m, there is a $\mathcal{N}_2$ network for each prime divisor of m, and there is a $\mathcal{N}_3$ network for each prime divisor of m whose multiplicity in m is greater than one.

Theorem V.1. *For each $m \geq 2$, network $\mathcal{N}_4(m)$ is solvable over an alphabet of size m.*

Proof idea: Lemma III.1 and Corollaries II.3 and IV.4 show each disjoint network in $\mathcal{N}_4(m)$ is solvable over an alphabet of size m. ■

Theorem V.2. *For each $m \geq 2$, if network $\mathcal{N}_4(m)$ is solvable over alphabet $\mathcal{A}$, then $|\mathcal{A}| \geq m$.*

Proof idea: Lemmas II.1, III.2, IV.2 show that if $\mathcal{N}_4(m)$ is solvable over $\mathcal{A}$, then $|\mathcal{A}| \geq m$. The $\mathcal{N}_2$ networks force any prime divisor of m to be a prime divisor of $|\mathcal{A}|$. The $\mathcal{N}_1$ networks force the prime divisors of m to be the only prime divisors of $|\mathcal{A}|$. The $\mathcal{N}_3$ networks force the multiplicity of each prime divisor in $|\mathcal{A}|$ to be at least as large as its multiplicity in m. ■

Theorem V.3. *For each prime p, network $\mathcal{N}_4(p)$ is scalar linearly solvable over* $\mathrm{GF}(p)$.

Proof idea: Since p is prime, network $\mathcal{N}_4(p)$ is precisely $\mathcal{N}_2(p,1)$, which by Lemma III.3, is scalar linearly solvable over $\mathrm{GF}(p)$. ■

Theorem V.4. *For each composite number m, network $\mathcal{N}_4(m)$ is not vector linearly solvable over any R-module alphabet.*

Proof idea: Lemmas III.3 and IV.3 show $\mathcal{N}_4(m)$ is not scalar linearly solvable over any standard R-module alphabet when m is composite, so by Lemma I.2, network $\mathcal{N}_4(m)$ is not vector linearly solvable over any R-module alphabet when m is composite. ■

Theorem V.5. *For each $m \geq 2$ network $\mathcal{N}_4(m)$ has:*

(a) *capacity equal to* 1*, and*

(b) *linear capacity bounded away from* 1 *over all finite-field alphabets, if m is composite.*

Proof idea: Lemmas II.4, III.4, and IV.5 show that the linear capacity of $\mathcal{N}_4$ is bounded away from 1 when m is composite. ■

Calculating the exact linear capacity of $\mathcal{N}_4(m)$ over every finite-field alphabet is left as an open problem.

Example V.6. *Consider the special cases of the square-free integer* 6*, the prime power* 27*, and the integer* 100 *which is neither square-free nor a prime power.*

- $\mathcal{N}_4(6)$ *is the disjoint union of networks:*

$$\mathcal{N}_2(2,3) \cup \mathcal{N}_2(3,2).$$

- $\mathcal{N}_4(27)$ *is the disjoint union of networks:*

$$\mathcal{N}_1(2) \cup \mathcal{N}_1(5) \cup \mathcal{N}_1(7) \cup \mathcal{N}_2(27,1) \cup \mathcal{N}_3(3,9).$$

- $\mathcal{N}_4(100)$ *is the disjoint union of networks:*

$$\begin{gathered} \mathcal{N}_1(3) \cup \mathcal{N}_1(7) \cup \mathcal{N}_2(4,25) \cup \mathcal{N}_2(25,4) \\ \cup\ \mathcal{N}_3(2,50) \cup \mathcal{N}_3(5,80). \end{gathered}$$

For each composite number m, we have demonstrated a network which is solvable over an alphabet of size m yet is not vector linearly solvable over any R-module alphabet. Does there exist a network which is solvable over some alphabet of prime size yet is not vector linearly solvable over any R-module alphabet?

There remain numerous other open questions regarding the existence of solvable networks which are not vector linearly solvable. Are many/most solvable networks not vector/scalar linearly solvable? Can such networks be efficiently characterized? Can such networks be algorithmically recognized? We leave these questions for future research.

References

[1] A. Blasiak, R. Kleinberg, and E. Lubetzky, "Lexicographic products and the power of non-linear network coding," *IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 609–618, Oct 2011.

[2] T. Chan and A. Grant, "Dualities between entropy functions and network codes," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4470–4487, Oct 2008.

[3] J. Connelly and K. Zeger, "A class of non-linearly solvable networks," submitted to *IEEE Transactions on Information Theory*, Jan 14, 2016,
http://arxiv.org/abs/1601.03803.

[4] R. Dougherty, C. Freiling, and K. Zeger, "Insufficiency of linear coding in network information flow," *IEEE Transactions on Information Theory*, vol. 51, no. 8, pp. 2745–2759, Aug 2005.

[5] R. Koetter, Keynote presentation at *International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks* (WiOpt 2008), Mar 31 – Apr 4, 2008, Berlin, Germany, http://www.wiopt.org/wiopt08/pdf/talk_Koetter_WiOpt08.pdf.

[6] F. Kschischang, "An Introduction to Network Coding," chapter 1 in: *Network Coding: Fundamentals and Applications*, M. Médard and A. Sprintson, editors, Academic Press, 2012.

[7] P. Krishnan and B.S. Rajan, "A matroidal framework for network-error correcting codes," *IEEE Transactions on Information Theory*, vol. 61, no. 2, pp. 836–872, February 2015.

[8] B.K. Rai and B.K. Dey, "On network coding for sum-networks", *IEEE Transactions on Information Theory*, vol. 58, no. 1, pp. 50–63, January 2012.

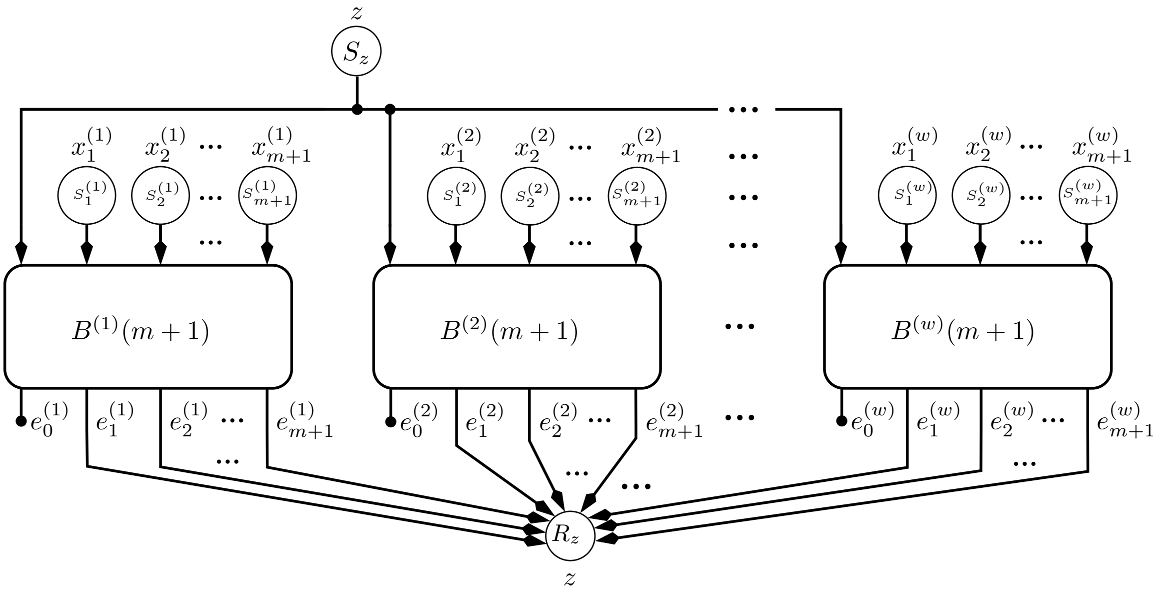

Fig. 3. Network $\mathcal{N}_2(m, w)$ is constructed from w blocks of $B(m+1)$ together with $w(m+1)+1$ source nodes and an additional receiver R_z. The shared message z is the 0th input to each $B^{(l)}(m+1)$. Each of the output edges of $B^{(l)}(m+1)$, except the 0th, is an input to the shared receiver R_z, which demands the shared message z.

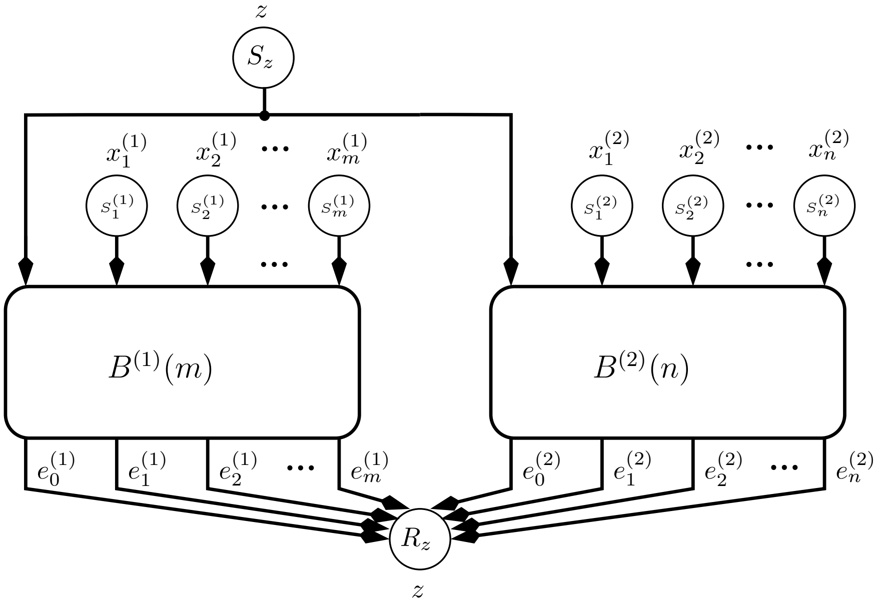

Fig. 4. The network $\mathcal{N}_3(m, n)$ is constructed from $B(m)$ and $B(n)$ blocks together with $m+n+1$ source nodes and an additional receiver R_z. The shared message z is the 0th input to both $B^{(1)}(m)$ and $B^{(2)}(n)$. The additional receiver R_z receives all of the output edges of $B^{(1)}(m)$ and $B^{(2)}(n)$ and demands the shared message z.