

Network Communication with operators in Dedekind Finite and Stably Finite Rings

Riis, S

http://arxiv.org/abs/1507.01249

For additional information about this publication click this link. http://qmro.qmul.ac.uk/xmlui/handle/123456789/11053

Information about this research object was correct at the time of download; we occasionally make corrections to records, please therefore check the published record when citing. For more information contact scholarlycommunications@qmul.ac.uk

Network Communication with operators in Dedekind Finite and Stably Finite Rings

Søren Riis

Centre of Discrete Mathematics School of Electronic Engineering & Computer Science Queen Mary University of London July 7, 2015

Abstract

Messages in communication networks often are considered as "discrete" taking values in some finite alphabet (e.g. a finite field). However, if we want to consider for example communication based on analogue signals, we will have to consider messages that might be functions selected from an infinite function space. In this paper, we extend linear network coding over finite/discrete alphabets/message space to the infinite/continuous case. The key to our approach is to view the space of operators that acts linearly on a space of signals as a module over a ring.

It turns out that modules over many rings R leads to unrealistic network models where communication channels have unlimited capacity. We show that a natural condition to avoid this is equivalent to the ring R being *Dedekind finite* (or *Neumann finite*) i.e. each element in R has a left inverse if and only if it has a right inverse. We then consider a strengthened capacity condition and show that this requirement precisely corresponds to the class of (faithful) modules over *stably finite rings* (or *weakly finite*).

The introduced framework makes it possible to compare the performance of digital and analogue techniques. It turns out that within our model, digital and analogue communication outperforms each other in different situations. More specifically we construct: 1) A communications network where *digital communication outperforms analogue communication* 2) A communication network where *analogue communication outperforms digital communication*.

The performance of a communication network is in the finite case usually measured in terms band width (or capacity). We show this notion also remains valid for finite dimensional matrix rings which make it possible (in principle) to establish gain of digital versus analogue (analogue versus digital) communications.

I. INTRODUCTION - GENERAL CONSIDERATIONS

Control theory is a branch of engineering and mathematics that deals with the operation of dynamical systems. The idea is that a controller manipulates the inputs to obtain the desired effect of the output of the system. The task is to ensure that one or more output variables have a particular behaviour when time progress.

Dynamic systems are often given by a graph with input and output nodes. This idea was presented in [10]. The graph might be cyclic containing a complicated structure of 'feedback loops'. On the edges are attached operators that modify the signals according to certain rules and transformations.

Control theory and dynamical systems have been intensively studied for more than 70 years [11], [1]. Certain types of dynamic systems date back to antiquity.

Mathematical theories of information flows in networks were developed even before modern information technology was developed. Some of the ideas used in designing Arpanet (the precursor of the internet) was for example based on queuing theory [6].

Email: s.riis@qmul.ac.uk

A crucial design idea for arplanet and the internet is called "packet-switching" [7], [6]). The idea is that messages are broken into a discrete number of pieces (packets). These pieces, each of which contains information on where it is supposed to go, would then be sent out through a network and once arriving at their destination they would be reassembled into the original message.

In modern information systems packet-switching still plays a central, crucial role. A packet of information behaves primarily as a car in a traffic system. To get from A to B, the packet of information follows a particular path. During transmission, packets are not modified or mixed with other messages.

Contrary to this approach, in (typical) dynamic control systems signals and influences are spread out and travels along many distinct paths and might even appear in complicated feedback structures. Thus, we cannot realistically expect a (non-trivial) link between regular routing (packet switching) and (standard) control theory.

Recently a new approach to communication networks has been introduced. As part of multiuser information theory *network coding* is concerned with organising and planning information flows in communication networks. However in network coding there is *no* a priori assumption that each message has to follow just one path, or that messages cannot be modified and combined during transmission [17], [16], [8], [15], [12]. Intuitively, the behaviour of messages in network coding resembles the action of signals in dynamic systems in control theory, and in this paper I will initiate an investigation into this potential overlap of research areas.

We can consider the senders in a communication network as controllers - in the sense of control theory. The output of the system is the messages/signals received at their destinations. This makes it possible to consider a typical communication problem as particular type of control problem.

Control theory typically deals with signals taking values in infinite "continuous" structures (e.g. complex-valued functions on some space), while messages in communication networks often are considered as "discrete" taking values in finite "discrete" alphabets/sets (e.g. finite fields). In this paper, I will show how the finite/discrete and infinite/continuous in the linear case naturally can be unified into one general theory.

The basic idea in network coding can be explained by considering two ground stations that are communicating via a satellite (see figure I.1)

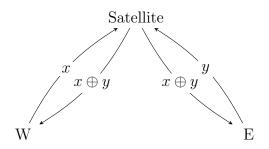


Fig. I.1. Satellite communication problem

Example I.1. Suppose that W (for west) want to send a bit $x \in \{0, 1\}$ to E (for east). Further, suppose that E wants to send a bit $y \in \{0, 1\}$ to W. The satellite receives the two bits $(x, y) \in \{0, 1\} \times \{0, 1\}$. In traditional packet routing the satellite would have to beam back to earth both the bit x and the bit y i.e. the satellite would have to transmit two bits. Using network coding we can reduce this to a single bit by letting the satellite transmit the exclusive $OR \ x \oplus y \in \{0, 1\}$. W can calculate $y = (x \oplus y) \oplus x$ and E can calculate $x = (x \oplus y) \oplus y$.

We want to include to our approach the case where the space of messages is *infinite*. We do this by considering the space of messages as a set M (commutative group) where a space of operators R acts in a linear fashion. More specifically, let $\tilde{M} = (R, M)$ be a module over a ring R. The messages are the elements in the module (i.e. the elements in M) while the space of operators that acts on the signals form the ring R.

Example I.2. Assume that W wants to send an element $m_W \in M$ to E, that simultaneously wants to send an element $m_E \in M$ to W. The satellite receives the messages m_W and m_E and transmit a message $m = r_W m_W + r_E m_E$ where $r_W, r_E \in R$. Assume that r_E has a left inverse $r_E^{-1,\text{left}}$ in R. In this case W can calculate

$$m_{\rm E} = r_{\rm E}^{-1,\rm left} (r_{\rm W} m_{\rm W} + r_{\rm E} m_{\rm E}) - r_{\rm E}^{-1,\rm left} r_{\rm W} m_{\rm W}$$

If r_W has a left inverse $r_W^{-1,left}$ station E can compute

$$m_{\rm W} = r_{\rm W}^{-1,\rm left} (r_{\rm W} m_{\rm W} + r_{\rm E} m_{\rm E}) - r_{\rm W}^{-1,\rm left} r_{\rm E} m_{\rm E}$$

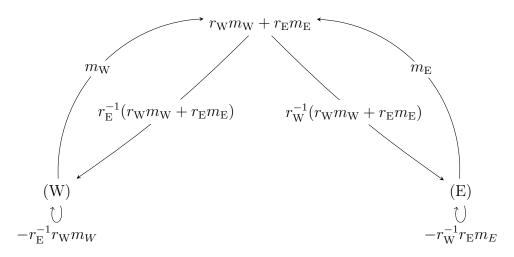
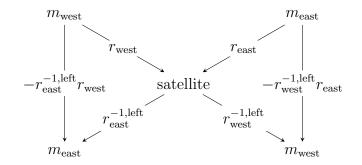


Fig. I.2. Satellite communication problem: solution over a module $\tilde{M} = (R, M)$

We can represent the satellite problem in figure I.2 as the so-called butterfly network in figure I.3



*

Notice that the sum of the products along the (two) paths from the node in the top left corner to the lower left corner is

$$(r_{\rm E}^{-1,\rm left}r_{\rm W} - r_{\rm E}^{-1,\rm left}r_{\rm W})m_{\rm W} = 0$$

and the product of the path from the upper right node to the lower left node is

$$(r_{\rm E}^{-1,\rm left}r_{\rm E})m_{\rm E}=m_{\rm E}$$

The contribution of a node n is then given by the sum of the products of all paths from the source nodes to n^{-1}

We will use this point of calculation later when we analyse solutions to more complicated communication networks. In the actual case, we can calculate the message received by the lower left node by summing the products along each path from the source nodes (upper left and upper right nodes) to the lower left node.Explicitly this sum of products is

$$(r_{\rm E}^{-1,{\rm left}}r_{\rm W} - r_{\rm E}^{-1,{\rm left}}r_{\rm W})m_{\rm W} + (r_{\rm E}^{-1,{\rm left}}r_{\rm E})m_{\rm E} = (0+1)m_{\rm E} = m_{\rm E}$$

which shows that the lower left node receives message $m_{\rm E}$ as required. A similar computation shows that the lower right node receives message $m_{\rm W}$ as required.

Now consider the communication network in figure I.4

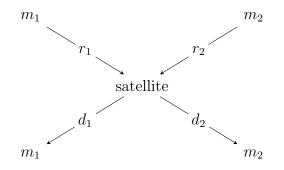


Fig. I.4. Wingless butterfly network

This is a network similar to the butterfly network but without the wings. The network corresponds to the case with two senders, two receivers and a satellite. Sender 1 wants to send a message $m_1 \in M$ via the satellite to his friend receiver 1. And sender 2 wants to send a message $m_2 \in M$ via the satellite to his friend receiver 2. Can this communication be solved, so the satellite just broadcasting one message? Intuitively, in a realistic physical model it should not be possible to solve this problem as it ought to be impossible encode two messages as one.

Now if the space of messages is infinite, it's easy to provide linear operators that solve the wingless butterfly communication problem,

Example I.3. Let M = (k, V) be a k-module where V be in infinite dimension vector space over the field k such that there is a k-isomorphism $\theta : V \to V \oplus V$. Define projections $p_1, p_2 :$ $V \oplus V \to V$ by $p_1(v_1, v_2) := v_1$ and $p_2(v_1, v_2) := v_2$ and define inclusions $i_1, i_2 : V \to V \oplus V$ by $i_1(v) = (v, 0) \in V \oplus V$ and $i_2(v) = (0, v) \in V \oplus V$.

¹An elaboration of this idea that reassembles the Feynman integral can be found in [14]

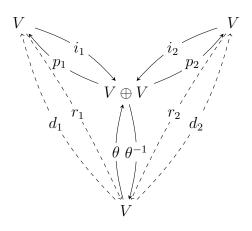


Fig. I.5. Commutative diagram

Consider the commutative diagram in figure I.5. The k-homomorphisms r_1, r_2, d_1 and d_2 on the dashed lines are uniquely determined by $d_1 := p_1 \theta$, $d_2 := p_2 \theta$, $r_1 := \theta^{-1} i_1$, $r_2 := \theta^{-1} i_2$.

The communication problem in figure I.4 can now be solved by letting the satellite broadcast the message

$$m_{\text{satellite}} := \theta^{-1} i_1 v_1 + \theta^{-1} i_2 v_2$$

where $v_1 := m_1$, $v_2 := m_2$, and thus $m_1 = p_1 \theta m_{\text{satellite}}$ and $m_2 = p_2 \theta m_{\text{satellite}}$.

This example illustrate that: The issue whether operators (like r_1, r_2, d_1 and d_2) should be considered realistic from a physical point of view (they are not) is determined by properties of the ring they generate.

The wingless butterfly communication problem can be expressed in mathematical terms as follows: The satellite receives the messages $m_1 \in M$ and $m_2 \in M$ and broadcast a message of the form $m = r_1m_1 + r_2m_2 \in M$. For this communication to work there need to be ring elements $d_1, d_2 \in R$ that the receivers can use for decoding. More specifically the communication problem has a solution over the module $\tilde{M} = (R, M)$ if and only

(*)
$$\exists r_1, r_2, d_1, d_2 \in R \ \forall m_1, m_2 \in M : m_1 = d_1(r_1m_1 + r_2m_2) \text{ and } m_2 = d_2(r_1m_1 + r_2m_2)$$

We will often assume that R acts faithfully on M i.e. if an operator behaves like the identity, it is the identity i.e. $\forall r \in R : (\forall m \in M \ rm = m) \rightarrow r = 1$. This is logically equivalent to the the statement that two operators are identical if on only if the behave the same way i.e. $\forall r, s \in R : (\forall m \in M \ rm = sm) \rightarrow r = s$. This in turn is equivalent to the most common definition of R acting faithfully: $\forall r \in R \setminus \{0\} \ \exists m \in M : rm \neq 0$.

If R acts faithfully on M (*) is equivalent to

$$(**)$$
 $\exists r_1, r_2, d_1, d_2 \in R: d_1r_1 = d_2r_2 = 1$ and $d_1r_2 = d_2r_1 = 0$

For many rings (**) is valid, but as we just noted in a *realistic physical model* it should not be possible to encode two messages as one. From a mathematic point of view this is of course unproblematic to consider modules over rings R that satisfy (**), however we want to formalise the idea that each channel has bounded finite capacity rather than unbounded capacity. We take the view that a module $\tilde{M} = (R, M)$ over a ring R that satisfies (**) cannot be implemented by any realistic physical system.

*

II. DEDEKIND FINITE RINGS AND THE CAPACITY CONDITION

A. Dedekind finite rings

A ring R (with 1-element) is *Dedekind finite* (or von Neumann finite, or directly finite) if

$$\forall x, y \in R : xy = 1 \to yx = 1$$

i.e. all one-sided inverses in R are two-sided [9]

Many classes of rings are Dedekind finite. Commutative rings, finite rings, and the matrix rings $M_n(F)$ are Dedekind finite. Domains are Dedekind finite and so are left as well as right Noetherian rings. For a field k any finitely dimensional k-algebra is Dedekind finite. And for any group G the group algebra kG is Dedekind finite. Rings with only finitely many nilpotent elements (i.e. elements x where $x^n = 0$ for some $n \in \{1, 2, ...\}$) are Dedekind finite. Reversible rings i.e. rings where $\forall x, y \ (xy = 0 \rightarrow yx = 0)$ are Dedekind finite. Any direct product of Dedekind finite rings is Dedekind finite.

Example II.1. Let V be a vector space and let R be the ring of linear operators acting on V. A linear operator $T \in R$ is injective (i.e. 1-1) if and only if it has a left-inverse, and it is surjective (i.e. onto) if and only if it has a right-inverse. More concretely, assume we try to solve an operator equation Tx = v for some $v \in V$. If T has a left inverse $T^{-1,\text{left}}$ we know that Tx = v has either no or one solution. Furthermore, if the equation has a solution, it is given by $T^{-1,\text{left}}v$. If T has a right inverse $T^{-1,\text{right}}w$ know that $T^{-1,\text{right}}v$ is a solution, but the equation Tx = v might have other solutions. Dedekind finite rings are rings R of operators where surjective, injective or bijective are equivalent properties.

There are various ways to express that a ring R is Dedekind finite. The following list is not exhaustive but is sufficient for our purpose.

Theorem II.2. Let R be a ring with 1 element. Then the following statements are equivalent:

- 1) *R* is Dedekind finite i.e. $\forall x, y \in R \ (xy = 1 \rightarrow yx = 1)$
- 2) Each element that has a right inverse has a left inverse i.e. $\forall x \ ((\exists y \ xy = 1) \rightarrow (\exists z \ zx = 1))$
- 3) $\forall x, y, z \in R \ ((xy = 1 \land xz = 0) \rightarrow z = 0) \ (capacity \ condition)$
- 4) Each element has at most one right inverse i.e. $\forall x, y, z \in R \ ((xy = 1 \land xz = 1) \rightarrow y = z)$
- 5) Each element that has a left inverse have a two sided inverse i.e. $\forall x, y \ ((yx = 1) \rightarrow (\exists z \ xz = zx = 1))$
- 6) Each element that has a left inverse has a right inverse i.e. $\forall x \ ((\exists y \ yx = 1) \rightarrow (\exists z \ xz = 1))$
- 7) $\forall x, y, z \in R$ ($(yx = 1 \land zx = 0) \rightarrow z = 0$) (the dual of the capacity condition)
- 8) Each element has at most one left inverse i.e. $\forall x, y, z \in R$ $((yx = 1 \land zx = 1) \rightarrow y = z)$
- 9) Each element that has a right inverse have a two sided inverse i.e. $\forall x, y \ ((xy = 1) \rightarrow (\exists z \ xz = zx = 1))$

To the best of my knowledge condition 3 and condition 7 are new ways of expressing that a ring is Dedekind finite.

Proof:

(1) ⇒ (2): (1) can be stated as ∀x ((∃y xy = 1 → yx = 1) which logically implies (2)
(2) ⇒ (3): Assume xy = 1 and xz = 0 and assume that (2). Then since x has a right inverse y it has a left inverse w so wx = 1. But then 0 = w0 = w(xz) = (wx)z = 1z = z.
(3) ⇒ (4): Assume y₁, y₂ are right inverse of x ∈ R. Then xy₁ = 1 and xy₂ = 1 and so x(y₂ - y₁) = 0. But then according to the assumption (3) y₂ - y₁ = 0 and y₁ = y₂.

(4) \implies (1): Assume that xy = 1. Consider the element (1 - yx + y) and notice that x(1 - yx + y) = x - xyx + xy = xy = 1. Since we assumed that x has at most one right inverse it follows that y = (1 - yx + y), than thus that yx = 1.

(1) \implies (5): Assume that y has left inverse x i.e. that xy = 1. Then according to 1 it follows that yx = 1 i.e. that y has a two sided inverse.

(5) \implies (1): Assume xy = 1 i.e. y has a left inverse. But then y has a two sided inverse i.e the exist $z \in R$ s.t. zy = yz = 1. But then yx = yx(yz) = y(xy)z = yz = 1 i.e. xy = yx = 1.

This shows that $(1) \iff (2) \iff (3) \iff (4) \iff (5)$. The dual versions $(1) \iff (6) \iff (7) \iff (8) \iff (9)$ can be shown in by simillar (but dual) arguments.

B. The Capacity condition

Consider the network in figure II.1.

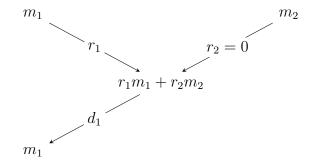


Fig. II.1. Capacity condition

The network takes two massage m_1 and m_2 as input and the message m_1 can be calculated at the left lower receiver. We could have added a receiver at the lower right, but since this receiver node has no special requirement we omit it. Intuitively the full bandwidth of the involved channels is used to transmit the message m_1 and thus $r_1m_1 + r_2m_2$ cannot depend on m_2 . In other words if d_1 is a decoding operator i.e. $d_1(r_1m_1 + r_2m_2) = m_1$ i.e. if $d_1r_1 = 1$ and $d_1r_2 = 0$ then $r_2 = 0$ (see figure II.2 for a commutative diagram expressing the capacity condition).

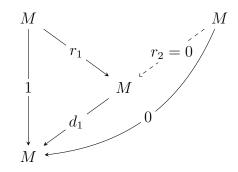


Fig. II.2. Commutative diagram: Capacity condition

This condition on R can formally be expressed as:

$$\forall x, y, z \in R \ ((xy = 1 \land xz = 0) \to z = 0) \tag{1}$$

We showed in the previous section that this condition is equivalent to R being a Dedekind finite ring.

Example II.3. Let R be a ring that satisfies condition (**) we considered previously i.e.

(**)
$$\exists r_1, r_2, d_1, d_2 \in R$$
: $d_1r_1 = d_2r_2 = 1$ and $d_1r_2 = d_2r_1 = 0$

Clearly R is not Dedekind finite since if R were Dedekind finite $d_1r_1 = 1$ and $d_1r_2 = 0$ would imply that $r_2 = 0$ (by the capacity condition) which would be a contradiction since $1 = d_2r_2 = d_20 = 0$.

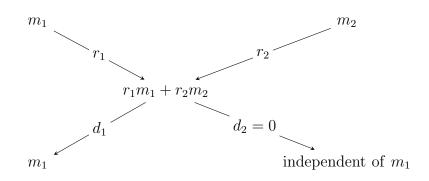


Fig. II.3. Dual capacity condition

Example II.4. Consider figure II.3. A message m_1 is being transmitted through a channel and being decoded such that $d_1r_1m_1 = m_1$. Then intuitively r_1m_1 is bijective so if for some operator d_2 , $d_2r_1m_1 = 0$ then $d_2 = 0$. Thus if $d_1r_1 = 1$ and $d_2r_1 = 0$, then $d_2 = 0$ (see figure II.4 for a commutative diagram expressing this condition).

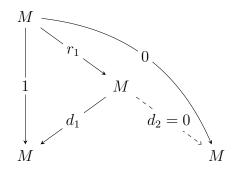


Fig. II.4. Commutative diagram: Dual capacity condition

This principle can be stated as:

$$\forall x, y, z \in R \ ((yx = 1 \land zx = 0) \to z = 0) \tag{2}$$

which is the dual capacity condition. As we showed in the previous section, this condition is also equivalent to R being Dedekind finite.

Example II.5. Polynomial identity rings (PI-rings) have been extensively investigated in the literature [4], [5]. PI-rings (are isomorphic to) rings that occur by considering a commutative ring S and then consider formal polynomial expressions $p \in S[x_1, x_2, ..., x_n]$ in non-commuting

variables that satisfies at least one identity $p(a_1, a_2, ..., a_n) = 0$ for all $a_1, ..., a_n \in S[x_1, ..., x_n]$. If A is a PI-ring then obviously every subring of A and homomorphic image of A will satisfy the identity as well. It can be shown that every PI ring is Dedekind finite.

The case where $p = x_1x_2 - x_2x_1 = 0$ corresponds to commutative rings (that trivially are Dedekind finite).

Consider the ring $A = M_2(S)$ of 2×2 matrices with coefficients in S. For any $a_1, a_2 \in A$, clearly $tr(a_1a_2 - a_1a_1) = 0$ and thus by the Cayley-Hamilton Theorem $(a_1a_2 - a_2a_1)^2 = s1$ for some $s \in S$. Therefore $(a_1a_2 - a_2a_1)^2$ commute with every element in A. Thus A is a PI-ring since it satisfies the polynomial identity $p = (x_1x_2 - x_2x_1)^2x_3 - x_3(x_1x_2 - x_2x_1)^2 = 0$.

More, generally the Amitsur-Levitzki Theorem provide a (multilinear) polynomial identity for each ring $M_k(S)$ of $k \times k$ matrices with coefficients in S.

III. FINITELY STABLE RINGS AND THE STRENGTHENED CAPACITY CONDITION

A. Finitely stable rings

For a ring R we can consider the matrix ring $M_k(R)$ that consists of $k \times k$ matrices with entries in R. Multiplication is the usual matrix multiplication and addition is matrix addition.

Definition III.1. We say that a ring R is k-stable if the matrix ring $M_k(R)$ is Dedekind finite ² We say R is finitely stable (or fully Dedekind finite or weakly finite) if R is k-stable for each $k \in \{1, 2, 3, ...\}$.

Commutative rings can be shown to be finitely stable. Noetherian rings and Artinian rings are stably finite. A subring of a stably finite ring and a matrix ring over a stably finite ring is stably finite.

1-stable is the same as Dedekind finite. Notice that *m*-stable implies *k*-stable when m > k. Thus each 2-stable ring is Dedekind finite. The converse is not valid: There exists a Dedekind finite ring *R* (in fact *R* can be chosen to be a domain) such that *R* fails to be a 2-stable. (see exercise 1.18 that outlines the argument). More generally there exists for each k > 1 a *k*-stable ring *R* that is not (k + 1)-stable.

Example III.2. The nth Weyl algebra is the ring $R_{weyl,n} := k[x_1, x_2, ..., x_n, \frac{\partial}{x_1}, \frac{\partial}{x_2}, ..., \frac{\partial}{x_n}]$ of differential operators $\frac{\partial}{x_1}, \frac{\partial}{x_2}, ..., \frac{\partial}{x_n}$ on the polynomial ring of n variables over a field k with the obvious relations. Weyl algebras are named after Hermann Weyl, who introduced them to study the Heisenberg uncertainty principle in quantum mechanics. Each Weyl algebra $R_{weyl,n}$ is an infinitely dimensional vector space over k. The nth Weyl algebra is a simple Noetherian domain and thus stably finite.

B. Requirements from finite capacity

We will now argue that the class of Dedekind finite rings is too broad to serve as the class of rings that intuitively should be considered rings of *legitimate* operators.

Consider the network in figure III.1.

²There doesn't seem to be an agreed name for k-stable rings though this class of rings certainly have been considered in the literature

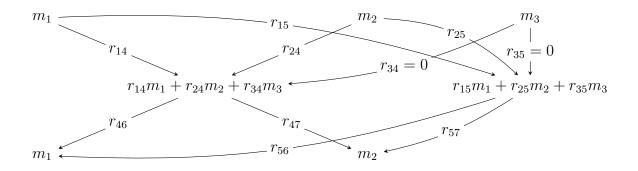


Fig. III.1. Strengthened capacity condition

If we can assign operators $r_{ij} \in R$ $i, j \in \{1, 2, 3, 4, 5, 6, 7, 8\}$ to the edges in the graph such that m_1 and m_2 can be reconstructed correctly at the two lower bottom nodes we get the following identitity:

$$\begin{bmatrix} r_{46} & r_{56} \\ r_{47} & r_{57} \end{bmatrix} \begin{bmatrix} r_{14} & r_{24} & r_{34} \\ r_{15} & r_{25} & r_{35} \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} = \begin{bmatrix} m_1 \\ m_2 \end{bmatrix}$$

which can also be written as

$$\begin{bmatrix} r_{46} & r_{56} \\ r_{47} & r_{57} \end{bmatrix} \begin{bmatrix} r_{14} & r_{24} \\ r_{15} & r_{25} \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \end{bmatrix}$$
$$\begin{bmatrix} r_{46} & r_{56} \\ r_{47} & r_{57} \end{bmatrix} \begin{bmatrix} r_{34} \\ r_{35} \end{bmatrix} [m_3] = \begin{bmatrix} 0 \\ 0 \end{bmatrix} [m_3]$$

Now these matrix equations have a solution if and only if the following matrix equations are solvable for a suitable choice of operators $r_{i,j} \in R$ i.e.

$\begin{bmatrix} r_{46} \\ r_{47} \end{bmatrix}$	$\begin{bmatrix} r_{56} \\ r_{57} \end{bmatrix} \begin{bmatrix} r \\ r \end{bmatrix}$	$\begin{bmatrix} 14 & r_{24} \\ 15 & r_{25} \end{bmatrix}$	$=\begin{bmatrix}1\\0\end{bmatrix}$	$\begin{bmatrix} 0\\1 \end{bmatrix}$
$\begin{bmatrix} r_{46} \\ r_{47} \end{bmatrix}$	$\begin{bmatrix} r_{56} \\ r_{57} \end{bmatrix} \begin{bmatrix} r \\ r \end{bmatrix}$	$_{34}^{34} r_{34}' \ _{35}^{r_{35}'}$	$=\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix} 0\\ 0 \end{bmatrix}$

and

and

This condition is equivalent to the matrix ring $M_2(R)$ satisfying the condition

$$\forall x, y, z \in R \ ((xy = 1 \land xz = 0) \to z = 0)$$

where

$$x = \begin{bmatrix} r_{46} & r_{56} \\ r_{47} & r_{57} \end{bmatrix}, y = \begin{bmatrix} r_{14} & r_{24} \\ r_{15} & r_{25} \end{bmatrix}, z = \begin{bmatrix} r_{34} & r'_{34} \\ r_{35} & r'_{35} \end{bmatrix}$$

Using proposition II.2 we conclude that the matrix equations have a solution if and and only ring $M_2(R)$ Dedekind finite. Thus the matrix equations are solvable if and only if R is 2-stable.

Example III.3. A ring R has the Invariant Basis Number property (IBN-property) if R^m and R^n are isomorphic as R modules if and only if m = n. Stably finite rings are IBN rings.

Consider figure III.2 and consider the principle Prin(n) that $x_1, x_2, ..., x_{n+1}$ cannot all be reconstructions at the n + 1 corresponding receiver nodes. Prin(1) is equivalent to condition

(**). For $n \ge 1$ the principle Prin(n) can be shown to be equivalent to the property that \mathbb{R}^n is not isomorphic to \mathbb{R}^{n+1} . The principle Prin(n) for n = 1, 2, 3, ... can be shown to be equivalent to \mathbb{R} has the IBN-property.

Consider figure III.2. Intuitively, if $x_1, x_2, ..., x_n$ can be reconstructed correctly at the receiver notes $x_1, x_2, ..., x_n$, then the message received by node n + 1 must be independent of x_{n+1} .

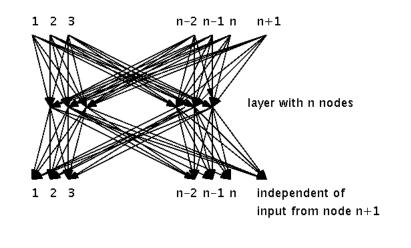


Fig. III.2.

The case n = 1 is the network where the condition Cond(1) on R is equivalent to R being Dedekind finite. The condition arising for n = 2 is the condition Cond(2) we just considered leading to the requirement that $M_2(R)$ is Dedekind finite.

Now consider Cond(k). Let the inputs denote $m_1, m_2, ..., m_k$ for nodes 1, 2, ..., k and denote the input to node k+1 by m_{k+1} . Cond(k) can be written as the condition that the matrix identity

$$\tilde{B}\tilde{A} = 1, \tilde{B}\tilde{C} = 0$$

of $k \times k$ matices in $M_k(R)$ implies that $\tilde{C} = 0$. Thus Cond(k) is equivalent to the condition that the matrix ring $M_k(R)$ satisfies the condition

$$\forall x, y, z \in R \ ((xy = 1 \land xz = 0) \to z = 0)$$

Again, applying proposition II.2 this is equivalent to the matrix ring $M_k(R)$ being Dedekind finite. Thus we get:

Proposition III.4. A ring R satisfies condition Cond(k) if and only if R is k-stable. A ring R satisfies each condition Cond(k) for $k \in \{1, 2, 3, ...\}$ if and only if R is stably finite.

IV. DIGITAL SIGNALS CAN BE MORE EFFICIENT THAN ANALOGUE SIGNALS

As previous consider a R-module $\tilde{M} = (R, M)$, where the elements in the ring R acts on the elements in the additive space of messages (signals) M. In general when signals (i.e. point in M) are real or complex valued functions, f(t) + f(t) = 0 only when f(t) = 0. Thus if $1 \in R$ is the identity operator $1 + 1 \neq 0$. On the other hand if data consists of binary strings $\operatorname{bit}(j), j \in I$ (with I finite or infinite), $\operatorname{bit}(j) + \operatorname{bit}(j) = 0$ and thus 1 + 1 = 0.

Consider the following Information Network in figure IV. This network was constructed based on intuitive, informal considerations. It is possible to be more systematic and apply the

+

constructions in [2]. However, these methods only seem to work for commutative rings, and a lot of extra work would be needed to implement this approach. Also, the resulting networks would be larger and more complex than the ad hoc network constructed here. In the communication network we have constructed in figure IV, the task is to transmit messages $x, y, z \in M$ from node 1, 2 and 3 to the notes 7, 9, 10 and 11 as indicated.

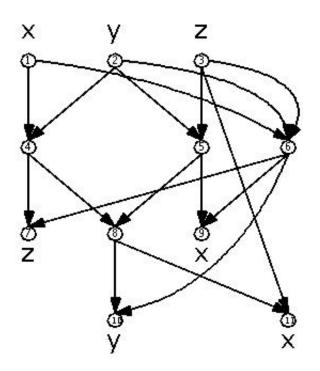


Fig. IV.1.

We will show:

Theorem IV.1. The Communication Network in figure IV has a linear solution over any ring where 1 + 1 = 0, but has no solutions over Dedekind finite rings where $1 + 1 \neq 0$

Proof: Let us denote the operators (ring elements) assigned to the different edges by

 $r_{1,4}, r_{1,6}, r_{2,4}, r_{2,5}, r_{2,6}, r_{3,5}, r_{3,6}, r_{3,11}, r_{4,7}, r_{4,8}, r_{5,8}, r_{5,9}, r_{6,7}, r_{6,9}, r_{6,10}, r_{8,10}, r_{8,11}, r_{4,7}, r_{4,8}, r_{5,8}, r_{5,9}, r_{6,7}, r_{6,9}, r_{6,10}, r_{8,10}, r_{8,11}, r_{1,6}, r_{$

The ring elements provide a solution to the communication problem if and only if the following 12 equations hold.

- (1) paths from i_x to o_x : $r_{6,9}r_{1,6} = 1$
- (2) paths from i_x to o_y : $r_{8,10}r_{4,8}r_{1,4} + r_{6,10}r_{1,6} = 0$
- (3) paths from i_x to o_z : $r_{4,7}r_{1,4} + r_{6,7}r_{1,6} = 0$
- (4) paths from i_x to \bar{o}_x : $r_{8,11}r_{4,8}r_{1,4} = 1$
- (5) paths from i_y to o_x : $r_{5,9}r_{2,5} + r_{6,9}r_{2,6} = 0$
- (6) paths from i_y to o_y : $r_{8,10}r_{4,8}r_{2,4} + r_{8,10}r_{5,8}r_{2,5} + r_{6,10}r_{6,2} = 1$

- (7) paths from i_y to o_z : $r_{4,7}r_{2,4} + r_{6,7}r_{2,6} = 0$
- (8) paths from i_y to \bar{o}_x : $r_{8,11}r_{4,8}r_{2,4} + r_{8,11}r_{5,8}r_{2,5} = 0$
- (9) paths from i_z to o_x : $r_{5,9}r_{3,5} + r_{6,9}r_{3,6} = 0$
- (10) paths from i_z to o_y : $r_{6,10}r_{3,6} + r_{8,10}r_{5,8}r_{3,5} = 0$
- (11) paths from i_z to o_z : $r_{6,7}r_{3,6} = 1$
- (12) paths from i_z to \bar{o}_x : $r_{8,11}r_{5,8}r_{3,5} + r_{3,11} = 0$

The first part of the theorem follows since the equations (1)-(12) have a solution over any ring where 1 + 1 = 0 since equations (1)-(12) holds if we chose each $r_{ij} = 1$ i.e.

$$r_{1,4} = r_{1,6} = r_{2,4} = r_{2,5} = r_{2,6} = r_{3,5} = r_{3,6} = r_{3,11} =$$

$$r_{4,7} = r_{4,8} = r_{5,8} = r_{5,9} = r_{6,7} = r_{6,9} = r_{6,10} = r_{8,10} = r_{8,11} = 1$$

To show the second part of the theorem we need to show that any Dedekind finite ring R that satisfies equations (1)-(12) is forced to have 1 + 1 = 0.

(13) According to (1) $r_{6,9}r_{1,6} = 1$. Thus $r_{1,6}$ and $r_{6,9}$ each have a two-sided inverse.

(14) According to (4) $r_{8,11}r_{4,8}r_{1,4} = 1$. Thus $r_{8,11}, r_{4,8}$ and $r_{1,4}$ each have a two-sided inverse.

(15) According to (8) $r_{8,11}r_{4,8}r_{2,4} + r_{8,11}r_{5,8}r_{2,5} = 0$. Since $r_{8,11}$ has a left inverse (14), it follows that $r_{4,8}r_{2,4} + r_{5,8}r_{2,5} = 0$.

(16) According ro (6) $r_{8,10}r_{4,8}r_{2,4}+r_{8,10}r_{5,8}r_{2,5}+r_{6,10}r_{2,6} = 1$. According to (15) $r_{8,10}(r_{4,8}r_{2,4}+r_{5,8}r_{2,5})+r_{6,10}r_{2,6}=r_{6,10}r_{2,6}=1$. Thus $r_{2,6}$ and $r_{6,10}$ each have a two-sided inverse.

(17) According to (5) $r_{5,9}r_{2,5} + r_{6,9}r_{2,6} = 0$. We showed that $r_{2,6}$ has a two-sided inverse (16), and that $r_{6,9}$ has a two-sided inverse (13). Thus $r_{5,9}r_{2,5}r_{2,6}^{-1}r_{6,9}^{-1} = -1$ from which its straight forward to conclude that $r_{5,9}$ and $r_{2,5}$ each have a two sided inverse.

(18) According to (11) $r_{6,7}r_{3,6} = 1$. Thus $r_{3,6}$ and $r_{6,7}$ each have a two sided inverse.

(19) According to (9) $r_{5,9}r_{3,5} + r_{6,9}r_{3,6} = 0$. We have already shown that $r_{3,6}$ has a two-sided inverse (18), and we also have shown that $r_{6,9}$ has a two-sided inverse (13). Thus $r_{5,9}r_{3,5}r_{3,6}^{-1}r_{6,9}^{-1} = -1$ and thus $r_{3,5}$ has a two sided inverse.

(20) According to (7) $r_{4,7}r_{2,4}+r_{6,7}r_{2,6}=0$. We already showed that $r_{6,7}$ has a two-sided inverse (18), and we also showed that $r_{2,6}$ has a two-sided inverse (16). Thus $r_{4,7}r_{2,4}r_{2,6}^{-1}r_{6,7}^{-1}=-1$. Thus $r_{4,7}$ and $r_{2,4}$ each have a two-sided inverse.

(21) According to (10) $r_{6,10}r_{3,6} + r_{8,10}r_{5,8}r_{3,5} = 0$. Now $r_{3,6}$ and $r_{6,10}$ each has a two-sided inverse (18),(16). From this we conclude that $r_{8,10}r_{5,8}r_{3,5}r_{3,6}^{-1}r_{6,10}^{-1} = -1$ and that $r_{8,10}$ and $r_{5,8}$ each has a two sided inverse.

(22) According to (8) $r_{4,8}r_{2,4} + r_{5,8}r_{2,5} = 0$. We already showed that $r_{2,5}$ and $r_{5,8}$ each has a two-sided inverse (17),(21). Thus $r_{4,8}r_{2,4}r_{2,5}^{-1}r_{5,8}^{-1} = -1$ and $r_{4,8}$ has a two sided inverse.

(23) According to (1) $r_{6,9}r_{1,6} = 1$. From this we already concluded in (13) that $r_{6,9}$ and $r_{1,6}$ each has a two-sided inverse, and thus $r_{1,6} = r_{6,9}^{-1}$.

(24) According to (2) $r_{8,10}r_{4,8}r_{1,4} + r_{6,10}r_{1,6} = 0$ thus according to (13), (14) and (21) we can conclude that $r_{1,4} = -r_{4,8}^{-1}r_{8,10}^{-1}r_{6,10}r_{6,9}^{-1}$.

(25) According to (3) $r_{4,7}r_{1,4}+r_{6,7}r_{1,6}=0$. Thus according to (24) it follows that $r_{4,7}(-r_{4,8}^{-1}r_{8,10}^{-1}r_{6,10}r_{6,9}^{-1})+r_{6,7}r_{6,9}^{-1}=0$. From this and (13) we conclude that $r_{6,7}=r_{4,7}r_{4,8}^{-1}r_{8,10}^{-1}r_{6,10}$.

(26) According to (4) $r_{8,11}r_{4,8}r_{1,4} = 1$. From (24) we conclude that $r_{8,11} = r_{1,4}^{-1}r_{4,8}^{-1} = (-r_{4,8}^{-1}r_{8,10}^{-1}r_{6,10}r_{6,10}r_{6,10}^{-1}r_{4,8}^{-1} = -r_{6,9}r_{6,10}^{-1}r_{8,10}$

(27) According to (5) $r_{5,9}r_{2,5}+r_{6,9}r_{2,6}=0$. According to (17) it follows that $r_{2,5}=-r_{5,9}^{-1}r_{6,9}r_{2,6}$.

(28) According to (8) $r_{8,11}r_{4,8}r_{2,4} + r_{8,11}r_{5,8}r_{2,5} = 0$. According to (21) $r_{4,8}r_{2,4} + r_{5,8}r_{2,5} = 0$ and (14) $r_{2,4} = -r_{4,8}^{-1}r_{5,8}r_{2,5}$. Substituting (22) into this we get $r_{2,4} = -r_{4,8}^{-1}r_{5,8}r_{2,5} = -r_{4,8}^{-1}r_{5,8}(-r_{5,9}^{-1}r_{6,9}r_{2,6}) = r_{4,8}^{-1}r_{5,9}r_{6,9}r_{2,6}$.

(29) According to (6) $r_{8,10}r_{4,8}r_{2,4} + r_{8,10}r_{5,8}r_{2,5} + r_{6,10}r_{2,6} = 1$. According to (16) $r_{6,10}r_{2,6} = 1$ and thus $r_{2,6} = r_{6,10}^{-1}$.

(30) According to (27) and (29) $r_{2,5} = -r_{5,9}^{-1}r_{6,9}r_{2,6} = -r_{5,9}^{-1}r_{6,9}r_{6,10}^{-1}$

(31) According to (7) $r_{4,7}r_{2,4} + r_{6,7}r_{2,6} = 0$. According to (28) we have $0 = r_{4,7}r_{2,4} + r_{6,7}r_{2,6} = r_{4,7}(r_{4,8}^{-1}r_{5,8}r_{5,9}^{-1}r_{6,9}r_{6,10}^{-1}) + (r_{4,7}r_{4,8}^{-1}r_{8,10}^{-1}r_{6,10})r_{6,10}^{-1}$. Thus $0 = r_{4,7}r_{4,8}^{-1}r_{5,8}r_{5,9}^{-1}r_{6,9}r_{6,10}^{-1} + r_{4,7}r_{4,8}^{-1}r_{8,10}^{-1}r_{6,10}r_{6,10}^{-1} = r_{4,7}r_{4,8}^{-1}r_{5,9}r_{6,9}r_{6,10}^{-1} + r_{4,7}r_{4,8}^{-1}r_{8,10}^{-1}$. Thus $r_{8,10} = -r_{6,10}r_{6,9}^{-1}r_{5,9}r_{5,8}^{-1}$ and $r_{8,10}^{-1} = -r_{5,8}r_{5,9}^{-1}r_{6,9}r_{6,10}^{-1}$.

(32) According to (24) and (31) $r_{1,4} = -r_{4,8}^{-1}r_{8,10}^{-1}r_{6,10}r_{6,9}^{-1} = -r_{4,8}^{-1}(-r_{5,8}r_{5,9}^{-1}r_{6,9}r_{6,10}^{-1})r_{6,10}r_{6,9}^{-1} = r_{4,8}^{-1}r_{5,9}r_{5,9}^{-1}r_{6,9}r_{6,10}^{-1}$

(33) According to (25) and (31) $r_{6,7} = r_{4,7}r_{4,8}^{-1}r_{6,10} = r_{4,7}r_{4,8}^{-1}(-r_{5,8}r_{5,9}^{-1}r_{6,9}r_{6,10}^{-1})r_{6,10} = -r_{4,7}r_{4,8}^{-1}r_{5,8}r_{5,9}^{-1}r_{6,9}$

(34) According to (26) and (31) $r_{8,11} = -r_{6,9}r_{6,10}^{-1}r_{8,10} = -r_{6,9}r_{6,10}^{-1}(-r_{6,10}r_{6,9}^{-1}r_{5,9}r_{5,8}^{-1}) = r_{5,9}r_{5,8}^{-1}$.

(35) According to (9) $r_{5,9}r_{3,5} + r_{6,9}r_{3,6} = 0$. Thus according to (17) $r_{3,5} = -r_{5,9}^{-1}r_{6,9}r_{3,6}$.

(36) Finally according to (10) $r_{6,10}r_{3,6} + r_{8,10}r_{5,8}r_{3,5} = 0$. Combining this with (31) and (35) we get $0 = r_{6,10}r_{3,6} + r_{8,10}r_{5,8}r_{3,5} = r_{6,10}r_{3,6} + (-r_{6,10}r_{6,9}^{-1}r_{5,9}r_{5,8}^{-1})r_{5,8}(-r_{5,9}^{-1}r_{6,9}r_{3,6}) = r_{6,10}r_{3,6} + r_{6,10}r_{3,6} = 2(r_{6,10}r_{3,6}).$

(37) Multiplying (36) with $r_{3,6}^{-1}r_{6,10}^{-1}$ from the right (or from the left) we get 0 = 2.

Remark: We did not use equation (12) in this derivation. And equation (11) was only used to show each ring element r_{ij} had a two sided inverse.

Corollary IV.2. The network N in figure IV cannot be solved over any ring R (Dedekind finite) of operators that acts on analogue signals (i.e. $1 + 1 \neq 0$). The network N is solvable over any ring R that acts on digital (binary) signals (i.e. where 1 + 1 = 0).

Remark: The communication network is not a multiple unicast network (i.e. a communication network where each message is required at exactly one receiver node), however it can be shown- as explained in section XII: multiple unicast networks [13] - that it possible to modify the network so it becomes a multiple unicast networks that separate digital from analogue.

V. COMMUNICATION NETWORK THAT FAVOURS ANALOGUE SIGNALS OVER DIGITAL SIGNALS

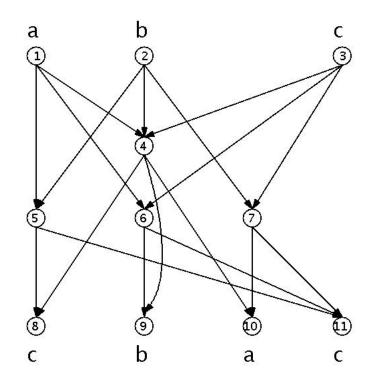


Fig. V.1.

Consider the communication network in figure V. We will show

Theorem V.1. The Network in figure V is solvable over any ring R where the element 1 + 1 is invertible. The network is not solvable over any Dedekind finite ring R where 1 + 1 fails to be invertible.

Proof: Let R be a Dedekind finite ring. Any solution over R-module (where R acts faithfully) must satisfy the following 12 equations:

- (1) Path from *a* to *a*: $r_{10,4}r_{4,1} = 1$
- (2) Path from *b* to *b*: $r_{9,4}r_{4,2} = 1$
- (3) Path from c to c_l : $r_{8,4}r_{4,3} = 1$
- (4) Paths from c to c_r : $r_{11,7}r_{7,3} + r_{11,6}r_{6,3} = 1$
- (5) Paths from a to b: $r_{9,6}r_{6,1} + r_{9,4}r_{4,1} = 0$
- (6) Paths from a to c_l : $r_{8,5}r_{5,1} + r_{8,4}r_{4,1} = 0$

- (7) Paths from a to c_r : $r_{11,6}r_{6,1} + r_{11,5}r_{5,1} = 0$
- (8) Paths from b to a: $r_{10,7}r_{7,2} + r_{10,4}r_{4,2} = 0$
- (9) Paths from b to c_l : $r_{8,5}r_{5,2} + r_{8,4}r_{4,2} = 0$
- (10) Paths from b to c_r : $r_{11,7}r_{7,2} + r_{11,5}r_{5,2} = 0$
- (11) Paths from c to a: $r_{10,7}r_{7,3} + r_{10,4}r_{4,3} = 0$
- (12) Paths from c to b: $r_{9,6}r_{6,3} + r_{9,4}r_{4,3} = 0$

We now use these equations and the fact that R is a Dedekind finite ring so having a right inverse implies having an left inverse.

- (13) $r_{10,4}$ and $r_{4,1}$ have two sided inverses (1)
- (14) $r_{9,4}$ and $r_{4,2}$ have two sided inverses (2)
- (15) $r_{8,4}$ and $r_{4,3}$ have two sided inverses (3)

(16) $r_{9,6}r_{6,1} = -r_{9,4}r_{4,1}$ according to (5) and thus using (13) and (14) we have $r_{4,1}^{-1}r_{9,4}^{-1}(-1)r_{9,6}r_{6,1} =$ 1. From this we conclude that $r_{6,1}$ has a left inverse, and thus $r_{6,1}$ has a two sided inverse.

(17) $r_{9,6}r_{6,1} = -r_{9,4}r_{4,1}$ (5) and thus using (13) and (14) $r_{9,6}r_{6,1}(-1)r_{4,1}^{-1}r_{9,4}^{-1} = 1$. From this we conclude that $r_{9,6}$ has a right inverse, and thus $r_{9,6}$ has a two sided inverse.

- (18) We conclude that $r_{8,5}$ has a two sided inverse.
- (19) We conclude that $r_{5,1}$ has a two sided inverse.
- (20) $r_{10,7}$ has a two sided inverse.
- (21) $r_{7,2}$ has a two sided inverse.
- (22) $r_{9,6}$ has a two sided inverse.
- (23) $r_{6,3}$ has a two sided inverse.

(24) According to (4), (7) and (10) and the fact $r_{6,1}$ and $r_{7,2}$ are invertible we get: $1 = (r_{11,7}r_{7,3} + r_{11,6}r_{6,3}) + (r_{11,5}r_{5,1} + r_{11,6}r_{6,1})r_{6,1}^{-1}r_{6,3} + (r_{11,5}r_{5,2} + r_{11,7}r_{7,2})r_{7,2}^{-1}r_{7,3}$

(25) By expanding (24) we get: $1 = r_{11,7}r_{7,3} + r_{11,6}r_{6,3} + r_{11,6}r_{6,1}r_{6,1}^{-1}r_{6,3} + r_{11,7}r_{7,2}r_{7,2}^{-1}r_{7,3} + r_{11,5}r_{5,1}r_{6,1}^{-1}r_{6,3} + r_{11,5}r_{5,2}r_{7,2}^{-1}r_{7,3} = 2(r_{11,7}r_{7,3} + r_{11,6}r_{6,3}) + r_{11,5}(r_{5,1}r_{6,1}^{-1}r_{6,3} + r_{5,2}r_{7,2}^{-1}r_{7,3})$

(26) $r_{6,1}^{-1} = -r_{4,1}^{-1}r_{9,4}^{-1}r_{9,6}$ according to (5) and the fact that $r_{6,1}, r_{4,1}$ and $r_{9,4}$ are invertible.

(27) $r_{7,2}^{-1} = -r_{4,2}^{-1}r_{10,4}^{-1}r_{10,7}^{-1}$ according to (8) and the fact that $r_{7,2}, r_{4,2}$ and $r_{10,4}$ are invertible.

(28) Substituting (26) and (27) into (25) gives: $1 = 2(r_{11,7}r_{7,3} + r_{11,6}r_{6,3}) + r_{11,5}(r_{5,1}(-r_{4,1}^{-1}r_{9,4}^{1}r_{9,6})r_{6,3} + r_{5,2}(-r_{4,2}^{-1}r_{10,4}^{-1}r_{10,7})r_{7,3}$

(29) According to (12) $r_{9,6}r_{6,3} = -r_{10,7}r_{7,3}$

(30) According to (11) $r_{10,7}r_{7,3} = -r_{10,4}r_{4,3}$

(31) Inserting (29) and (30) into (28) we get: $1 = 2(r_{11,7}r_{7,3} + r_{11,6}r_{6,3}) + r_{11,5}(r_{5,1}r_{4,1}^{-1}r_{9,4}r_{1,4}r_{4,3} + r_{5,2}r_{4,2}^{-1}r_{10,4}r_{10,4}r_{4,3} = 2(r_{11,7}r_{7,3} + r_{11,6}r_{6,3}) + r_{11,5}(r_{5,1}r_{4,1}^{-1} + r_{5,2}r_{4,2}^{-1})r_{4,3}$

(32) $r_{5,1} = -r_{8,5}^{-1}r_{8,4}r_{4,1}$ according to (6)

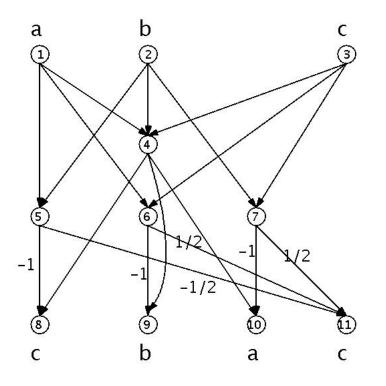
(33) $r_{5,2} = -r_{8,5}^{-1}r_{8,4}r_{4,2}$ according to (9)

(34) Substituting (32) and (33) into (31) we get $1 = 2(r_{11,7}r_{7,3} + r_{11,6}r_{6,3}) + r_{11,5}((-r_{8,5}^{-1}r_{8,4}r_{4,1}r_{4,1}^{-1} - r_{8,5}^{-1}r_{8,4}r_{4,2}r_{4,2}^{-1})r_{4,3}$

(35) Reducing (34) we finally get: $1 = 2(r_{11,7}r_{7,3} + r_{11,6}r_{6,3} - r_{11,5}r_{8,5}^{-1}r_{8,4}r_{4,3})$

This shows that if the equations (1)-(12) has a solution over a Dedekind finite ring R, 1+1=2 must be invertible in R.

On the other hand we claim that the equations (1)-(12) are solvable in any ring R where 1+1 is invertible.



A general solution that is valid over any ring R where 2 = 1 + 1 is invertible is indicated in figure V. Explicitly a solution is given by letting $r_{4,1} = r_{5,1} = r_{6,1} = r_{4,2} = r_{5,2} = r_{7,2} =$ $r_{4,3} = r_{6,3} = r_{7,3} = r_{8,4} = r_{9,4} = r_{4,10} = 1$, letting $r_{8,5} = r_{9,6} = r_{10,7} = -1$ and letting $r_{11,6} = r_{11,7} = -r_{11,5} = \frac{1}{2}$ where $\frac{1}{2}$ denote the multiplicative inverse of 2.

Corollary V.2. The network N can be solved over any ring R of operators that acts on analogue signals. The network N is unsolvable over any ring R (that is Dedekind finite) that acts on digital (binary) signals.

Proof: Assume M is a space of analogue signals (messages). We assume such signals have amplitudes (e.g. reals or complex numbers) and that we can double and half amplitudes. Thus

the space R of linear operators that contain the operator 2 (doubling the amplitude) as well as its inverse 2^{-1} (halfing the amplitude). Now, R acts faithfully so $m = 2^{-1}(m+m) = 2^{-1}2m = 1m$ and it follows that the doubling and the halving operators indeed are 2 and 2^{-1} which satisfied $2^{-1}2 = 1$.

Next assume that M is a space of digital (binary) signals. More specifically, any $b \in M$ is a string (possible infinite) of binary symbols with b + b = 0. Thus 2b = b + b = 0 for all $b \in M$, and since R acts faithfully it follows that 2 = 1 + 1 = 0 fail to be invertible.

VI. ANALYSIS OF NETWORK CAPACITY

A. Definitions and methods

In the general case where R is stably finite its not obvious that its possible to define the capacity (reciprocal to bandwidth) of a network in a proper manner. To make the definition meaningful we will strengthen the assumption on the ring R from being stably finite (or Dedekind finite) and assume that R is a finite dimensional matrix ring $GL_n(F)$ over some field F (finite or infinite). In fact we will assume R is a field, but notice that the definition of network capacity ensures that the capacity of a network with regards to a field F is the same as the capacity with regards to any finite dimensional matrix ring over F. With this restriction we can now define the capacity of a communication network as in [3].

Definition VI.1. Assume F is a field and that $k, n \in \{1, 2, 3,\}$. We say that a network has a solution that achieve capacity $\frac{k}{n}$ (or use bandwidth $\frac{n}{k}$) if there is a solution where each sender edge is assigned a $n \times k$ R-matrix (i.e. a matrix with entries in R), each edge ending in a receiver node is assigned a $k \times n$ R-matrix, and each inner edge is assigned a $n \times n$ R-matrix. The capacity of the communication network N over a field F is given by

capacity
$$(N, F) = \sup\{\frac{k}{n} : N \text{ has a solution over } F \text{ that has capacity } \frac{k}{n}\}$$

B. Simple example

Let's first consider a rather trivial example that illustrate the idea of capacity of a communication network.

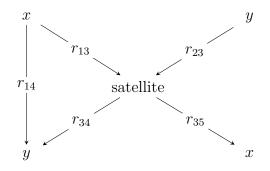


Fig. VI.1. Simple example

Proposition VI.2. The satellite communication problem in figure VI.1 has capacity $c = \frac{1}{2} = 0.5$. Equivalently, the problem can be solved if and only if the bandwidth of the communication to and from the satellite has bandwidth at least 2.

Proof: This communication has a solution of capacity $\frac{k}{n}$ if the following system (1)-(4) of matrix equations has a solution:

- (1) $r_{1,4}^{k,k} + r_{3,4}^{k,n}r_{1,3}^{n,k} = 0^{k,k}.$
- $(2) r_{3,5}^{k,n}r_{1,3}^{n,k} = 1^{k,k}.$
- (3) $r_{3,4}^{k,n}r_{2,3}^{n,k} = 1^{k,k}.$
- $(4) \quad r_{3,5}^{k,n}r_{2,3}^{n,k} = 0^{k,k}.$

For n = 2 and k = 1 we have the following solution:

$$r_{1,4}^{1,1} = \begin{bmatrix} 0 \end{bmatrix}, \quad r_{3,4}^{1,2} = \begin{bmatrix} 0 & 1 \end{bmatrix}, \quad r_{1,3}^{2,1} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad r_{3,5}^{1,2} = \begin{bmatrix} 1 & 0 \end{bmatrix}, \quad r_{2,3}^{2,1} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

This shows that $c \geq \frac{1}{2}$.

For the upper bound we proceed as follows: From (2) we conclude that

$$k = \operatorname{rank}(1^{k,k}) = \operatorname{rank}(r_{3,5}^{k,n}r_{1,3}^{n,k}) \le \min(\operatorname{rank}(r_{3,5}^{k,n}), \operatorname{rank}(r_{1,3}^{n,k}))$$

Since $k \leq n$ it follows that $\operatorname{rank}(r_{3,5}^{k,n}) \leq k$ and $\operatorname{rank}(r_{1,3}^{n,k}) \leq k$. From this we conclude that $\operatorname{rank}(r_{3,5}^{k,n}) = \operatorname{rank}(r_{1,3}^{n,k}) = k$.

From (3) we conclude that

$$k = \operatorname{rank}(1^{\mathbf{k},\mathbf{k}}) = \operatorname{rank}(r_{3,4}^{k,n}r_{2,3}^{n,k}) \le \min(\operatorname{rank}(r_{3,4}^{k,n}), \operatorname{rank}(r_{2,3}^{n,k}))$$

Since $k \leq n$ it follows that $\operatorname{rank}(r_{3,4}^{k,n}) \leq k$ and $\operatorname{rank}(r_{2,3}^{n,k}) \leq k$. From this we conclude that $\operatorname{rank}(r_{3,4}^{k,n}) = \operatorname{rank}(r_{2,3}^{n,k}) = k.$

From (4) we conclude that

$$2k - n = \operatorname{rank}(r_{3,5}^{k,n}) + \operatorname{rank}(r_{2,3}^{n,k}) - n \le \operatorname{rank}(r_{3,5}^{k,n}r_{2,3}^{n,k}) = \operatorname{rank}(0^{k,k}) = 0$$

i.e. $n \ge 2k$ and thus that $c \le \frac{1}{2}$. Notice we did not use condition (1) so the network has $c = \frac{1}{2}$ with or without an edge from node 1 to node 4.

VII. DIGITAL COMMUNICATION CAN ACHIEVE HIGHER CAPACITY THAN ANALOGUE COMMUNICATION

A. Basic considerations (digital versus analogue)

Let us revisit the communication network in figure IV. The communication network has capacity $\frac{k}{n}$ over the field F if the network has a solution where each edge from a sender mode is assigned a $n \times k$ F-matrix, each edge ending in a receiver node is assigned a $k \times n$ F-matrix, and each inner edge is assigned a $n \times n$ F-matrix. We want to lower and upper bound the capacity given by

capacity
$$(N, F) = \sup\{\frac{k}{n} : N \text{ has a solution over } F \text{ that has capacity } \frac{k}{n}\}$$

Proposition VII.1. The communication network in figure IV has capacity at least $\frac{3}{4} = 0.75$, and at most 1.

Proof (stating the problem): More specifically the network has a solution of capacity $\frac{k}{n}$ if the matrix equations (1)-(12) below can be solved simultaneously. Lower and upper bounds on the capacity of the communication network depend on the solvability of the the matrix equations (1)-(12) for various choices of k and n.

(12) paths from i_z to \bar{o}_x : $r_{8,11}^{k,n}r_{5,8}^{n,n}r_{3,5}^{n,k} + r_{3,11}^{k,k} = 0^{k,k}$

Proof (lower bound): For the lower bound we construct a solution for n = 4 and k = 3. The matrix solution was non-trivial to construct, but can be checked by hand. The main idea behind the construction was to construct a solution based on "timesharing". In the solution n represents 4 time slots, and each message is split into 3 parts. After, extensive calculations (compute checked) we found the following matrix solution that shows that the capacity of the communication network is at least $\frac{3}{4}$:

$$r_{1,4}^{4,3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad r_{1,6}^{4,3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad r_{2,4}^{4,3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad r_{2,5}^{4,3} = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad r_{2,6}^{4,3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad r_{3,3}^{4,3} = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad r_{4,7}^{4,3} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

$$r_{6,9}^{3,4} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad r_{6,10}^{3,4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}, \quad r_{8,10}^{3,4} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad r_{8,11}^{3,4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

This solution shows that the capacity of the communication network is at least $\frac{3}{4} = 0.75$. *Proof (upper bound):* The upper bound of 1 follows from the fact that each matrix ring $M_k(F)$ is Dedekind finite with $1^{k,k} + 1^{k,k} \neq 0^{k,k}$. Applying Theorem IV.1 to this fact shows that the network has no analogue solution for k = n.

VIII. ANALOGUE COMMUNICATION CAN ACHIEVE HIGHER CAPACITY THAN DIGITAL COMMUNICATION

A. Basic considerations (Analogue versus digital)

We have already seen that communication network in figure V is only solvable over Dedekind finite rings where 1 + 1 is invertible. In the section we want to quantify this difference. For the definition of capacity to be well defined we only consider the case where the underlying ring is a matrix ring $GL_{F,m}$ of $m \times m$ matrices with elements in the field F.

Proposition VIII.1. *The communication network in figure V has capacity at least* $\frac{3}{4} = 0.75$, *and at most* 1.

Proof (stating the problem):

- (1) Path from a to a: $r_{10,4}^{k,n}r_{4,1}^{n,k} = 1^{k,k}$
- (2) Path from b to b: $r_{9,4}^{k,n}r_{4,2}^{n,k} = 1^{k,k}$
- (3) Path from c to c_l : $r_{8,4}^{k,n}r_{4,3}^{n,k} = 1^{k,k}$
- (4) Paths from c to c_r : $r_{11,7}^{k,n}r_{7,3}^{n,k} + r_{11,6}^{k,n}r_{6,3}^{n,k} = 1^{k,k}$
- (5) Paths from a to b: $r_{9,6}^{k,n}r_{6,1}^{n,k} + r_{9,4}^{k,n}r_{4,1}^{n,k} = 0^{k,k}$
- (6) Paths from a to c_l : $r_{8,5}^{k,n}r_{5,1}^{n,k} + r_{8,4}^{k,n}r_{4,1}^{n,k} = 0^{k,k}$
- (7) Paths from a to c_r : $r_{11,6}^{k,n}r_{6,1}^{n,k} + r_{11,5}^{k,n}r_{5,1}^{n,k} = 0^{k,k}$
- (8) Paths from b to a: $r_{10,7}^{k,n}r_{7,2}^{n,k} + r_{10,4}^{k,n}r_{4,2}^{n,k} = 0^{k,k}$
- (9) Paths from b to c_l : $r_{8,5}^{k,n}r_{5,2}^{n,k} + r_{8,4}^{k,n}r_{4,2}^{n,k} = 0^{k,k}$
- (10) Paths from b to c_r : $r_{11,7}^{k,n}r_{7,2}^{n,k} + r_{11,5}^{k,n}r_{5,2}^{n,k} = 0^{k,k}$
- (11) Paths from c to a: $r_{10,7}^{k,n}r_{7,3}^{n,k} + r_{10,4}^{k,n}r_{4,3}^{k,n} = 0^{k,k}$

(12) Paths from c to b: $r_{9,6}^{k,n}r_{6,3}^{n,k} + r_{9,4}^{k,n}r_{4,3}^{n,k} = 0^{k,k}$

Proof (lower bound): For the lower bound we can get a solution for n = 4 and k = 3. Like in the solution in the previous section we construct the solution by "timesharing" where n represents 4 time slots, and each message is split into 3 parts. Like in the previous case by extensive computer checked calculations we found the following matrix solution that shows the capacity of the communication network over rings with 1 + 1 = 0 is at least $\frac{3}{4}$:

Proof (upper bound): The upper bound of 1 follows from the fact that each matrix ring $M_k(F)$ is Dedekind finite with $1^{k,k} + 1^{k,k} = 0^{k,k}$. Applying Theorem V.1 to this fact shows that the network has no digital solution for k = n.

IX. OPEN PROBLEMS AND CONCLUSION

A. A few specific questions

In the simple example in section VI-B we were able to provide a matching lower and upper bound. For the two main cases we considered (digital versus analogue, and analogue versus digital) there is a gap between the lower and upper bound. This naturally leads to the following questions and conjectures

Open question IX.1. *Determine the analogue capacity of the communication network in figure IV.*

Open question IX.2. Determine the digital capacity of the communication network in figure V

Conjecture IX.3. The analogue capacity of the network in figure IV is strictly less than 1.

Conjecture IX.4. The digital capacity of the network in figure V is strictly less than 1.

Open question IX.5. Considering all communication problems N where digital communication outperforms analogue communication, what is the maximal ratio $\frac{\text{digital capacity}}{\text{analogue capacity}}$

Open question IX.6. Considering all communication problems N where analogue communication outperforms digital communication, what is the maximal ratio $\frac{\text{analogue capacity}}{\text{digital capacity}}$

Conjecture IX.7. The maximal ratio in IX.5 is strictly larger than 1

Conjecture IX.8. The maximal ratio in IX.6 is strictly larger than 1

Notice that Conjecture IX.3 implies Conjecture IX.5, and that Conjecture IX.4 implies Conjecture IX.6.

B. More open ended questions

Are the digital vs analogue (analogue vs digital) network in constructed in the paper the simplest possible?

For any pair of (Dedekind finite) rings R_1 and R_2 we might ask if there exist a communication problem that is solvable over R_1 , but unsolvable over R_2 . And vise versa. In certain questions of this type the general approach developed in [2] might be useful though a lot of detains will need to be checked.

More specifically can for example the *n*th Weyl algebra be separated from the (n+1)th -Weyl algebra? Does there exists a communication problem that not is solvable over any commutative ring, but is solvable over a given non-commutative ring (e.g. the 1st Weyl algebra)? Does there exist communication problems that has a solution over some Dedekind finite ring, but has no solution over any finite ring? F

Does the class of stably finite rings precisely capture the condition that bottlenecks are well behaved? Or is it possible to impose natural requirements that impose stronger restrictions than the ring being stably finite?

One general class of questions concerns *quantum communication*, where we consider for example a module consisting of a ring of operators acting on a Hilbert space. It would be interesting to develop a general theory of quantum network communication based on our approach. Does there exist communication problems that cannot be solved classically, but has quantum mechanical solutions?

We defined the capacity of a communication networks over finitely dimension matrix rings $GL_n(F)$. Can this definition be extended to a larger class of Rings?

Finally, it would be interesting to expand the theory we developed to accommodate networks with feedback loops in the style of (non-commutative) control theory.

C. Conclusion

In the paper, we developed linear network coding over rings and modules. We showed that information bottlenecks are somewhat well behaved over Dedekind finite rings, and even more so over stably finite rings. Network coding over rings and modules seems to be a fertile area with many changeling questions that combine algebra, with problems of a graph theoretical and combinatorial flavour.

REFERENCES

- [1] H.S Black. Stabilized feedback amplifiers. Bell Syst. Tech. J., 14:1-18, 1934.
- [2] R. Dougherty and Zeger K. Freiling, C. Linear network codes and systems of polynomial equations. *IEEE Transactions* on Information Theory, (5):2303–2316, 2008.
- [3] Randall Dougherty, Chris Freiling, and Kenneth Zeger. Unachievability of network coding capacity. *IEEE Transactions* on Information Theory, 52(6):2365–2372, 2006.
- [4] M. Hall. Projective planes. Transactions Amer. Math. Soc, pages 229-277, 1943.
- [5] I. Kaplansky. Rings with a polynomial identity. Bull. Amer. Math. Soc, (6):575-580, 1948.
- [6] L. Kleinrock. Stochastic Message Flow and Delay. McGraw-Hill Book Company, New York, 1964. (Out of Print) Reprinted by Dover Publications, 1972, 1964.
- [7] L. Kleinrock. Sequential processing machines (spm) analyzed with a queueing theory model. *Journal of the ACM*, 13(2), 1966.
- [8] R Koetter and M Medard. Beyond routing: An algebraic approach to network coding. In *Proceedings of the 2002 IEEE Infocom*, 2002.
- [9] T.Y Lam. Exercises in Modules and Rings. Springer-Verlag, 2007.
- [10] S.J. Mason. Feedback theory some properties of signal flow graphs. Proceedings of IRE, 64:1144–1156, 1953.
- [11] H. Nyquist. Regeneration theory. Bell Syst. Tech. J., 11:126-147, 1932.
- [12] S. Riis. Linear versus non-linear boolean functions in network flow. In Proceeding of CISS 2004.
- [13] S Riis. Utilising public information in network coding. In General Theory of Information Transfer and Combinatorics, volume 4123 of Lecture Notes in Computer Science, pages 866–897, 2006.
- [14] S. Riis. Reversible and irreversible information networks. *IEEE Transactions on Information Theory*, (11):4339–4349, 2007.
- [15] S. Riis and R Ahlswede. Problems in network coding and error correcting codes. NetCod 2005.
- [16] Yeung and Zhang. Distributed source coding for satellite communications. *IEEE Transactions on Information Theory*, (IT-45):1111–1120, 1999.
- [17] R W Yeung. Multilevel diversity coding with distortion. *IEEE Transactions on Information Thory*, 41:412–422, March 1995.