

EE 520: Topics in Communications: Network Coding

August 22, 2007

Scribe: Aditya Ramamoorthy

Lecture 1**1 Introduction**

Network coding is a relatively new research area at the intersection of networking and information theory. The basic idea of network coding is to allow nodes in a network to compute functions of their incoming packets before transmitting them further. Thus, it is more general than routing which is currently the dominant network information transfer paradigm. It turns out that the use of network coding can provably improve network throughput and robustness. In this course we shall study the basics of network coding theory and its applications. In this lecture we overview the basic model of communication network that we shall be working with and some examples that demonstrate the power of network coding.

2 Model of a communication network

In this course a communication network shall be modeled as a finite directed graph $G = (V, E)$ where V is a set of vertices (or nodes) and E is a set of directed edges. Sometimes we shall use the term channel instead of edge. We shall also typically assume that each edge in the network can carry one data unit per unit time (we shall call it a unit capacity edge). The data unit could be a bit or a packet consisting of several bytes. If an edge has higher capacity then it is modeled by introducing multiple edges of unit capacity. A network is called *acyclic* when it does not have any directed cycles. As we shall see later on in the course working with directed acyclic graphs somewhat simplifies the operation of a network code.

The nodes that inject messages into the network shall be called sources and the set of sources shall typically be denoted by S . Similarly the nodes that request the messages shall be called terminals and the set of terminals shall typically be denoted by T . Our convention shall be to assume that there are no incoming edges into the sources and no outgoing edges from the terminals. the questions that we seek to address in this class shall revolve around whether we can satisfy the demands of the terminals for a given network, whether we can do it under certain resource constraints, whether we can do it in a distributed manner etc. We shall now demonstrate the power of network coding via some examples.

3 Illustrative Examples

Consider the network shown in Fig. 1 with source node S and terminal nodes T_1 and T_2 . All edges have a capacity of one bit per unit time. The node S generates two bits per unit time and the terminals T_1 and T_2 want to receive these two bits per unit time.

Two important points need to be noted. Both T_1 and T_2 have exactly two incoming edges, so they can receive information at a maximum of 2 bits/unit time. Next, the labeling demonstrated in Fig. 1 shows a means by which the terminals can actually receive information at 2 bits/unit time.

Each node in the network operates in a *replicate and forward* mode. In this course this mode of operation shall be called a routing mode. Thus, in this case routing is optimal.

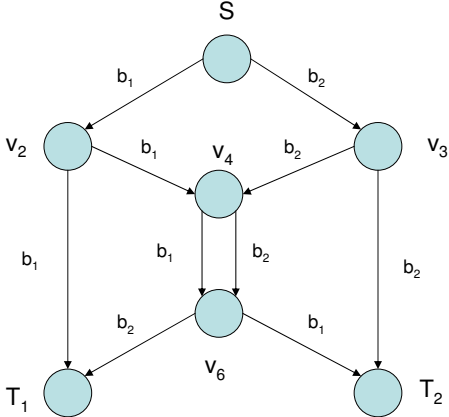


Figure 1: Routing suffices to achieve the maximum simultaneous throughput possible.

Now consider the network shown in Fig. 2(a). In this case there is only one edge between v_4 and v_6 . In in a given time slot the edge $v_4 \rightarrow v_6$ can either carry b_1 or b_2 . Thus, the simultaneous rate of transfer to both T_1 and T_2 has to be strictly less than 2 bits/unit time.

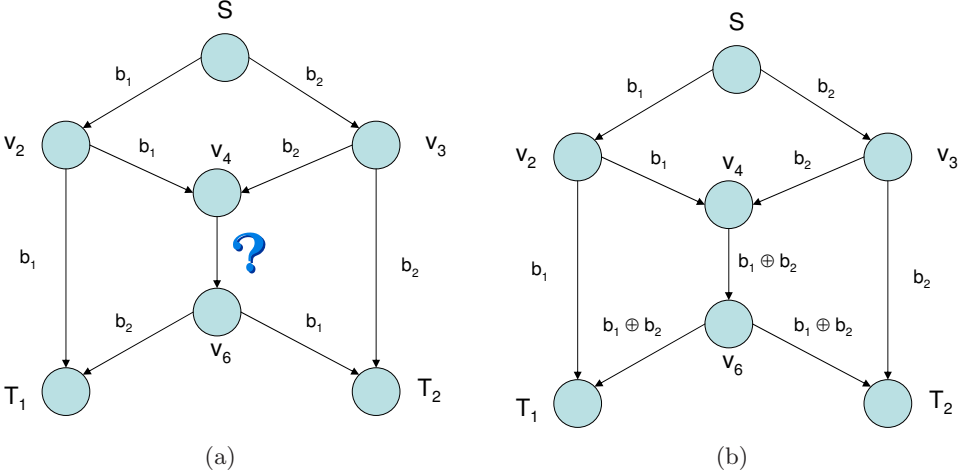


Figure 2: (a) Under a routing solution edge $v_4 \rightarrow v_6$ can either transmit b_1 or b_2 . (b) Allowing network coding results in an optimal solution.

However there is a simple solution to this problem. As demonstrated in Fig. 2(b) one can simply transmit $b_1 \oplus b_2$ on edge $v_4 \rightarrow v_6$ instead of either b_1 or b_2 . Note that since $b_1 \oplus (b_1 \oplus b_2) = b_2$, terminal T_1 can recover b_2 , since it receives b_1 on edge $v_2 \rightarrow T_1$. This network is referred to as the butterfly network and was first introduced in the seminal paper of Ahlswede et al.

We now consider an example from wireless networks. Consider three wireless base stations X, Y and Z that have equal transmission power as shown in Fig. 3 such that

- X and Z are at a distance which is twice the wireless transmission range.
- Both X and Z are within the transmission range of Y .

Suppose that X and Z want to exchange a bit of information. Note that the wireless medium has a broadcast nature. We assume that as long as a receiver node is within the transmission range of a transmitter node and there are no collisions i.e. no other simultaneous transmissions take place within its range, the transmission is successful. Conversely, if there is a collision when the transmission takes place the transmission is deemed unsuccessful. Fig. 3 shows a strategy by which bits can be exchanged between X and Z within three time slots. It is easy to verify that a solution that operates without any coding shall require at least four time slots. Finally we conclude with

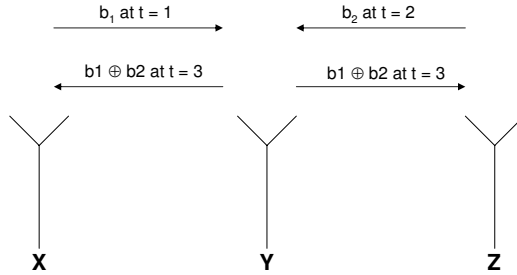


Figure 3: A solution based on network coding for information exchange between base stations X and Z .

an example from network security. Consider the network shown in Fig. 4(a) and suppose that A (Alice) wants to transmit at 2 data units/unit time to B (Bob). For this example think about the data units as elements of a finite field or even real numbers. Under a routing solution as shown in the labeling in Fig. 4(a) Alice transmits b_1 along the path $A \rightarrow v_1 \rightarrow B$ and b_2 along $A \rightarrow v_2 \rightarrow B$. If a wiretapper (Eve) has access to any of one the edges in the network then she knows at least half of the useful information being communicated from Alice to Bob.

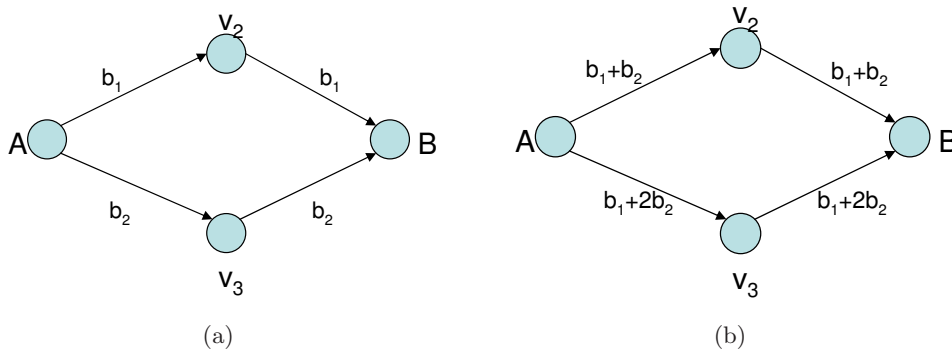


Figure 4: (a) Tapping one edge results in half the information being compromised when routing is used. (b) No single edge can provide any useful information when the information is coded.

On the other hand if the data is coded by Alice as shown in Fig. 4(b), then it is clear that by tapping one edge, Eve only has access to a linear combination of the data units b_1 and b_2 (either $b_1 + b_2$ or $b_1 + 2b_2$) and has no way of uniquely recovering either b_1 or b_2 . Thus, in this case coding is useful from the point of view of security.