

**EE 520: Topics in Communications: Network Coding**

Sept. 7, 2007

Scribe: Mohammad Fraiwan

**Lecture 4**

We saw the proof of the maximum flow minimum cut algorithm in the previous lecture. In this lecture we show that it is possible to find a set of disjoint paths corresponding to the maximum flow. We also introduce finite fields.

**1 Disjoint Paths In Directed Graphs**

Consider a directed graph  $G$  with unit capacity edges and suppose that the maximum flow from  $s$  to  $t$  is  $k$ . It turns out that we can show that there exist  $k$  edge-disjoint paths from  $s$  to  $t$ .

**Definition 1** *Edge-disjoint paths.* A set of paths is said to be edge disjoint if no edge is common between any two paths.

**Lemma 1** Consider a directed graph  $G$  with unit capacity edges, a source node  $s$  and a terminal node  $t$ . If there are  $k$  edge-disjoint paths from  $s$  to  $t$  then the  $s - t$  maximum flow  $\geq k$ .

*Proof.* Let the set of paths be  $S_p = \{p_1, p_2, \dots, p_n\}$ . Assign  $f(e) = 1$ , if edge  $e$  participates in any path, then obviously that the flow is valid. Clearly this is a flow of value  $k$ . ■

Next, we show that if there exists a flow of value  $k$  in  $G$ , then there exists  $k$  edge-disjoint paths from  $s$  to  $t$ .

**Lemma 2** Consider a directed graph  $G$  with unit capacity edges, a source node  $s$  and a terminal node  $t$ . If  $f$  is a  $0 - 1$  valued flow of value  $\nu$ , then the set of edges with flow value  $f(e) = 1$  contains a set of  $\nu$  edge disjoint paths. (Note: unit-capacity edges  $\Rightarrow$  that flow's value can either be 0 or 1).

*Proof:* Use induction on the number of edges in  $f$  that have flows assigned to be 1.

a) Base case.

Suppose the number of edges carry flow = 1 is zero. In this case  $\nu = 0$  and there is nothing to prove. The statement of the lemma is trivially true.

b) Induction step.

Assume the induction hypothesis i.e. that the lemma is true when the number of edges carrying flow =1 is less than or equal to  $N \geq 1$ . Now we show that the lemma is true in the case when the number of edges carrying flow =1 is  $N + 1$ . Suppose that in this case we denote the flow  $\nu$  and note that  $\nu$  has to be greater than 1. We shall construct a list of edge disjoint paths of size  $\nu$ .

This implies that there exists an edge  $(s, v)$  that has flow =1, and since flow conservation needs to hold at  $v$ , there is an edge  $(v, u)$  with flow = 1. Continuing this process we can construct a path from  $s$ . One of two things can happen.

1. Case 1: We reach  $t$  before visiting any other node more than once.  
 In this case we have found one path from  $s$  to  $t$ , let this path be  $P$ . Add  $P$  to the list of paths. Next, assign the flow on all edges in  $P$  the value 0. The new flow value is  $\nu - 1$  and the number of edges in  $G$  carrying flow =1 has strictly decreased i.e. it is strictly less than  $N + 1$ . Now, use induction hypothesis to obtain the required result.
2. Case 2: We visit a node on the path again.  
 An example is demonstrated in Fig. 1. Let the node that is visited again be denoted  $u$ . Let  $Cyc = \{\text{set of edges visited in between two visits to } u\}$ . We claim that setting the flow value on edges in  $Cyc$  to zero continues to maintain a valid flow. This is true since a directed cycle has one edge going in and one edge going out of a node. Thus reducing the flow on the edges by 1 continues to maintain a valid flow. Note that this does not reduce the flow since there are no cycles in which  $s$  participates in i.e. the value of the flow is still  $\nu$ . Now, the number of edges in  $G$  carrying flow =1 has strictly decreased to less than  $N + 1$  and we can use induction hypothesis to obtain the result. Fig. 1 shows the second case of the proof. The loop is entered at node  $u$ , and the list of visited edges in the loop is  $\{uv, vw, wx, xu\}$ . Setting the flow value at these edges will not reduce the  $\nu$ , because the flow did not change at  $su$ . ■

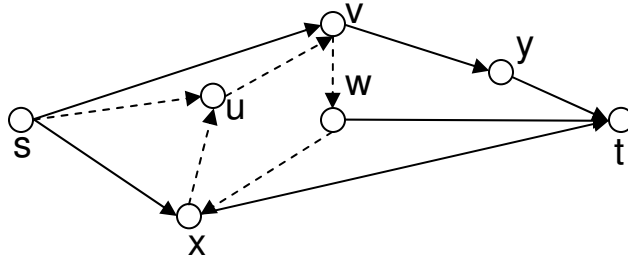


Figure 1: The second case of the proof. All edges are assigned flow =1. The dotted edges represent the path formed by visiting nodes starting at  $s$ .

In summary we have shown the following result.

**Theorem 3** *There are  $k$  edge disjoint paths in a directed graph  $G$  with unit capacities from  $s$  to  $t$  if and only if the value of the maximum flow from  $s$  to  $t$  is at least  $k$ .*

The preceding discussion has been in the context of unit capacity edges. It is easy to see that the case when edges have higher capacity can be treated similarly. Fig. 2 shows how we can deal with edges having capacity  $> 1$ . In this figure, we introduce two nodes  $uv^1$  and  $uv^2$ . Edge  $uv$  is replaced by two unit capacity paths  $u - uv^1 - v$ , and  $u - uv^2 - v$ .

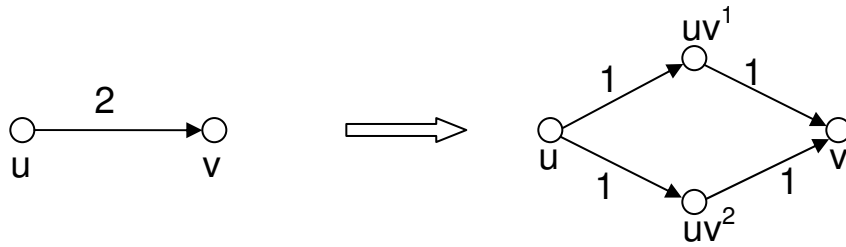


Figure 2: Transforming an edge with a capacity of 2 into unit capacity edges.

## 2 Finite Fields

**Definition 2** *Group.* A group is a set along with a binary operation  $+$ , such that the following properties hold:

1. *Closure:* if  $a, b \in G$  then  $a + b \in G$ .
2. *Associativity:*  $(a + b) + c = a + (b + c)$ .
3. *Identity (existence):*  $\exists$  element  $e \in G$  such that  $a + e = a$  for all  $a \in G$ .
4. *Inverse:* For all  $a \in G, \exists a^{-1} \in G$  such that  $a + a^{-1} = e$ .

A group is called commutative (Abelian) if  $a + b = b + a$ . Some examples of groups are given below.

- a) The set of integers with integer addition.
- b) The set of integers  $\{0, 1, \dots, m - 1\}$  under modulo  $m$  addition.
- c) The set of integers  $\{1, 2, \dots, p - 1\}$  under modulo  $p$  multiplication if  $p$  is a prime.

In this class we shall almost exclusively be working with fields. Roughly a field is a set with two binary operations  $+$  (addition) and  $\cdot$  (multiplication), such that we can perform addition, multiplication, and division without leaving the set. The operations satisfy commutativity, associativity, and distributivity.

**Definition 3** *Field.* Let  $F$  be a set of elements in which two binary operations are defined  $+$ , and  $\cdot$ .  $F$  is a field if:

1.  $F$  is an Abelian group under addition. The identity element is denoted by 0.
2. The set of non-zero elements form an Abelian group under multiplication. The identity element here is denoted by 1.
3. Multiplication distributes over addition. i.e.

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Common examples of fields include

- The set of real numbers  $\mathbb{R}$  under real addition and multiplication.
- The set of complex numbers  $\mathbb{C}$  under complex addition and multiplication.

In this class we shall almost exclusively be concerned with finite fields. A simple example is the binary field  $F = \{0, 1\}$ , also known as Galois field  $GF(2)$  (in honor of Evariste Galois who first showed their existence) under binary multiplication and addition. Fig. 3 shows the multiplication and addition tables.

<b>+</b>	<b>0</b>	<b>1</b>
<b>0</b>	<b>0</b>	<b>1</b>
<b>1</b>	<b>1</b>	<b>0</b>

<b>.</b>	<b>0</b>	<b>1</b>
<b>0</b>	<b>0</b>	<b>0</b>
<b>1</b>	<b>0</b>	<b>1</b>

Figure 3: The addition and multiplication tables for  $GF(2)$ .

We can work with elements of a finite field almost exactly as we would with real numbers. Another example is the following.

1. The set  $\{0, 1, 2, \dots, p - 1\}$  under modulo  $p$  addition and multiplication when  $p$  is a prime. Note that if  $p$  is not prime, then this is not a field. To see this consider modulo 4 addition and multiplication. Here we have  $(2 + 2) \bmod 4 = 0$  i.e. adding two non-zero elements results in a zero).

It is possible to show that finite fields exist only for sizes  $p$  (where  $p$  is prime), or  $p^m$ , where  $m \geq 1$ .  $GF(p^m)$  is called the extension field of  $GF(p)$ . We now show how one can extend a finite field. The discussion here is not particularly rigorous. It just serves as an intuitive justification of the process.

Consider how the real numbers are extended to the complex numbers. We pick an equation that has no solution over the reals e.g.  $x^2 + 1 = 0$ . Suppose that we call the solution of this equation  $i$  and add it to the field. Now, we can generate more elements such as  $a + ib$ , where  $a, b \in \mathbb{R}$  by addition and multiplication. This process can be continued. However we shall always reduce the final expression modulo the fact that  $i^2 + 1 = 0$ . e.g.  $a + ib + i^2c + i^3d = a + ib - c - id = (a - c) + i(b - d)$ . It turns out that the new field that is generated this way is the complex field and every element here can be represented in the form  $x + iy$  where  $x, y \in \mathbb{R}$ .

*The main idea here is to find a equation with no solution over the current field, assume a solution to that equation, augment the field with that solution, generate new expressions and reduce these expressions modulo the original equation .*

We now demonstrate how we can construct a finite field with four elements using this procedure. Note that  $2^2 = 4$  i.e. the field with four elements can be formed by extending  $GF(2)$ .

- First we pick an equation that has no solution in  $GF(2)$  e.g.  $z^2 + z + 1 = 0$ .
- Call  $x$  to be the solution to the above equation and add  $x$  to the field and start forming new expressions by addition and multiplication.

- Note that these expressions are polynomials in  $x$  with coefficients from  $GF(2)$ . Now we reduce the polynomial (say  $p(x)$ ) modulo the fact that  $x^2 + x + 1 = 0$ , as follows. we first divide  $p(x)$  by  $x^2 + x + 1$  to obtain

$$p(x) = q(x)(x^2 + x + 1) + r(x) \text{ where } \deg(r(x)) < 2$$

Next since  $x^2 + x + 1 = 0$  it means that the above expression equals  $r(x)$  modulo  $x^2 + x + 1$ . Now, add  $r(x)$  to the field. Note that since  $r(x)$  is the remainder its degree has to be  $\leq 1$ .

It should be clear that the elements in the field that are formed this way are  $\{0, 1, x, x + 1\}$  since the remainder has to be of degree at most 1.

This is the construction of  $GF(4)$  i.e. it consists of the set  $\{0, 1, x, x + 1\}$  under addition and multiplication modulo  $x^2 + x + 1$ . (i.e., all the elements of the form  $b_1 + b_2x$ , where  $b_1, b_2 \in GF(2)$ ). In a similar manner we can construct  $GF(2^3)$  by using the polynomial  $x^3 + x + 1 = 0$ . The polynomials that are used for reduction are called *irreducible polynomials* and their existence can be shown for any degree.

This concludes our brief introduction to finite fields. The important lesson to take away is that finite fields exist only for prime powers and we can for all practical purposes perform all mathematical operations that we do in the reals such addition, multiplication, division, solving linear equations etc. in them. More in-depth material in finite fields can be found in a variety of texts.