Introduction to Network Coding, Bounds and Constructions

Lecture 5

Algebraic Approach for Network Coding

Tuvi Etzion
Algebraic Approach

Outline

Algebraic representation for network coding

Multicasting is solvable with network coding

Linear information flow algorithm
Multicast with Network Coding

Fragouli, Soljanin 2006
Multicast with Network Coding
Multicast with Network Coding
Multicast with Network Coding

\[ x, y \]

\[ S \rightarrow A, B, C \]
\[ A \rightarrow R_2, B \]
\[ B \rightarrow D, E \]
\[ C \rightarrow R_1 \]
\[ R_2 \rightarrow F \]
\[ R_1 \rightarrow R_3 \]
\[ D \rightarrow R_1 \]
\[ E \rightarrow R_3 \]
Multicast with Network Coding
Multicast with Network Coding

\[
\begin{pmatrix}
1 & 0 \\
\alpha_3 + \alpha_1 \alpha_4 & \alpha_2 \alpha_4
\end{pmatrix}
\]

\[
\begin{pmatrix}
\alpha_1 x + \alpha_2 y \\
\alpha_1 x + \alpha_2 y
\end{pmatrix}
\]

\[
\begin{pmatrix}
0 & 1 \\
\alpha_1 & \alpha_2
\end{pmatrix}
\]

\[
\begin{pmatrix}
\alpha_1 \\
\alpha_3 + \alpha_1 \alpha_4 \\
\alpha_2 \alpha_4
\end{pmatrix}
\]
The source $S$ has $h$ messages, $X^t = (x_1, x_2, ..., x_h)$. There are $N$ receivers $R_1, R_2, ..., R_N$ each one demands all the $h$ messages.

Can all the messages be received simultaneously by receiver $R_j$?

Yes, if

- The min-cut between $S$ and $R_j$ has size at least $h$.
- There are $h$ edge-disjoint paths between $S$ and $R_j$. 

OR
Can all the messages be received simultaneously by all receivers?

Yes, if each node can re-encode the information.

Edges carry linear combinations of their parent node inputs, where \( \{\alpha_i\} \) are the coefficients used in these linear combinations.

Edges carry linear combinations of the \( h \) messages.
Edges carry linear combinations of their parent node inputs, where \( \{\alpha_i\} \) are the coefficients used in these linear combinations.

The coefficients of the given edge form the local coding vector.

Edges carry linear combinations of the \( h \) messages.

The coefficients of these linear combinations form the global coding vector.
Let $y_j^i$ be the symbol on the last edge in the path from node $S_i$ to the receiver $R_j$.

Let $c_1(e), c_2(e), ..., c_h(e)$ be the coefficients of $x_1, x_2, ..., x_h$ in the linear combination on the edge $e$, i.e., if $y$ is the symbol computed on the edge $e$ then

$$y = c_1(e) \cdot x_1 + c_2(e) \cdot x_2 + \cdots + c_h(e) \cdot x_h$$

or

$$y = (c_1(e), c_2(e), ..., c_h(e)) \cdot X.$$

$(c_1(e), c_2(e), ..., c_h(e))$ is the global coding vector of the edge $e$. 
Let $c^j_i$ be the global coding vector on the last edge in the path from node $S_i$ to the receiver $R_j$.

Let $C_j$ be the $h \times h$ matrix whose $i$th row is $c^j_i$.

$C_j$ is the transfer matrix of receiver $R_j$.

Receiver $R_j$ has to solve the system of equations

$$Y_j = C_j \cdot X,$$

where

$$Y_j = (y^j_1, y^j_2, ..., y^j_h)^t.$$
Receiver $R_j$ has to solve the system of equations

$$Y_j = C_j \cdot X,$$

where $Y_j = (y_1^j, y_2^j, ..., y_h^j)^t$.

How can we make sure that each receiver will compute the right messages?

The matrices $C_1, C_2, ..., C_N$ must be of full rank.

Select coefficients $\{\alpha_i\}$ such that

$$f(\{\alpha_i\}) \triangleq \det(C_1) \cdot \det(C_2) \cdots \det(C_N) \neq 0.$$
Let $f(z_1, z_2, \ldots, z_\eta)$ be a polynomial over $\mathbb{F}_q$ such that the maximum degree of each variable in a term of $f(z_1, z_2, \ldots, z_\eta)$ is at most $d$. Let $A$ be a set of $d + 1$ distinct elements of $\mathbb{F}_q$. If $f(a_1, a_2, \ldots, a_\eta) = 0$ for all $\eta$-tuples in $A^n$, then $f$ is identically the zero polynomial.
The proof is by induction on $\eta$. For $\eta = 1$, $f$ is a polynomial in a single variable of degree at most $d$ and hence it can have at most $d$ zeros. Suppose that for some $\eta \geq 1$ the claim is true for all such polynomials. Let $f(z_1, z_2, ..., z_\eta, z_{\eta+1})$ such polynomial. It can be written as

$$f(z_1, ..., z_\eta, z_{\eta+1}) = \sum_{i=0}^{d} f_i(z_1, ..., z_\eta)z_{\eta+1}^i$$

where $f_i$ are polynomials with degrees bounded by $d$. 
Suppose \( f(z_1, ..., z_\eta, z_{\eta+1}) = 0 \) for all \((\eta + 1)\)-tuples in \( A^{\eta+1} \). Then each polynomial \( f(a_1, ..., a_\eta, z_{\eta+1}) \) in \( z_{\eta+1} \) (fixing \((a_1, ..., a_\eta)\)) has at least \( d + 1 \) zeros, and hence must be identically zero. Therefore, \( f_i(a_1, ..., a_\eta) = 0 \) for all \((a_1, ..., a_\eta) \in A^\eta\). By the assumption each such \( f_i \) must be identically zero polynomial which implies that \( f \) is identically zero.
Introduction to Network Coding, Bounds and Constructions

A SHORT BREAK
Sparse Zeroes Lemma

Let \( f(z_1, z_2, ..., z_\eta) \) be a polynomial over \( \mathbb{F}_q \) such that

- \( f(z_1, z_2, ..., z_\eta) \) is not identically zero;
- The maximum degree of each variable in a term of \( f(z_1, z_2, ..., z_\eta) \) is at most \( d \);
- \( q > d \).

Then, there exist values \( b_1, b_2, ..., b_\eta \in \mathbb{F}_q \) such that

\[
 f(b_1, b_2, ..., b_\eta) \neq 0.
\]
$f(z_1, z_2, \ldots, z_\eta)$ is a polynomial over $\mathbb{F}_q$, where

- $f(z_1, z_2, \ldots, z_\eta)$ is not identically zero;
- The sum of degrees of all the variables in a term of $f(z_1, z_2, \ldots, z_\eta)$ is at most $d$;
- $q > d$.

There exist values $b_1, b_2, \ldots, b_\eta \in \mathbb{F}_q$ such that

$$f(b_1, b_2, \ldots, b_\eta) \neq 0.$$ 

**Why not any field?**

The polynomial

$$x(x + 1) + x + x^2$$

is identically zero over $\mathbb{F}_2$.

The polynomial

$$x(x - \alpha^0)(x - \alpha^1) \cdots (x - \alpha^{q-2})$$

$\alpha$ primitive, evaluated to zero on all elements of $\mathbb{F}_q$. 
A multicast network is solvable if and only if the min-cut for each receiver is at least the number of messages.

A network with $h$ sources, where each one has exactly one message, is solvable if and only if the min-cut to each receiver is at least $h$. 
The theorem does not hold for undirected graphs.
Algebraic Approach

Three inputs

\[ \mathbf{z} = \mathbf{x} \cdot \mathbf{M} \]

\( \mathbf{M} \) - transfer matrix

\[ \begin{align*}
Y(e_1) &= \alpha_{1,e_1} X(v, 1) + \alpha_{2,e_1} X(v, 2) + \alpha_{3,e_1} X(v, 3) \\
Y(e_2) &= \alpha_{1,e_2} X(v, 1) + \alpha_{2,e_2} X(v, 2) + \alpha_{3,e_2} X(v, 3) \\
Y(e_3) &= \alpha_{1,e_3} X(v, 1) + \alpha_{2,e_3} X(v, 2) + \alpha_{3,e_3} X(v, 3) \\
Y(e_4) &= \beta_{e_1,e_4} Y(e_1) + \beta_{e_2,e_4} Y(e_2) \\
Y(e_5) &= \beta_{e_1,e_5} Y(e_1) + \beta_{e_2,e_5} Y(e_2) \\
Y(e_6) &= \beta_{e_3,e_6} Y(e_3) + \beta_{e_4,e_6} Y(e_4) \\
Y(e_7) &= \beta_{e_3,e_7} Y(e_3) + \beta_{e_4,e_7} Y(e_4) \\
Z(v', 1) &= \varepsilon_{e_5,1} Y(e_5) + \varepsilon_{e_6,1} Y(e_6) + \varepsilon_{e_7,1} Y(e_7) \\
Z(v', 2) &= \varepsilon_{e_5,2} Y(e_5) + \varepsilon_{e_6,2} Y(e_6) + \varepsilon_{e_7,2} Y(e_7) \\
Z(v', 3) &= \varepsilon_{e_5,3} Y(e_5) + \varepsilon_{e_6,3} Y(e_6) + \varepsilon_{e_7,3} Y(e_7).
\]
Algebraic Approach

\[ Y(e_1) = \alpha_{1,e_1} X(v, 1) + \alpha_{2,e_1} X(v, 2) + \alpha_{3,e_1} X(v, 3) \]
\[ Y(e_2) = \alpha_{1,e_2} X(v, 1) + \alpha_{2,e_2} X(v, 2) + \alpha_{3,e_2} X(v, 3) \]
\[ Y(e_3) = \alpha_{1,e_3} X(v, 1) + \alpha_{2,e_3} X(v, 2) + \alpha_{3,e_3} X(v, 3) \]
\[ Y(e_4) = \beta_{e_1,e_4} Y(e_1) + \beta_{e_2,e_4} Y(e_2) \]
\[ Y(e_5) = \beta_{e_1,e_5} Y(e_1) + \beta_{e_2,e_5} Y(e_2) \]
\[ Y(e_6) = \beta_{e_3,e_6} Y(e_3) + \beta_{e_4,e_6} Y(e_4) \]
\[ Y(e_7) = \beta_{e_3,e_7} Y(e_3) + \beta_{e_4,e_7} Y(e_4) \]
\[ Z(v', 1) = \varepsilon_{e_5,1} Y(e_5) + \varepsilon_{e_6,1} Y(e_6) + \varepsilon_{e_7,1} Y(e_7) \]
\[ Z(v', 2) = \varepsilon_{e_5,2} Y(e_5) + \varepsilon_{e_6,2} Y(e_6) + \varepsilon_{e_7,2} Y(e_7) \]
\[ Z(v', 3) = \varepsilon_{e_5,3} Y(e_5) + \varepsilon_{e_6,3} Y(e_6) + \varepsilon_{e_7,3} Y(e_7) \]

\[ z = x \cdot M \]

\[
A = \begin{pmatrix}
\alpha_{1,e_1} & \alpha_{1,e_2} & \alpha_{1,e_3} \\
\alpha_{2,e_1} & \alpha_{2,e_2} & \alpha_{2,e_3} \\
\alpha_{3,e_1} & \alpha_{3,e_2} & \alpha_{3,e_3}
\end{pmatrix}
\]

\[
B = \begin{pmatrix}
\varepsilon_{e_5,1} & \varepsilon_{e_5,2} & \varepsilon_{e_5,3} \\
\varepsilon_{e_6,1} & \varepsilon_{e_6,2} & \varepsilon_{e_6,3} \\
\varepsilon_{e_7,1} & \varepsilon_{e_7,2} & \varepsilon_{e_7,3}
\end{pmatrix}
\]

\[
M = \begin{pmatrix}
\beta_{e_1,e_5} & \beta_{e_1,e_4} \beta_{e_4,e_6} & \beta_{e_1,e_4} \beta_{e_4,e_7} \\
\beta_{e_2,e_5} & \beta_{e_2,e_4} \beta_{e_4,e_6} & \beta_{e_2,e_4} \beta_{e_4,e_7} \\
0 & \beta_{e_3,e_6} & \beta_{e_3,e_7}
\end{pmatrix} B^T
\]
Algebraic Approach

\[ Y(e_1) = \alpha_{1,e_1}X(v,1) + \alpha_{2,e_1}X(v,2) + \alpha_{3,e_1}X(v,3) \]
\[ Y(e_2) = \alpha_{1,e_2}X(v,1) + \alpha_{2,e_2}X(v,2) + \alpha_{3,e_2}X(v,3) \]
\[ Y(e_3) = \alpha_{1,e_3}X(v,1) + \alpha_{2,e_3}X(v,2) + \alpha_{3,e_3}X(v,3) \]
\[ Y(e_4) = \beta_{e_1,e_4}Y(e_1) + \beta_{e_2,e_4}Y(e_2) \]
\[ Y(e_5) = \beta_{e_1,e_5}Y(e_1) + \beta_{e_2,e_5}Y(e_2) \]
\[ Y(e_6) = \beta_{e_3,e_6}Y(e_3) + \beta_{e_4,e_6}Y(e_4) \]
\[ Y(e_7) = \beta_{e_3,e_7}Y(e_3) + \beta_{e_4,e_7}Y(e_4) \]
\[ Z(v',1) = \varepsilon_{e_5,1}Y(e_5) + \varepsilon_{e_6,1}Y(e_6) + \varepsilon_{e_7,1}Y(e_7) \]
\[ Z(v',2) = \varepsilon_{e_5,2}Y(e_5) + \varepsilon_{e_6,2}Y(e_6) + \varepsilon_{e_7,2}Y(e_7) \]
\[ Z(v',3) = \varepsilon_{e_5,3}Y(e_5) + \varepsilon_{e_6,3}Y(e_6) + \varepsilon_{e_7,3}Y(e_7) \]

\[ z = x \cdot M \]

\[ M = A \cdot C \cdot B^T \]

\[ C \text{ forms the combination of } e_5, e_6, e_7 \text{ as functions of } e_1, e_2, e_3. \]
A network $G = (V, E)$ with $h$ sources $S_1, \ldots, S_h \in V$ and $N$ receivers $R_1, \ldots, R_N \in V$. Each source has one message and each receiver demands all the messages.

Remove each edge which will not disconnect a source-receiver pair. The new subgraph is a minimal multicast subgraph of $G$; assume $G$ is minimal.
Linear Information Flow Algorithm

Find $h$ edge-disjoint paths

\{ $(S_i, R_j) : 1 \leq i \leq h$ \} in the network $G$

to each receiver $R_j, 1 \leq j \leq N$.

A coding point is an edge where a path $(S_i, R_j)$
merges with $(S_\ell, R_m)$, where $i \neq \ell$ and $j \neq m$.

$i = \ell$ same information on paths

$j = m$ paths to receiver not edge-disjoint
Let $R(\delta)$ be the set of all receivers which have a path with coding point $\delta$.

Each coding point $\delta$ appears in at most one path $(S_i, R_j)$ for $R_j$ ($h$ disjoint paths to $R_j$).

Let $f_j^i(\delta)$ denote the predecessor coding point to $\delta$ along the path $(S_i, R_j)$. 

Find $h$ edge-disjoint paths $\{ (S_i, R_j) : 1 \leq i \leq h \}$ in the network $G$ to each receiver.
For $R_j$ the algorithm maintain a set $P_j$ of last visited $h$ coding points and a set $B_j = \{c^j_1, ..., c^j_h\}$ of the $h$ global coding vectors.

Initially $P_j$ contains the source nodes and $B_j$ contains the unity vectors.

$B_j$ must contain $h$ linearly independent vectors.
The network is scanned in a way that an edge is scanned only after all the incoming edges of its parent node were scanned.

At step $k$, the algorithm assigns a coding vector $c(\delta_k)$ to the coding point $\delta_k$, and replaces for each $R_j \in R(\delta_k)$:

- the associated vector $c(f^j_{\leftarrow}(\delta_k))$ in $B_j$ with $c(\delta_k)$.
- the point $f^j_{\leftarrow}(\delta_k)$ in $P_j$ with the point $\delta_k$. 

Linear Information Flow Algorithm
The algorithm selects the vector $c(\delta_k)$ in a way that for every receiver $R_j \in R(\delta_k)$ the set 
\[
\left( B_j \setminus \{c\left(f_j^i(\delta_k)\right)\} \right) \cup \{c(\delta_k)\}
\]
form a basis for the $h$-dimensional space.

Such a choice always exists provides that the field $\mathbb{F}_q$ has size $q > N$.

When the algorithm terminates $B_j$ contains the set of linearly independent equations for $R_j$. 
Consider a coding point $\delta$ with $m \leq h$ parents and a receiver $R_j \in R(\delta)$. Let $V(\delta)$ be the $m$-dimensional subspace spanned by the coding vectors of the parents of $\delta$, and $V(R_j, \delta)$ be the $(h - 1)$-dimensional subspace spanned by the elements of $B_j$ after removing $c(f^j_\leftarrow(\delta))$. Then
\[
\dim\{V(\delta) \cap V(R_j, \delta)\} = m - 1.
\]
Consider a coding point $\delta$ with $m \leq h$ parents and a receiver $R_j \in R(\delta)$. Let $V(\delta)$ be the $m$-dimensional subspace spanned by the coding vectors of the parents of $\delta$, and $V(R_j, \delta)$ be the $(h - 1)$-dimensional subspace spanned by the elements of $B_j$ after removing $c(f^j_{\leftarrow}(\delta))$. Then

$$\dim (V(\delta) \cap V(R_j, \delta)) = m - 1.$$ 

**Proof**

$$\dim (A \cap B) = \dim A + \dim B - \dim (A \cup B).$$

We only have to show that $\dim ((V(\delta) \cup V(R_j, \delta)) = h$. This is true since $V(\delta)$ contains $c(f^j_{\leftarrow}(\delta))$ and $V(R_j, \delta)$ contains the rest of the basis $B_j$. 

**Lemma**
The algorithm successfully identifies a valid network code using any field $\mathbb{F}_q$ of size $q > N$.

Consider a coding point $\delta$ with $m \leq h$ parents and a receiver $R_j \in R(\delta)$. The coding vector $c(\delta)$ is a nonzero vector in the $m$-dimensional subspace $V(\delta)$ spanned by the coding vectors of the parents of $\delta$. There are $q^m - 1$ such vectors, feasible for $c(\delta)$. To make the network solvable for receiver $R_j$, $c(\delta)$ should not belong to the intersection of $V(\delta)$ and the $(h - 1)$-dimensional subspace $V(R_j, \delta)$ spanned by the elements of $B_j$ after $c\left(f^j_{\leftarrow}(\delta)\right)$ is removed.
**Linear Information Flow Algorithm**

**Proof** Consider a coding point $\delta$ with $m \leq h$ parents and a receiver $R_j \in R(\delta)$. The coding vector $c(\delta)$ has to be a nonzero vector in the $m$-dimensional subspace $V(\delta)$ spanned by the coding vectors of the parents of $\delta$. There are $q^m - 1$ such vectors, feasible for $c(\delta)$. To make the network solvable for $R_j$, $c(\delta)$ should not belong to the intersection of $V(\delta)$ and $V(R_j, \delta)$ spanned by the elements of $B_j$ after removing $c(f^j_-(\delta))$.

The dimension of this intersection is $m - 1$, and thus the number of vectors it excludes from $V(\delta)$ is $q^{m-1} - 1$. Therefore, the number of vectors excluded by the receivers in $R(\delta)$ is at most $|R(\delta)|q^{m-1} - 1 \leq Nq^{m-1} - 1$ (the $-1$ is the all-zero). Therefore, provided that $q^m > Nq^{m-1} \iff q > N$, a valid value for $c(\delta)$ can be found. This argument is applied to all the coding points.
Introduction to Network Coding, Bounds and Constructions

END OF LECTURE 5