On Success Probability in Random Network Coding
(A review)

Olav Geil
Aalborg University

COST action meeting, Zurich, June 2013

...there is

random network coding

...and then there is

random network coding.

This talk is mostly on random network coding and only a little on random network coding.

...there is

random network coding

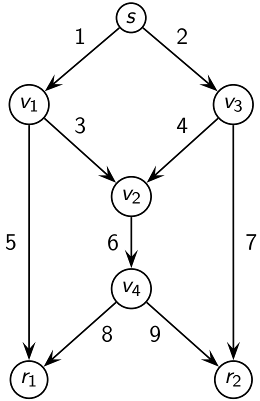
...and then there is

random network coding.

This talk is mostly on random network coding and only a little on random network coding.

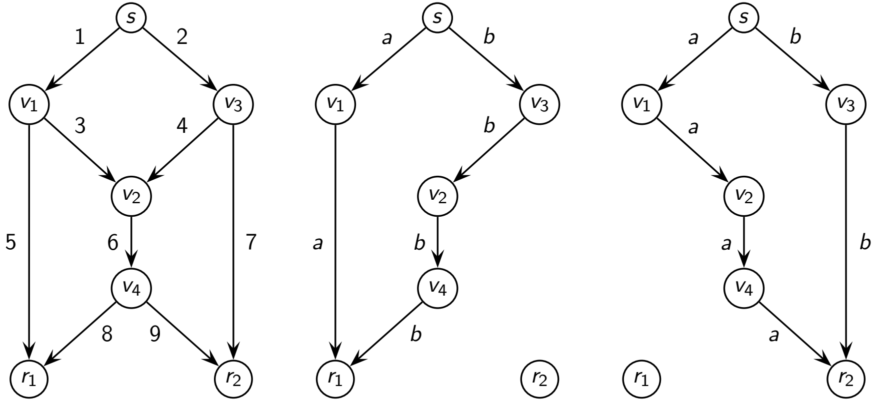
- Ho, T., Médard, M., Koetter, R., Karger, D.R., Effros, M., Shi, J., Leong, B.: *A Random Linear Network Coding Approach to Multicast*. IEEE Transactions on Information Theory, vol. 52, issue 10, pp. 4413–4430, October 2006.
- From description of COST Action IC 1104: "Random network coding emerged through an award-winning paper by R. Koetter and F. Kschischang in 2008 and has since then opened a major research area in communication technology with widespread applications for communication networks like ..."

Simplest possible network coding problem



Sender s wants to send two messages $a, b \in \mathbb{F}_2$ to both receivers r_1 and r_2 simultaneously.

Two partial solutions



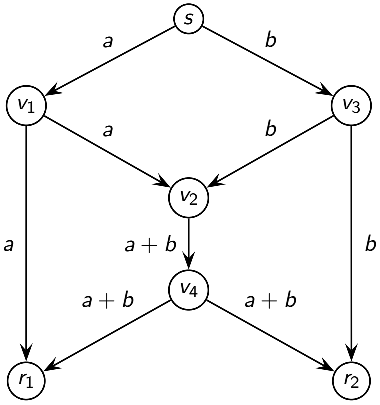
The network   Flow F_1 Flow F_2

The flow system is $\mathcal{F} = \{F_1, F_2\}$

$F_1 = \{(1,5),(2,4,6,8)\}, F_2 = \{(1,3,6,9),(2,7)\}$

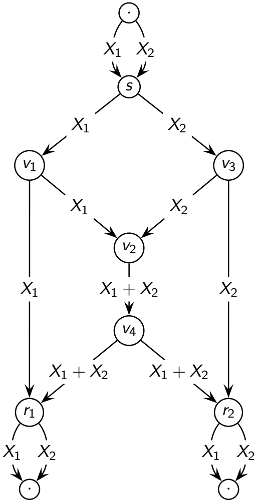
A solution

Routing is insufficient, but problem is solvable



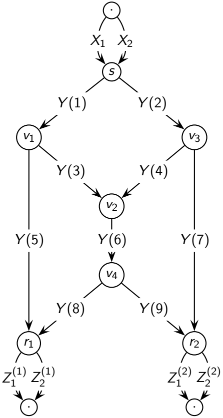
Receiver r_1 can reconstruct b as $a + (a + b)$
Receiver r_2 can reconstruct a as $(a + b) + b$

Linear network coding



Think of X_1 and X_2 as variables that take values in $\mathbb{F}_q = \mathbb{F}_2$.

Linear network coding



$$Y(1) = a_{11}X_1 + a_{21}X_2 = 1 \cdot X_1 + 0 \cdot X_2 = X_1$$
$$Y(2) = a_{12}X_1 + a_{22}X_2 = 0 \cdot X_1 + 1 \cdot X_2 = X_2$$

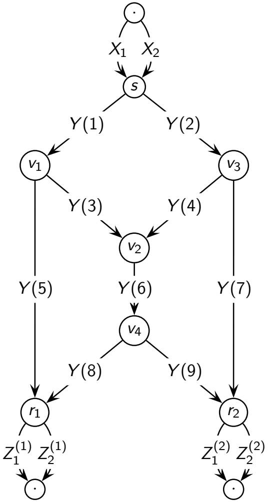
$$Y(3) = f_{13}Y(1) = 1 \cdot Y(1) = X_1$$
$$Y(4) = f_{24}Y(2) = 1 \cdot Y(2) = X_2$$
$$Y(5) = f_{15}Y(1) = 1 \cdot Y(1) = X_1$$
$$Y(6) = f_{36}Y(3) + f_{46}Y(4)$$
$$= 1 \cdot Y(3) + 1 \cdot Y(4) = X_1 + X_2$$

$$\vdots$$

$$Z_2^{(1)} = b_{52}^{(r_1)}Y(5) + b_{82}^{(r_1)}Y(8)$$
$$= 1 \cdot Y(5) + 1 \cdot Y(8) = X_1 + X_1 + X_2 = X_2$$

$$\vdots$$

Linear network coding

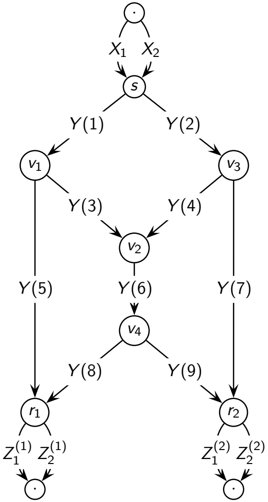


Alphabet is $\mathbb{F}_q = \mathbb{F}_2$ and coefficients below belong to $\mathbb{F}_q = \mathbb{F}_2$.

$$Y(j) = \sum_{i \in \text{in}(j)} f_{i,j} Y(i) + \sum_{K(X_i) = \text{tail}(j)} a_{i,j} X_i$$

$$Z_j^{(r_l)} = \sum_{i \in \text{in}(r_l)} b_{i,j}^{(r_l)} Y(i)$$

The matrix A



$$h = \#\{X_1, X_2\} = 2.$$

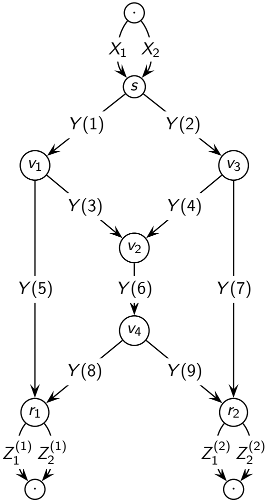
$$|E| = 9.$$

$$A = \begin{bmatrix} a_{11} & a_{12} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

A is $h \times |E|$.

The matrix F

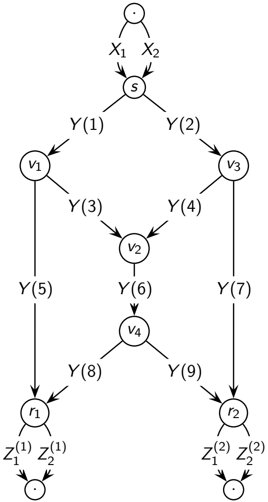


$|E| = 9.$

$$F = \begin{bmatrix} 0 & 0 & f_{13} & 0 & f_{15} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & f_{24} & 0 & 0 & f_{27} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & f_{36} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & f_{46} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & f_{68} & f_{69} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

F is $|E| \times |E|$.

The matrix $B^{(r_i)}$



$h = \#\{X_1, X_2\} = 2$, $|E| = 9$.

$$B^{(r_1)} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ b_{51}^{(r_1)} & b_{52}^{(r_1)} \\ 0 & 0 \\ 0 & 0 \\ b_{81}^{(r_1)} & b_{82}^{(r_1)} \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$B^{(r_i)}$ is $|E| \times h$.

Matrices

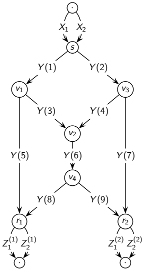
A is $h \times |E|$
$A_{i,j} = a_{i,j}$ if $K(X_i) = \text{tail}(j)$
$A_{i,j} = 0$ else

F is $|E| \times |E|$
$F_{i,j} = f_{i,j}$ if $i \in \text{in}(j)$
$F_{i,j} = 0$ else

For $l = 1, \ldots, |R|$

$B^{(r_l)}$ is $|E| \times h$
$B^{(r_l)}_{i,j} = b^{(r_l)}_{i,j}$ if $i \in \text{in}(r_l)$
$B^{(r_l)}_{i,j} = 0$ else

Paths in the network



$$F^2 =$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & (f_{13}f_{36}) & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & (f_{24}f_{46}) & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & (f_{36}f_{68}) & (f_{36}f_{69}) \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & (f_{46}f_{68}) & (f_{46}f_{69}) \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Topological meaning of F^s

The $F_{i,j}$ "holds" information on all paths of length 2 starting in edge i and ending in edge j.

The (i,j)th entry of F^n "holds" information on all paths of length $n+1$ starting in edge i and ending in edge j.

$$\left(F^n\right)_{i,j} = \sum_{\substack{(i=j_0,j_1,\ldots,j_n=j) \\ \text{a path} \\ \text{in } G}} f_{i=j_0,j_1} f_{j_1,j_2} \cdots f_{j_{n-1},j_n=j}$$

G being cycle free $F^N = 0$ for some big enough N.

$I + F + \cdots + F^{N-1}$ holds information on all paths of any length.

Topological meaning of F^s

The $F_{i,j}$ "holds" information on all paths of length 2 starting in edge i and ending in edge j.

The (i,j)th entry of F^n "holds" information on all paths of length $n+1$ starting in edge i and ending in edge j.

$$\left(F^n\right)_{i,j} = \sum_{\substack{(i=j_0,j_1,\ldots,j_n=j) \\ \text{a path} \\ \text{in } G}} f_{i=j_0,j_1} f_{j_1,j_2} \cdots f_{j_{n-1},j_n=j}$$

G being cycle free $F^N = 0$ for some big enough N.

$I + F + \cdots + F^{N-1}$ holds information on all paths of any length.

Topological meaning of F^s

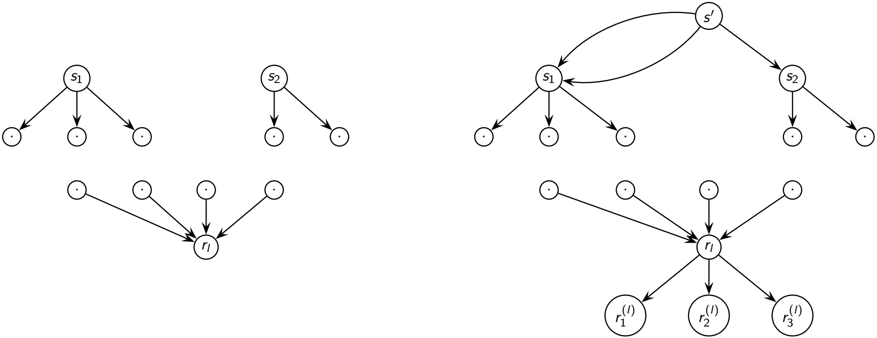
The $F_{i,j}$ "holds" information on all paths of length 2 starting in edge i and ending in edge j.

The (i,j)th entry of F^n "holds" information on all paths of length $n+1$ starting in edge i and ending in edge j.

$$\left(F^n\right)_{i,j} = \sum_{\substack{(i=j_0,j_1,\ldots,j_n=j) \\ \text{a path} \\ \text{in } G}} f_{i=j_0,j_1} f_{j_1,j_2} \cdots f_{j_{n-1},j_n=j}$$

G being cycle free $F^N = 0$ for some big enough N.

$I + F + \cdots + F^{N-1}$ holds information on all paths of any length.



Modification of network. In original network two sources at s_1 and one source at s_2.

In modified network the $a_{i,j}$'s and the $b_{i,j}^{(r_l)}$'s from the original network play the same role as the $f_{i,j}$'s

Transfer matrix

Lemma:
$M^{(r_l)} = A(I + F + \cdots + F^{N-1})B^{(r_l)}$
holds information on all paths from s' to $\{r_1^{(l)}, \ldots, r_h^{(l)}\}$

From this we derive:

Theorem: $(X_1, \ldots, X_h)M^{(r_l)} = (Z_1^{(r_l)}, \ldots Z_h^{(r_l)})$

$M^{(r_l)}$ is called the transfer matrix for r_l

Transfer polynomial

For successful encoding/decoding we require
$M^{(r_1)} = \cdots = M^{(r_{|R|})} = I$

Relaxed requirement:
$\det(M^{(r_l)}) \neq 0$ for $l = 1, \ldots, |R|$.

Success iff
$\prod_{l=1,\ldots,|R|} \det(M^{(r_l)}) \neq 0$

Considered as a polynomial in the $a_{i,j}$'s, $f_{i,j}$'s and $b_{i,j}^{(r_l)}$'s this product is called the transfer polynomial.

Transfer polynomial

For successful encoding/decoding we require
$M^{(r_1)} = \cdots = M^{(r_{|R|})} = I$

Relaxed requirement:
$\det(M^{(r_l)}) \neq 0$ for $l = 1, \ldots, |R|$.

Success iff
$\prod_{l=1,\ldots,|R|} \det(M^{(r_l)}) \neq 0$

Considered as a polynomial in the $a_{i,j}$'s, $f_{i,j}$'s and $b_{i,j}^{(r_l)}$'s this product is called the transfer polynomial.

Transfer polynomial

For successful encoding/decoding we require
$M^{(r_1)} = \cdots = M^{(r_{|R|})} = I$

Relaxed requirement:
$\det(M^{(r_l)}) \neq 0$ for $l = 1, \ldots, |R|$.

Success iff
$\prod_{l=1,\ldots,|R|} \det(M^{(r_l)}) \neq 0$

Considered as a polynomial in the $a_{i,j}$'s, $f_{i,j}$'s and $b_{i,j}^{(r_l)}$'s this product is called the transfer polynomial.

Topological meaning of det M^{r_l}

Theorem: The permanent per$(M^{(r_l)})$ is the sum of all monomial expressions in the $a_{i,j}$'s, $f_{i,j}$'s and $b_{i,j}^{(r_l)}$'s which correspond to a flow of size h from s' to $\{r_1^{(l)}, \ldots, r_h^{(l)}\}$ in the modified graph.

Proof: Apply the lemma carefully.

As a consequence det$(M^{(r_l)})$ is a linear combination of the expressions corresponding to flows. The coefficients being 1 or -1.

In the transfer polynomial $\prod_{l=1,\ldots,|R|} \det(M^{(r_l)})$ every monomial corresponds to a flow system.

Coefficients are integers
which in $\mathbb{F}_q$ becomes elements in $\mathbb{F}_p$, p being the characteristic.

Topological meaning of det M^{r_l}

<u>Theorem:</u> The permanent $\mathrm{per}(M^{(r_l)})$ is the sum of all monomial expressions in the $a_{i,j}$'s, $f_{i,j}$'s and $b_{i,j}^{(r_l)}$'s which correspond to a flow of size h from s' to $\{r_1^{(l)}, \ldots, r_h^{(l)}\}$ in the modified graph.

Proof: Apply the lemma carefully.

As a consequence $\det(M^{(r_l)})$ is a linear combination of the expressions corresponding to flows. The coefficients being 1 or -1.

In the transfer polynomial $\prod_{l=1,\ldots,|R|} \det(M^{(r_l)})$ every monomial corresponds to a flow system.

Coefficients are integers
which in $\mathbb{F}_q$ becomes elements in $\mathbb{F}_p$, p being the characteristic.

Main theorem on linear network coding

Terms MAY cancel out when taking the product of the $\det(M^{(r_l)})$'s.

If all $\det(M^{(r_l)})$'s are different from 0 then so is the transfer polynomial.

Theorem: A multicast problem is solvable iff the graph contains a flow system of size h. If solvable then solvable with linear network coding whenever $q \geq |R|$.

Proof (almost): Necessity follows from unicast considerations. Assume a flow system exists. The transfer polynomial is non-zero and no indeterminate appears in power exceeding $|R|$. Therefore if $q > |R|$ then over $\mathbb{F}_q$ a non-zero solution exists according to the footprint bound.

Main theorem on linear network coding

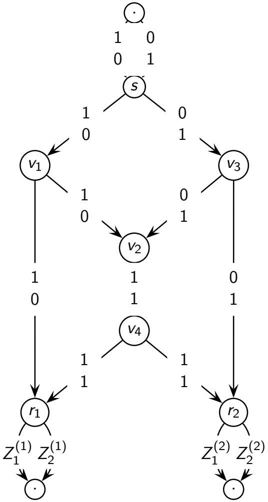
Terms MAY cancel out when taking the product of the $\det(M^{(r_l)})$'s.

If all $\det(M^{(r_l)})$'s are different from 0 then so is the transfer polynomial.

Theorem: A multicast problem is solvable iff the graph contains a flow system of size h. If solvable then solvable with linear network coding whenever $q \geq |R|$.

Proof (almost): Necessity follows from unicast considerations. Assume a flow system exists. The transfer polynomial is non-zero and no indeterminate appears in power exceeding $|R|$. Therefore if $q > |R|$ then over $\mathbb{F}_q$ a non-zero solution exists according to the footprint bound.

Global coding vectors



...actually these vectors later inspired Kötter et. al. to consider the subspace codes

Global coding vectors

In linear network coding we always have
$Y(i) = c_1 X_1 + \cdots + c_h X_h$ for some $c_1, \ldots, c_h \in \mathbb{F}_q$.

We shall call $(c_1, \ldots, c_h)$ the global coding vector for edge i.

A receiver that does not know how encoding was done can learn how to decode (if possible) as follows.

Senders inject into the system h message vectors
$(1, 0, \cdots, 0), (0, 1, 0 \ldots, 0), \ldots, (0, \ldots, 0, 1)$.

These generate the global coding vectors at each edge including the in edges of r_l.

If the received global coding vectors span $\mathbb{F}_q^h$ then proper $b_{i,j}^{(r_l)}$'s can be found.

Global coding vectors

In linear network coding we always have
$Y(i) = c_1 X_1 + \cdots + c_h X_h$ for some $c_1, \ldots, c_h \in \mathbb{F}_q$.

We shall call $(c_1, \ldots, c_h)$ the global coding vector for edge i.

A receiver that does not know how encoding was done can learn how to decode (if possible) as follows.

Senders inject into the system h message vectors
$(1, 0, \cdots, 0), (0, 1, 0 \ldots, 0), \ldots, (0, \ldots, 0, 1)$.

These generate the global coding vectors at each edge including the in edges of r_l.

If the received global coding vectors span $\mathbb{F}_q^h$ then proper $b_{i,j}^{(r_l)}$'s can be found.

Global coding vectors

In linear network coding we always have $Y(i) = c_1 X_1 + \cdots + c_h X_h$ for some $c_1, \ldots, c_h \in \mathbb{F}_q$.

We shall call $(c_1, \ldots, c_h)$ the global coding vector for edge i.

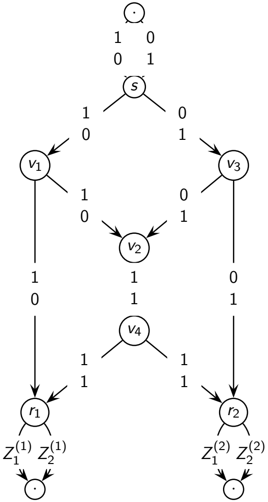
A receiver that does not know how encoding was done can learn how to decode (if possible) as follows.

Senders inject into the system h message vectors $(1, 0, \cdots, 0), (0, 1, 0 \ldots, 0), \ldots, (0, \ldots, 0, 1)$.

These generate the global coding vectors at each edge including the in edges of r_l.

If the received global coding vectors span $\mathbb{F}_q^h$ then proper $b_{i,j}^{(r_l)}$'s can be found.

Jaggi-Sanders algorithm



- Start by localizing a flow system.
- At the top of the flow system choose a basis.
- Update local coding coefficients edge by edge moving down the flow system, in a way such that basis is kept in the cut.

Jaggi-Sanders algorithm

Jaggi-Sanders algorithm takes as input a solvable multicast problem.
It adds a new source s' and moves all processes to this point and add edges $e_1, \dots, e_h$ from s' to S.
In the extended graph a flow system is found.

The algorithm for every receiver keeps a list of edges corresponding to a cut.

Also it updates along the way encoding coefficients in such a way that the global coding vectors corresponding to any of the $|R|$ cuts at any time span the whole of $\mathbb{F}_q^h$.

Edges in the flow system are visited according to an ancestral ordering.

In every update at most one edge is replaced in a given cut.

The Jaggi-Sanders algorithm cont.

Lemma 1.1: Given a basis $\{\vec{b}_1, \ldots, \vec{b}_h\}$ for $\mathbb{F}_q^h$
and $\vec{c} \in \mathbb{F}_q^h$,
there is exactly one choice of $a \in \mathbb{F}_q$ such that
$\vec{c} + a\vec{b}_h \in \text{span}_{\mathbb{F}_q}\{\vec{b}_1, \ldots, \vec{b}_{h-1}\}$.

From the Jaggi-Sanders algorithm we get $q \geq |R|$ is enough!!!
(the zero-solution does not work for any receiver)

Random network coding

In random network coding a (possibly empty) subset of the $a_{i,j}{}'s, f_{i,j}{}'s$ are chosen *a priori* in such a way that the resulting network coding problem is still solvable.

Remaining encoding coefficients are chosen in a distributed manner.
They are chosen independently by uniform distribution.

The transfer polynomial with the *a priori* chosen coefficients plugged in considered as a polynomial with coefficients in $\mathbb{F}_q(b_{i,j}^{(r)}{}'s)$, is called the *a priori* transfer polynomial.

Random network coding

In random network coding a (possibly empty) subset of the ${a_{i,j}}'s, {f_{i,j}}'s$ are chosen *a priori* in such a way that the resulting network coding problem is still solvable.

Remaining encoding coefficients are chosen in a distributed manner.
They are chosen independently by uniform distribution.

The transfer polynomial with the *a priori* chosen coefficients plugged in considered as a polynomial with coefficients in $\mathbb{F}_q({b_{i,j}^{(r)}}'s)$, is called the *a priori* transfer polynomial.

Success probability

Assume the *a priori* transfer polynomial F is non-zero.

Let $T_1^{i_1} \cdots T_m^{i_m}$ be its leading monomial with respect to $\prec$.
The number of combinations of $a_{i,j}{}'s$, $f_{i,j}{}'s$ that plugged into F give a non-zero element in $\mathbb{F}_q(b_{i,j}^{(r)}{}'s)$ is at least $(q-i_1)\cdots(q-i_m)$ (the footprint bound)

$\lim_{q\to\infty} \frac{(q-i_1)\cdots(q-i_m)}{q^m} = 1.$

Recall, $b_{i,j}^{(r_l)}$ appears in power at most 1.

For each of the above solutions:
$b_{i,j}^{(r_l)}$ can be chosen such that F evaluates to non-zero in $\mathbb{F}_q$.

In conclusion: $P_{\text{succ}} \geq (q-i_1)\cdots(q-i_m)/q^m = P_{\text{FP2}}$
(Matsumoto-Thomsen-G.)

Success probability

Assume the *a priori* transfer polynomial F is non-zero.

Let $T_1^{i_1} \cdots T_m^{i_m}$ be its leading monomial with respect to $\prec$.
The number of combinations of $a_{i,j}'s, f_{i,j}'s$ that plugged into F give a non-zero element in $\mathbb{F}_q(b_{i,j}^{(r)'} s)$ is at least $(q - i_1) \cdots (q - i_m)$ (the footprint bound)

$\lim_{q \to \infty} \frac{(q-i_1)\cdots(q-i_m)}{q^m} = 1.$

Recall, $b_{i,j}^{(r_l)}$ appears in power at most 1.

For each of the above solutions:
$b_{i,j}^{(r_l)}$ can be chosen such that F evaluates to non-zero in $\mathbb{F}_q$.

In conclusion: $P_{\text{succ}} \geq (q - i_1) \cdots (q - i_m)/q^m = P_{\text{FP2}}$
(Matsumoto-Thomsen-G.)

Success probability

Assume the *a priori* transfer polynomial F is non-zero.

Let $T_1^{i_1} \cdots T_m^{i_m}$ be its leading monomial with respect to $\prec$.
The number of combinations of $a_{i,j}$'s, $f_{i,j}$'s that plugged into F give a non-zero element in $\mathbb{F}_q(b_{i,j}^{(r)}$'s$)$ is at least $(q-i_1)\cdots(q-i_m)$ (the footprint bound)

$\lim_{q\to\infty} \frac{(q-i_1)\cdots(q-i_m)}{q^m} = 1.$

Recall, $b_{i,j}^{(r_l)}$ appears in power at most 1.

For each of the above solutions:
$b_{i,j}^{(r_l)}$ can be chosen such that F evaluates to non-zero in $\mathbb{F}_q$.

In conclusion: $P_{\text{succ}} \geq (q-i_1)\cdots(q-i_m)/q^m = P_{\text{FP2}}$
(Matsumoto-Thomsen-G.)

Success probability - cont.

Any monomial in the transfer polynomial corresponds to a flow system

$$
\begin{aligned}
P_{\text{succ}} &\geq \min\{(q-i_1)\cdots(q-i_m)/q^m \mid X_1^{i_1}\cdots X_m^{i_m} \text{ corresponds} \\
&\qquad\qquad\qquad\qquad \text{to a flow system in } G\} \\
&= P_{\text{FP1}}
\end{aligned}
$$

(Matsumoto-Thomsen-G.). Note

- not all flow systems need to appear in transfer polynomial
- not all monomials can be chosen as leading

Success probability - cont.

Lemma 1.2: Let $F \in k[T_1, \ldots, T_m] \backslash \{0\}$ where k is a field containing $\mathbb{F}_q$. Assume all monomials $T_1^{j_1} \cdots T_m^{j_m}$ in the support of F satisfies

1. $j_1, \ldots, j_m \leq d$, where d is some fixed number $d \leq q$.
2. $j_1 + \cdots + j_m \leq dN$ for some fixed integer N with $N \leq m$

The probability that F evaluates to a non-zero value when $(X_1, \ldots, X_m) \in \mathbb{F}_q^m$ is chosen by random (uniformly) and is plugged into F is at least

$$\left(\frac{q-d}{q}\right)^N$$

Proof 1: A lot of technical lemmas and the Schwartz-Zippel bound.

Proof 2: The footprint bound plus one simple observation.

Success probability - cont.

Every monomial in transfer polynomial comes from a flow system $\mathcal{F} = (F_1, \ldots, F_{|R|})$. Consider all possible flows (not systems).

For each flow count the number η of encoding coefficients (not chosen *a priori*). Let η' be the maximum of the numbers η. Then for all monomials we have cond. 1 and cond. 2 with $d = |R|$ and $N = \eta'$

We get

$$P_{\text{succ}} \geq \left(\frac{q - |R|}{q}\right)^{\eta'} = P_{\text{Ho2}}$$

Clearly $\eta' \leq |E|$ which gives

$$P_{\text{succ}} \geq \left(\frac{q - |R|}{q}\right)^{|E|} = P_{\text{Ho1}}$$

Success probability - cont.

Every monomial in transfer polynomial comes from a flow system $\mathcal{F} = (F_1, \ldots, F_{|R|})$. Consider all possible flows (not systems).

For each flow count the number η of encoding coefficients (not chosen *a priori*). Let η' be the maximum of the numbers η. Then for all monomials we have cond. 1 and cond. 2 with $d = |R|$ and $N = \eta'$

We get

$$P_{\text{succ}} \geq \left(\frac{q - |R|}{q}\right)^{\eta'} = P_{\text{Ho2}}$$

Clearly $\eta' \leq |E|$ which gives

$$P_{\text{succ}} \geq \left(\frac{q - |R|}{q}\right)^{|E|} = P_{\text{Ho1}}$$

Success probability - cont.

$$P_{\text{Ho1}} \leq P_{\text{Ho2}} \leq P_{\text{FP1}} \leq P_{\text{FP2}}$$

Applying the Jaggi-Sanders point of view one get "flow-bounds". These are always better than P_{Ho2}.

Combinatorial approach:

- Jaggi-Sanders visit edges in flowsystem one by one.
- Alternative approach by Balli, Yan and Zhang: Visit vertices in flowsystem one by one. Gives bound in terms of number of vertices.

Success probability - cont.

$$P_{\mathrm{Ho1}} \leq P_{\mathrm{Ho2}} \leq P_{\mathrm{FP1}} \leq P_{\mathrm{FP2}}$$

Applying the Jaggi-Sanders point of view one get "flow-bounds". These are always better than P_{Ho2}.

Combinatorial approach:

- Jaggi-Sanders visit edges in flowsystem one by one.
- Alternative approach by Balli, Yan and Zhang: Visit vertices in flowsystem one by one. Gives bound in terms of number of vertices.

Random network coding

The operator channel as used in random network coding could be based on:

- Linear random network coding.
- Edges being q-ary symmetric channels.

What:

- would be the success probability without random network coding?
- could be achieved in combination with random network coding?

Random network coding

The operator channel as used in random network coding could be based on:

- Linear random network coding.
- Edges being q-ary symmetric channels.

What:

- would be the success probability without random network coding?
- could be achieved in combination with random network coding?