Aspects of network coding - Part II

O. Geil, Aalborg University

S^3cm: Soria Summer School on Computational Mathematics,
Universidad de Valladolid, Soria
July 12-16 2010

The footprint

Let $\mathcal{M}(X_1, \ldots, X_m)$ be the set of monomials in $X_1, \ldots, X_m$.

Definition: A monomial ordering $\prec$ on $\mathcal{M}(X_1, \ldots, X_m)$ is a total ordering such that

- every subset has a smallest element
- if $M \prec N$ then $KM \prec KN$ holds for all $M, N \in \mathcal{M}(X_1, \ldots, X_m)$ and all $K \in \mathcal{M}(X_1, \ldots, X_m) \backslash \{0\}$.

One example is the lexicographic ordering, but there are infinitely many.

Definition: Given an ideal $I \subseteq k[X_1, \ldots, X_m]$ and a monomial ordering $\prec$ the footprint is $\Delta_{\prec}(I) = \{M \in \mathcal{M}(X_1, \ldots, X_m) \mid M \notin \mathrm{lm}(I)\}$.

Theorem:
$\{M + I \mid M \in \Delta_{\prec}(I)\}$ is a basis for $k[X_1, \ldots, X_m]/I$ as a vector space.

$I \subseteq \mathcal{I}(\mathcal{V}_k(I)) \Rightarrow \Delta_{\prec}(\mathcal{I}(\mathcal{V}_k(I))) \subseteq \Delta_{\prec}(I)$

Assume $\mathcal{V}_k(I)$ is finite. Say $\mathcal{V}_k(I) = \{P_1, \ldots, P_n\}$.

Let $\varphi : k[X_1, \ldots, X_m]/\mathcal{I}(\mathcal{V}_k(I)) \to k^n$ be given by $\varphi(f + \mathcal{I}(\mathcal{V}_k(I))) = (f(P_1), \ldots, f(P_n))$.

Lagrange interpolation tells us that surjective.

If $f + \mathcal{I}(\mathcal{V}_k(I)) \neq g + \mathcal{I}(\mathcal{V}_k(I))$ then cannot be identical under φ as this would imply $f - g \in \mathcal{I}(\mathcal{V}_k(I))$.

Hence, φ is a vector space isomorphism.

The footprint bound

Combining:

- $\varphi : k[X_1, \ldots, X_m]/\mathcal{I}(\mathcal{V}_k(I)) \to k^n$ is an isomorphism
- $\{M + \mathcal{I}(\mathcal{V}_k(I)) \mid M \in \Delta_{\prec}(\mathcal{I}(\mathcal{V}_k(I))\}$ is a basis for $k[X_1, \ldots, X_m]/\mathcal{I}(\mathcal{V}_k(I)$
- $n = \#\mathcal{V}_k(I) = \#\mathcal{V}_k(\mathcal{I}(\mathcal{V}_k(I)))$
- $\#\Delta_{\prec}(\mathcal{I}(\mathcal{V}_k(I))) \leq \#\Delta_{\prec}(I)$

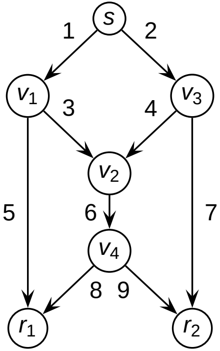
we get

Proposition 1.2: $\#\mathcal{V}_k(I) \leq \#\Delta_{\prec}(I)$

Corollary 1.1: Let k be any field containing $\mathbf{F}_q$. Let $F(X_1, \ldots, X_m) \in k[X_1, \ldots, X_m]$ with $\mathrm{lm}(F) = X_1^{i_1} \cdots X_m^{i_m}$. The number of non-zeros in $\mathbf{F}_q^m$ of F is at least $(q - i_1) \cdots (q - i_m)$.

Proof: The number of zeros in $\mathbf{F}_q^m$ is at most the size of $\Delta_{\prec}(\langle F(X_1, \ldots, X_m), X_1^q - X_1, \ldots, X_m^q - X_m \rangle)$.
This footprint is contained in $\Delta_{\prec}(\langle X_1^{i_1} \cdots X_m^{i_m}, X_1^q, \ldots, X_m^q \rangle)$. The latter footprint is of size $q^m - (q - i_1) \cdots (q - i_m)$.

Linear multicast



Consider the $a_{i,j}$, $j \in \mathrm{out}(K(X_i))$ and the $f_{i,j}$, $j \in \mathrm{out}(i)$ as variables that can take on values in $\mathbf{F}_q$.

Recall that we also have decoding variables $b_{i,j}^{(r_l)}$.

The transfer polynomial which is $\prod_{r\in R} \det(M^{(r)})$ can be considered as a polynomial in $\mathbf{F}_q(b_{i,j}^{(r)}{}' s)[a_{i,j}{}'s, f_{i,j}{}'s]$.

Recall from yesterday that receivers do not need to know the encoding functions.

Rather X_1 sends $(1, 0, \ldots, 0)$, X_2 sends $(0, 1, 0, \ldots, 0), ...,$ X_h sends $(0, \ldots, 0, 1)$

Receiver r_l observes the global coding vectors arriving on the in-coming edges.

If they span $\mathbf{F}_q^h$ then proper $b_{i,j}^{(r_l)'}s$ can be determined by linear algebra.

Random network coding

In random network coding a (possible empty) subset of the $a_{i,j}'s, f_{i,j}'s$ are chosen apriori 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.

As a consequence the vector of randomly chosen coefficients are chosen also from a uniform distribution.

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

Research problem: What is the success probability P_{succ}?

Assume the apriori transfer polynomial F is non-zero.

Let $X_1^{i_1} \cdots X_m^{i_m}$ be it 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 $\mathbf{F}_q(b_{i,j}^{(r)}{}'s)$ is at least
$(q - i_1) \cdots (q - i_m)$

If q is big enough this is a possitive number.

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

Applying the footprint bound again we see that for each of the above solutions $b_{i,j}^{(r_l)}$ can be chosen such that F evaluates to non-zero in $\mathbf{F}_q$.

In conclussion
$P_{\text{succ}} \geq (q - i_1) \cdots (q - i_m) = P_{\text{FP2}}$

Any monomial in transfer polynomial corresponds to a flow system

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

Note

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

Lemma 1.2: Let $F \in k[X_1, \ldots, X_m] \backslash \{0\}$ where k is a field containing $\mathbf{F}_q$. Assume all monomials $X_1^{i_1} \cdots X_m^{i_m}$ 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 $(X_1, \ldots, X_m) \in \mathbf{F}_q^m$ is chosen by random (uniformly) and is plugged into F is at least

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

Proof of lemma

With Corollary 1.1 in mind we want to establish

$$\frac{\prod_{t=1}^{m}(q-j_t)}{q^m} \geq \left(\frac{q-d}{d}\right)^N \tag{1}$$

for all $j_1, \ldots, j_m$ satisfying cond. 1 and cond. 2. Let $j_1, \ldots . j_m$ be such that lhs. of (1) is minimal. Wlog. assume $j_1 \geq \cdots j_m$. We have equality in cond. 2.

Observe that if $x \geq y$ then

$$(q-x)(q-y) > (q-(x+1))(q-(y-1))$$

Hence, $j_1 = \cdots = j_N = d, j_{N+1} = \cdots j_m = 0$.

This gives rhs. of (1)

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

Let η' be the maximal number of encoding coefficients not chosen apriori. Then for all monomials we have cond. 1 and cond. 2 with

$d = |R|$ and $N = \eta'$

We get

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

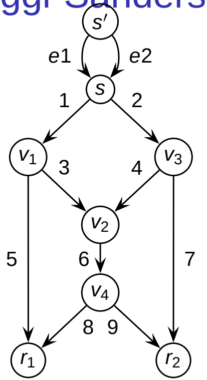
Clearly $\eta' \leq |E|$ which gives

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

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

Go to Example 1.2 and Example 1.3 in paper....

Jaggi-Sanders algorithm



<u>*Initialization:*</u> Add s' and $e_1, \dots, e_h$.

Set $C_1 = \cdots C_{|R|} = (e_1, \dots, e_h)$ and $B_1 = \cdots = B_{|R|} = ((1, 0, \dots, 0), \dots, (0, \dots, 0, 1))$.

Find $\mathcal{F} = (F_1, \dots, F_{|R|})$

<u>*Update:*</u> Consider next edge j acćording to ancestral ordering.

If $i \in \text{in}(j) \cap F_l$ then replace i with j in C_l.

Find encoding coefficients such that global coding vectors for all updated cuts do still span $\mathbf{F}_q^h$.

Ancestral ordering $1 \prec 2 \prec \cdots \prec 9$.

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

$\underline{j = 1}$:

$C_1 = C_2 = (1, e_2)$,

$a_{1,1} = 1$, $a_{2,1} = 0$

$B_1 = B_2 = ((1,0),(0,1))$

$\underline{j = 2}$:

$C_1 = C_2 = (1, 2)$,

$a_{1,2} = 0$, $a_{2,2} = 1$

$B_1 = B_2 = ((1,0),(0,1))$

$\underline{j = 3}$:

C_1 is unchanged.

$C_2 = (3, 2)$, $f_{1,3} = 1$

$B_2 = ((1,0),(0,1))$

$\underline{j = 4}$:

C_2 is unchanged.

$C_1 = (1, 4)$, $f_{2,4} = 1$

$B_1 = ((1,0),(0,1))$

$\underline{j = 5}$:

C_2 is unchanged.

$C_1 = (5, 4)$, $f_{1,5} = 1$

$B_1 = ((1,0),(0,1))$

$\underline{j = 6}$:

$C_1 = (5, 6)$, $C_2 = (6, 2)$

$f_{3,6} = 1$, $f_{4,6} = 1$

$B_1 = ((1,0),(1,1))$

$B_2 = ((1,1),(0,1))$

Modified Jaggi-Sanders algorithm

Assume ALL encoding coefficients are chosen by random (uniformly, independently)

Initialization part is kept.

Ín updating part we still update the cuts.
For every updated cut we CHECK if already chosen coefficients gives a full basis of global coding vectors. If not return “failure” and abort.

If visited all edges in flow system and having not returned “failure” then return “success”.

Situation is changed as we now get information from outside the flow system.

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

Given the algorithm arrived at j the probabiliy that it does not return “failure” in this step is at least:

$$\frac{q-k}{q} + \frac{k-1}{q^{|\text{in}'(j)|}}$$

where k is the number of receivers that uses edge j in $\mathcal{F}$.

Let $R_{\mathcal{F}}(e)$ be number of receivers that use edge e in $\mathcal{F}$.

$$\begin{aligned} P_{\text{succ}} &\geq P_{\text{FB2}} = \prod_{j \in \mathcal{F}} \left(\frac{q - R_{\mathcal{F}}(j)}{q} + \frac{R_{\mathcal{F}}(j) - 1}{q^{|\text{in}'(j)|}} \right) \\ &\geq P_{\text{FB1}} = \prod_{j \in \mathcal{F}} \frac{q - R_{\mathcal{F}}(j)}{q} \end{aligned}$$

It is possible to improve upon P_{FB1} and P_{FB2} by noting that if $C_{l_1}\setminus\{i_1\} = C_{l_2}\setminus\{i_2\}$ and i_1 respectively i_2 is replaced with j then in this step we have
success for r_{l_1} iff success for r_{l_2}.

These improvements rely on the chosen ancestral ordering.

See possibly Example 1.6

Combinatorial approach by Balli, Yan and Zhang

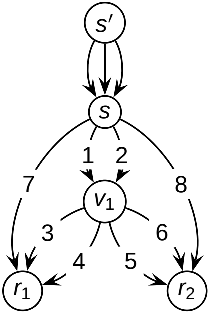
Network being cycle free also means that we can order VERTICES by ancestral ordering.

Further modified Jaggi-Sanders algorithm is derived.

Initialization part unchanged.

Update: Visit vertices in flow system according to ancestral ordering.
Update the cuts by replacing for every receiver r_l the edges in $\mathrm{in}'(w) \cap F_l$ with the edges in $\mathrm{out}(w) \cap F_l$.

Check if each of the corresponding sets B_l of global coding vectors do still span the whole of $\mathbf{F}_q^h$.



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

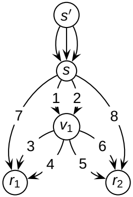
Initialization:

$C_1 = C_2 = (e_1, e_2, e_3)$
$B_1 = B_2 = ((1,0,0),(0,1,0),(0,0,1))$

Update:

Consider s:
$I_1 = I_2 = \{e_1, e_2, e_3\}$
$J_1 = \{1,2,7\}$, $J_2 = \{1,2,8\}$
$C_1 = (1,2,7)$, $C_2 = (1,2,8)$

Consider v_1:
$I_1 = I_2 = \{1,2\}$
$J_1 = \{3,4\}$, $J_2 = \{5,6\}$
$C_1 = (3,4,7)$, $C_2 = (5,6,8)$



At v_1 we need to “choose” encoding coefficients such that:

- $g_c(3)$ is lin. indep. of $\{g_c(7)\}$
- $g_c(4)$ is lin. indep. of $\{g_c(3), g_c(7)\}$

and such that

- $g_c(5)$ is lin. indep. of $\{g_c(8)\}$
- $g_c(6)$ is lin. indep. of $\{g_c(5), g_c(8)\}$

Lemma 1.3: Consider integers k, h, μ with $1 \leq k < h$ and $k + \mu < h$. Let $\{\vec{b}_1, \ldots, \vec{b}_h\}$ be a basis for $\mathbf{F}_q^h$ and let $\vec{b}'_{k+1}, \ldots, \vec{b}'_{k+\mu}$ be such that

$$V = \mathrm{span}_{\mathbf{F}_q}\{\vec{b}_1, \ldots, \vec{b}_k, \vec{b}'_{k+1}, \ldots, \vec{b}'_{k+\mu}\}$$

is of dimension $k + \mu$.
Given $\vec{c} \in \mathbf{F}_q^h$ the number of choices of $(a_{k+1}, \ldots, a_h)$, $a_i \in \mathbf{F}_q$ such that

$$\vec{c} + a_{k+1}\vec{b}_{k+1} + \cdots + a_h\vec{b}_h \in V$$

equals q^μ.

Let $I_l = \text{in}'(w) \cap F_l$ and $J_l = \text{in}'(w) \cap F_l$.
Note, $|I_l| = |J_l|$.

Consider the edges in J_l one by one.

Check if the global coding vector of the first edge in J_l is linearly independent from $B_l \backslash c_g(I_l)$.
This happens with probability $(q^{|J_l|} - 1)/q^{|J_l|}$.
If OK name it $\vec{b}'_{k+1}$ and add it to $B_l \backslash c_g(I_l)$.

Continuing this way we get...
The probability that the algortihm does not declare “failure” when r_l is checked at w

$$\begin{aligned} &\geq \prod_{i=1}^{|J_l|} \frac{q^{|J_l|} - q^{i-1}}{q^{|J_l|}} \\ &= \prod_{i=1}^{|J_l|} \left(1 - \frac{1}{q^{|J_l|-i+1}}\right) \geq 1 - \frac{1}{q-1} \end{aligned}$$

The probability of success at w is at least

$$1 - \frac{\rho(w)}{q-1}$$

where $\rho(w)$ is the number of receivers using w in $\mathcal{F}$.

Writing $\mathcal{I} = \{w \in V \mid \text{out}(w) \cap \mathcal{F} \neq \emptyset\}$
we get

$$\begin{aligned} P_{\text{succ}} &\geq P_{\text{Balli2}} = \prod_{w \in \mathcal{I}} \left(\frac{1 - \rho(w)}{q-1} \right) \\ &\geq P_{\text{Balli1}} = \left(1 - \frac{|R|}{q-1} \right)^{\mathcal{I}} \end{aligned}$$

We gained something in the probability estimations by allowing actually the flow system to change.

We paid some price when summing up error probabilities (assuming the worst cases).

It seems that Balli, Yan and Zhang’s bound are often better than the flow bounds.

However, we have examples where the opposite holds.

General communication situation

Demands $D(r_1), \dots, D(r_{|R|})$ need not be the same.

$$\begin{aligned} &[x_1, \dots, x_h]\left[M^{(r_1)}, \cdots, M^{(r_{|R|})}\right] \\ &= \left[z_1^{(r_1)}, \dots z_{|D(r_1)|}^{(r_1)}, \dots, z_1^{(r_{|R|})}, \dots, z_{|D(r_{|R|})|}^{(r_{|R|})}\right] \end{aligned}$$

Note, that $M^{(r_l)}$ is only quadratic if r_l demands all informations. Rather it is an $h \times |D(r_l)|$ matrix.

Let $D(r_l) = (X_{i_1^{(l)}}, \dots, X_{i_{|D(r_l)|}^{(l)}})$ for $l = 1, \dots, |R|$.

Success full coding:

- the sub matrix of $M^{(r_l)}$ consisting of rows $i_1^{(l)}, \dots, i_{|D(r_l)|}^{(l)}$ has a non-zero determinant for $i = 1, \dots, |R|$
- remaining entries in $M^{(r_l)}$ are all zero to not disturb.

So we have say k polynomials $f_1, \ldots, f_k$ that must evaluate to zero plus a polynomial say F (the product of the determinants) which must evaluate to non-zero.

Introducing a new variable ϵ we consider

$$\mathcal{V}_{\mathbf{F}_q}(\langle f_1, \ldots, f_k, 1 - \epsilon F \rangle).$$

Dougherty, Freiling and Zeger showed that any set of polynomial equations with INTEGER coefficients corresponds to a linear network coding problem in the following sense. The set of polynomials have a commen non-zero over $\mathbf{F}_q$ iff the network coding problem has a linear solution.