Network coding and cyclic convolutional codes

Fai Lung Tsang (HKUST, CUHK-INC)
join work with Wai Ho Mow (HKUST)

24-11-2010

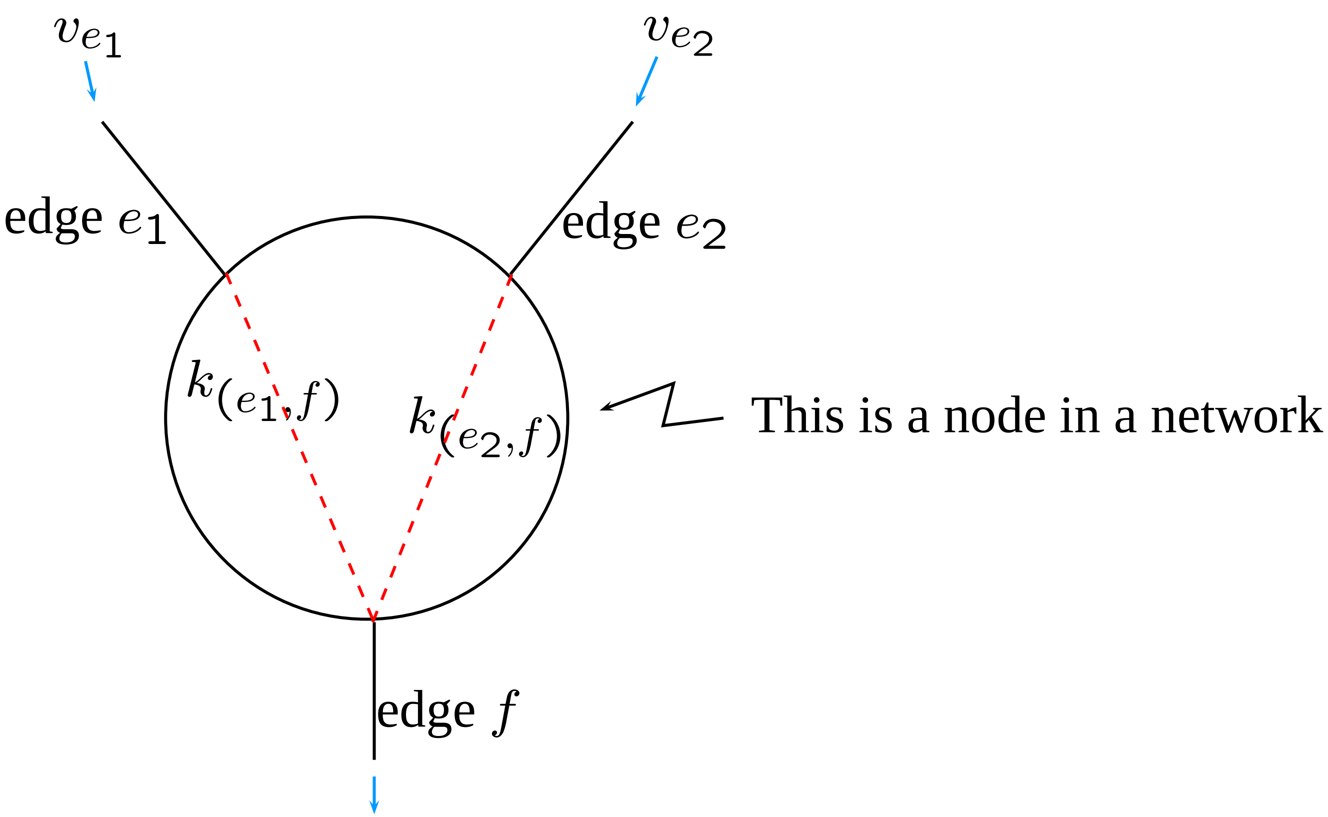
Network coding and cyclic convolutional codes

Outline:

a. Introduction: Koetter-Kschischang "subspace" network coding

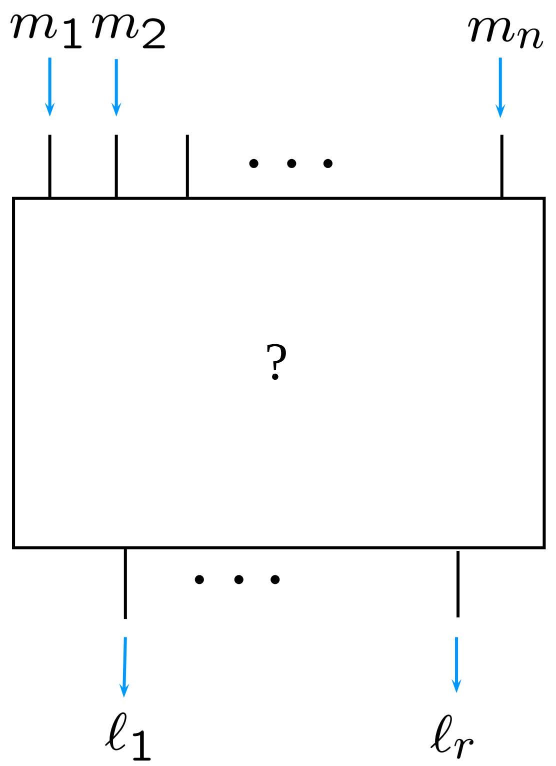
b. Our generalization

c. Cyclic convolutional codes and NC



$$v_f = k_{(e_1,f)} \cdot v_{e_1} + k_{(e_2,f)} \cdot v_{e_2}$$

Say, input: $v_{e_1} = (1,0,0)$, $v_{e_2} = (0,1,0)$.
The output vector v_f depending on the choice of
Local encoding coefficients: k's.



In an <u>unknown</u> (or <u>random</u>) network, without regard to the underlying topology, the output ℓ's are linear combinations of the input vectors m_i's.

a. K-Ks subspace NC

- Linear relation: $(\ell_1, \ldots, \ell_r)^T = G(m_1, \ldots, m_n)^T$.

- "There is *no* assumption here that the network operates synchronously or without delay or that the network is acyclic."

- They proposed:
  INPUT=X, a space generated by m's,
  OUTPUT=Y, a space generated by ℓ's.

a. K-Ks subspace NC (Cont.)

Start with a large vector space, say $M = \mathbb{F}^N$.
Let $P(M)$ be the collection of all subspaces of M.
A *code* $\mathcal{C}$ is a subset of $P(M)$.
INPUT: X, as a set of generators of X.
OUTPUT: Y, the space generated by observable outputs ℓ's.

If there is no errors, we must have $Y \subset X$.
If there is error, they modelled it as $Y = H_k(X) \oplus E$, here $k = \dim(X \cap Y)$ and H_k is an operator randomly choosing a k-dimensional subspace of X.

There is a distance concept in $P(M)$:
$d(U,V) := \dim(U + V) - \dim(U \cap V)$,
d makes $P(M)$ into a metric space.

a. K-Ks subspace NC (Cont.)

Comparison:

	Block code	Subspace NC
Code	$\mathcal{C} \subset \mathbb{F}^N$	$\mathcal{C} \subset P(\mathbb{F}^N)$
Codeword	x vector	X vector space
Metric	$d(x, y)$ Hamming	$d(U, V)$

a.$\rightarrow$b. Why generalize?

Some questions on Koetter-Kschischang's subspace NC framework:

1. What is the meaning of injecting vector spaces?

2. Really no assumption on delayness and cyclicity?

3. Is the model $Y = H_k(X) \oplus E$ sensible?

a.$\to$b. 1. What is the meaning of injecting vector spaces?

Let X be a space injected using its generators $\{m_1, \ldots, m_n\}$ ($\dim X \le n$). Since the network is noncoherent, the matrix G may or may not be of full rank.
If G has full rank, $Y = X$
    $\longrightarrow$ no problem.
If G has deficient rank, $\dim(Y) \le \min(rank(G), \dim(X))$
    $\longrightarrow$ even different injection order affects $\dim(Y)$, i.e., $d(Y, X)$ varies.
Note: **in no error case**
$d(Y, X) = \dim(Y + X) - \dim(Y \cap X) = \dim X - \dim Y$.

One needs to address the relationship between allowable rank loss ("erasure") and $d_{\mathcal{C}}$ when designing a code $\mathcal{C}$.

a.$\rightarrow$b. 2. No assumption needed on delayness and cyclicity?

We adopt the assumptions:

- If no delays, we do not allow cycles.

- Cycles must come with delays.

c.f., theory of convolutional codes.

a.→b. 3. Is the model $Y = H_k(X) \oplus E$ sensible?

Let $m_1, \ldots, m_n$ be the inputs which generates X.
The observable outputs are $\ell'_1, \ldots, \ell'_r$, where

$$\ell'_i = \ell_i + \epsilon_i \ , \quad \ell_i \in X$$

and ϵ_i represents the error (maybe 0). Y is generated by $\{\ell'_i\}$.

$X = \mathbb{F}(m_1, \ldots, m_n)$,
$Y = \mathbb{F}(\ell'_1, \ldots, \ell'_r) = \mathbb{F}(\ell_1 + \epsilon_1, \ldots, \ell_r + \epsilon_r)$.

It may happen that $\dim Y \cap X = 0$ or $k = 0$, hence $Y = E$.
Do we really want to model "error" and "erasure" in this way?

[Certainly we think there are better interpretations.]

b. Generalization.

Ingredients:
M a finitely generated free R module with R a principal ideal domain.

"finitely generated free": $M \approx R^N$
"domain": $a \cdot b = 0$ in R implies $a = 0$ or $b = 0$
"ideal": $I \subset R$ is an ideal if I is a subring and that $z \in I$ implies $a \cdot z \in I$ for all $a \in R$.
"subring": I is a subring if $a - b \in I$ for all $a, b \in I$.

Examples of (M, R): $(\mathbb{F}^N, \mathbb{F}) \leftarrow$ acyclic networks with no delay.
$(\mathbb{Z}^N, \mathbb{Z})$
$(\mathbb{F}[z]^N, \mathbb{F}[z]) \longleftarrow$ acyclic networks with delays.
$(\mathbb{F}[(z)]^N, \mathbb{F}[(z)]) \longleftarrow$ cyclic networks with delays (**Li-Sun**).
$(A[z;\sigma], \mathbb{F}[z]) \longleftarrow$ cyclic convolutional codes.

b. Generalization. (Cont.)

Admissible codewords:
$P(M)$ collection of all <u>saturated</u> submodules in M.
A code $\mathcal{C}$ is a subset of $P(M)$.

"saturated": X is a saturated submodule of M if
$0 \neq a \cdot x \in X \Rightarrow x \in X$.
Equivalent def.: if $X \oplus J = M$ for some $J \subset M$.

d a metric on $P(M)$:
$d(X,Y) := rank(X) + rank(Y) - 2 \cdot rank(X \cap Y)$
(can prove)$= rank(X+Y) - rank(X \cap Y)$.

"$rank(X)$" is the cardinality of a basis of X.

b. Our answers

Let $m_1, \ldots, m_n$ generate X (INPUT).
Observable outputs are $\ell'_1, \ldots, \ell'_r$ that generate Y (OUTPUT).
$\ell'_i = \ell_i + \epsilon_i$, here $\ell_i \in X$, ϵ_i is error.
Let $Y_0 := R(\ell_1, \ldots, \ell_r)$ and $E = R(\epsilon_1, \ldots, \epsilon_r)$.

If all $\epsilon_i = 0$ (no errors), then $Y = Y_0 \subset X$.
In other cases, $Y \subset Y_0 + E$.

"rank loss" $= rank(X) - rank(Y_0)$
"error" $= rank(E)$.

Theorem. Let $\mathcal{C}$ be a code with minimal distance $d_{\mathcal{C}}$. Then rank loss $+ 2 \cdot$ error $< d_{\mathcal{C}}/2$ implies $d(Y, X) < d_{\mathcal{C}}/2$.

c. Cyclic convolutional codes and NC

Let $R = \mathbb{F}[z]$ a polynomial ring.
$M = A[z;\sigma]$ a skew polynomial ring which is also a f.g. free module over R.

$A = \mathbb{F}\times\cdots\times\mathbb{F}$ (N-copies), A has *primitive idempotents* $e_1,\ldots,e_N$.
$A = \mathbb{F}e_1 + \cdots + \mathbb{F}e_N$. [If you like, you may think of $e_1 = (1,0,\ldots)$.]

$\sigma : A \to A$ automorphism which fixes $\mathbb{F}$ such that
$\sigma(e_i) = e_{i+1}$ and $\sigma(e_N) = e_1$.

Elements in M are polynomials
$a_0 + a_1 z + \ldots + a_s z^s$.

Multiplication of z follows the rule: $za = \sigma(a)z$.
Hence $z(a_0 + a_1 z + \ldots + a_s z^s) = \sigma(a_0)z + \ldots + \sigma(a_s)z^{s+1}$.

c. Cyclic convolutional codes and NC (Cont.)

Some facts:

- $M \approx R^N$.
- All elements in $P(M)$ are called *cyclic convolutional codes*.
- All elements in $P(M)$ are principal left M-ideal, i.e., $X = Mg$.
- Rank of an element in $P(M)$ is easily calculated, namely,
  if $g = g_0 + g_1 z + \dots$ then $rank(X) = \#\{i |\ g_0 e_i \neq 0\}$
- $d(X, Y)$ easily estimated, thus ease code design.

Further problems

1. Exists other metrics?

   [Injection metric]

2. Constructions of cyclic convolutional codes for NC?

   [We have a simple construction]

3. Simulation results?

References

R. Koetter and F. R. Kschischang. *Coding for errors and erasures in random network coding*. IEEE-IT 2008.

S.-Y. R. Li and Q. T. Sun. *Network coding theory via commutative algebra*. To appear in IEEE-IT.

Graphic tool: `http://latexdraw.sourceforge.net/`