Aspects of network coding - Part III

O. Geil, Aalborg University

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

We will present material from the seminal paper:

“Coding for Errors and Erasures in Random Network Coding”

by Ralf Kötter and Frank R. Kschischang, Recall that in the error free case we have success if the global coding vectors on the in-edges of every receiver span the whole of $\mathbf{F}_q^h$.

Idea: Given a collection of messages, identify each of them with a vector space. For a concrete message m inject into the system a (possible overcomplete) basis of the corresponding vector space $V(m)$.

The receiver collects a set of vectors which span some vector space U.

The receiver knows the code (the set of vector spaces that corresponds to messages).

If $U = V(m)$ then easy. Else we need some kind of decoding algorithm.

Kötter, Kschischang:

- introduced subspace codes
- described proper code parameters, and minimum distance decoding
- gave upper and lower bounds
- introduced the important Kötter-Kschischang codes (KK-codes)
- gave decoding algorithm for KK-codes

Recently Hessam Mahdavifar and Alexander Vardy modified KK-codes and presented a list decoding algorithm.

Codes

Given a so-called ambient (vector) space W of dimension N by $\mathcal{P}(W)$ we denote the set of all linear subspaces of W.

A code C is a collection of subspaces of W. That is $C \subseteq \mathcal{P}(W)$.

A code can be used to transmit $|C|$ different messages.

Channel model

We do not assume knowledge about the network.

- No information about min cut numbers
- No information about number of malicious messages and where they are injected into the system
- Encoding coefficients in network can be assumed to be chosen by random. Decoding coefficients are absent.

Always assume one sender. Input/output alphabet is $\mathcal{P}(W)$.

Assume V was send and U is received. We can write

$U = (V \cap U) \oplus E$

where $E \in \mathcal{P}(W)$

The number of erasures is $\rho = \dim(V) - \dim(V \cap U)$.

The number of errors is $t = \dim(E)$

The subspace distance

$d : \mathcal{P}(W) \times \mathcal{P}(W) \to \mathbf{N}$
$d(A, B) = \dim(A + B) - \dim(A \cap B)$

Since $\dim(A + B) = \dim(A) + \dim(B) - \dim(A \cap B)$ we get

$$\begin{aligned} d(A, B) &= \dim(A) + \dim(B) - 2\dim(A \cap B) \\ &= 2\dim(A + B) - \dim(A) - \dim(B) \end{aligned}$$

Note that if $U = (U \cap V) \oplus E$ and $\rho = \dim(V) - \dim(U \cap V)$ and $t = \dim(E)$ then
$d(U, V) = \dim(U) + \dim(V) - 2\dim(U \cap V) = t + \rho$

Lemma 1: $d(A, B)$ is a metric on $\mathcal{P}(W)$

Proof:
(i): $d(A, B) \geq 0$ with equality iff $A = B$ is OK

(ii): $d(A, B) = d(B, A)$ is OK

(iii): $d(A, B) \leq d(A, X) + d(X, B)$ is shown on next slide

Proof of (iii)

$$\begin{aligned}
& \frac{1}{2}\big(d(A,B) - d(A,X) - d(X,B)\big) \\
= \; & \frac{1}{2}\big(\dim(A) + \dim(B) - 2\dim(A \cap B) \\
& - \dim(A) - \dim(X) + 2\dim(A \cap X) \\
& - \dim(X) - \dim(B) + 2\dim(B \cap X)\big) \\
= \; & \dim(A \cap X) + \dim(B \cap X) - \dim(A \cap B) - \dim(X) \\
= \; & \dim(A \cap X \cap B) + \dim(A \cap X + B \cap X) - \dim(A \cap B) - \dim(X) \\
= \; & \dim(A \cap X + B \cap X) - \dim(X) + \dim(A \cap X \cap B) - \dim(A \cap B) \\
\leq \; & 0 + 0 = 0
\end{aligned}$$

Dual code

$U^\perp = \{v \in W \mid \vec{u} \cdot \vec{v} = 0 \ \forall \ u \in U\}$

$\dim(U) = k \Rightarrow \dim(U^\perp) = N - k$

We have $(U^\perp)^\perp = U$, $(U + V)^\perp = U^\perp \cap V^\perp$ and $(U \cap V)^\perp = U^\perp + V^\perp$

We get

$$\begin{aligned} & d(U^\perp, V^\perp) \\ = \ & \dim(U^\perp + V^\perp) - \dim(U^\perp \cap V^\perp) \\ = \ & \dim((U \cap V)^\perp) - \dim((U + V)^\perp) \\ = \ & N - \dim(U \cap V) - (N - \dim(U + V)) \\ = \ & \dim(U + V) - \dim(U \cap V) \\ = \ & d(U, V) \end{aligned}$$

Codes

$C \subseteq \mathcal{P}(W)$

$D(C) = \min\{d(X, Y) \mid X, Y \in C, X \neq Y\}$

Maximum dimension of C is
$l(C) = \max\{\dim(X) \mid X \in C\}$.

If all codewords are of the same dimension then constant dimension code

Parameters $[N, l(C), \log_q(|C|), D(C)]$.

N :	how many symbols per vector
$l(C)$:	how many vectors are needed
$\log_q(\|C\|)$:	how big is message space
$D(C)$:	error and erasure correction ability...

Minimum distance decoding

Given (received) word U a minimum distance decoder finds a codeword satisfying $d(V, U) < D(C)/2$ if such a word exists.

Theorem 2: Given $U \subseteq W$ and $V \in C$. If $d(U, V) < D(C)/2$ then the minimum distance decoder applied to U will return V.
Proof: Let T be any other codeword

$$D(C) \leq d(V, T) \leq d(V, U) + d(U, T)$$

but then

$$d(U, T) \geq D(C) - d(V, U) > D(C)/2$$

(See also page 7 of Silva, Kschischang, Kötter, “A Rank Metric Approach...”)

Constant dimension codes

Denote by $\mathcal{P}(W, l)$ the set of subspaces of W of dimension l.

A code is said to be constant dimensional if $C \subseteq \mathcal{P}(W, l)$.

In the following ALL CODES ARE CONSTANT DIMENSIONAL

q-ary Gaussian coefficients

For $l \leq n$

$$\begin{bmatrix} n \\ l \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n_l+1} - 1)}{(q^l - 1)(q^{l-1} - 1) \cdots (q - 1)}$$

Fact: $\begin{bmatrix} n \\ l \end{bmatrix}_q$ is the number of distinct l-dimensional subspaces of an n-dimensional vector space over $\mathbf{F}_q$.

Fact: $q^{l(n-l)} < \begin{bmatrix} n \\ l \end{bmatrix}_q < 4q^{l(n-l)}$

Singleton bound

Theorem 9: A q-ary code $C \subseteq \mathcal{P}(W, l)$ of type $[N, l, \log_q(|C|), D]$ must satisfy

$$|C| \quad \leq \quad \begin{bmatrix} N - (D-2)/2 \\ \max\{l, N-l\} \end{bmatrix}_q$$

To prepare for the proof we define a puncturing operation on C.

Recall, $\dim(W) = N$. Let $W' \subseteq W$ be of dimension $N - 1$.

The punctured code $C' = C|_{W'}$ is found by replacing each $V \in C$ with V' where $V' = V \cap W'$ in case this is of dimension $l - 1$.
Otherwise we choose V' to be any subspace of $V = V \cap W'$ of dimension $l - 1$.

Lemma (Theorem 8): Consider D with $D > 2$. $C' = C|_{W'}$ is a code of type $[N-1, l-1, \log_q(|C|), D']$ with $D' \geq D - 2$.

Proof: Given $U, V \in C$ consider U', V'.
By construction $(U' \cap V') \subseteq U \cap V$
and therefore $2\dim(U' \cap V') \leq 2\dim(U \cap V)$.
But $D \leq d(U, V) = 2l - 2\dim(U \cap V)$.
Hence, $-2\dim(U' \cap V') \geq D - 2l$
and therefore

$$\begin{aligned} d(U', V') &= 2(l-1) - 2\dim(U' \cap V') \\ &\geq 2l - 2 + (D - 2l) = D - 2 \end{aligned}$$

In particular no two different codewords U, V are mapped to the same codeword in C'.

Proof of Singleton bound

We can puncture the code C at least $(D-2)/2$ times without changing the code size (no collapsing).

After these puncturings all codewords are subspaces of a space $W^{\prime\prime\cdots\prime} = W^{(D-2)/2}$ which is of dimension $N-(D-2)/2$.

The number of subspaces of $W^{(D-2)/2}$ of size $N-l$ equals

$$\begin{bmatrix} N-(D-2)/2 \\ l-(D-2)/2 \end{bmatrix}_q = \begin{bmatrix} N-(D-2)/2 \\ N-l \end{bmatrix}_q$$

The “other result” comes by considering dual codes.

Linearized Polynomials

Let $\mathbf{F} = \mathbf{F}_{q^m}$. A linearized polynomial over $\mathbf{F}$ is a polynomial

$L(X) = \sum_{i=0}^{d} a_i X^{q^i}$, $a_i \in \mathbf{F}$

$L_1(X), L_2(X)$ linearized then also $L_1(X) + L_2(X)$ and
$L_1(X) \otimes L_2(X) = L_1(L_2(X))$

If $\deg(L_1) = q^{d_1}$ and $\deg(L_2) = q^{d_2}$ then $\deg(L_1 \otimes L_2) = q^{d_1+d_2}$.

If $\beta_1, \beta_2 \in \mathbf{F}$ and $\lambda_1, \lambda_2 \in \mathbf{F}_q$ then
$L(\lambda_1\beta_1 + \lambda_2\beta_2) = \lambda_1 L(\beta_1) + \lambda_2 L(\beta_2)$

Lemma 11: Assume L_1, L_2 with $\deg(L_1), \deg(L_2) < q^d$. If $\alpha_1, \ldots, \alpha_d \in \mathbf{F} = \mathbf{F}_{q^m}$ are linearly independent over $\mathbf{F}_q$ and $L_1(\alpha_i) = L_2(\alpha_i)$ holds for $i = 1, \ldots, d$, then $L_1 = L_2$.

Proof: First assumption implies that $L_1 - L_2$ cannot have more than q^{d-1} zeros. Second assumption implies that $L_1 - L_2$ has at least q^d zeros.

Kötter-Kschischang codes (KK-codes)

$\mathbf{F} = \mathbf{F}_{q^m}$ can be viewed as an m-dimensional vector space over $\mathbf{F}_q$.

Let $A = \{\alpha_1, \ldots, \alpha_l\} \subseteq \mathbf{F}$ be linearly independent over $\mathbf{F}_q$.

Ambient space

$$\begin{aligned} W &= \langle A \rangle \times \mathbf{F} \\ &= \{(\alpha, \beta) \mid \alpha \in \langle A \rangle, \beta \in \mathbf{F}\} \end{aligned}$$

is of dimension $l + m$

Encoding

Message $\vec{u} = (u_o, \dots, u_{k-1}) \in \mathbf{F}^k$
(this corresponds to q^{mk} symbols in $\mathbf{F}_q$!)

$$f(X) = \sum_{i=0}^{k-1} u_i X^{q^i}$$

$V = \langle (\alpha_1, f(\alpha_1)), \dots, (\alpha_l, f(\alpha_l)) \rangle \subseteq W$

Fact: If $|A| \geq k$ then no two different messages give the same space.

Assume therefore always $l \geq k$

So far $N = l + m$, $l(C) = l = constant$, $\log_q(C) = mk$. What about D?

Lemma 13: If $\{(\alpha'_1, f(\alpha'_1)), \ldots, (\alpha'_r, f(\alpha'_r))\} \subseteq W$ is linearly independent for some linearized polynomial f over $\mathbf{F}$ then $\{\alpha'_1, \ldots, \alpha'_r\}$ is also linearly independent (over $\mathbf{F}_q$)

Proof: Assume $\gamma_1, \ldots, \gamma_r \in \mathbf{F}_q$ and $\gamma_1\alpha'_1 + \cdots + \gamma_r\alpha'_r = 0$. Then in W, we have

$$\begin{aligned} \sum_{i=1}^{r} \gamma_i(\alpha'_i, f(\alpha'_i)) &= (0, \sum_{i=1}^{r} \gamma_i f(\alpha'_i)) \\ &= (0, f\big(\sum_{i_1}^{r} \gamma_i \alpha'_i)\big) \\ &= (0, f(0)) = (0, 0) \end{aligned}$$

By the assumption in the lemma we conclude $\gamma_1 = \cdots = \gamma_r = 0$

The minimum distance

Theorem 14: $D = 2(l - k + 1)$

Proof: Given f, g linearized and of degree at most q^{k-1} the codewords are

$$U = \langle(\alpha_1, f(\alpha_1)), \cdots, (\alpha_l, f(\alpha_l))\rangle$$

$$V = \langle(\alpha_1, g(\alpha_1)), \cdots, (\alpha_l, g(\alpha_l))\rangle$$

Let $r = \dim(U \cap V)$. Then we can find r linearly independent elements

$$(\alpha'_1, \beta'_1), \ldots, (\alpha'_r, \beta'_r)$$

such that $f(\alpha'_i) = g(\alpha'_i)$ for $i = 1, \ldots, r$ (they span $U \cap V$).

Proof cont.

It follows from Lemma 13 that $\alpha'_1, \ldots, \alpha'_r$ are linearly independent.

As f and g linearized polynomials, all linear combinations of $\alpha'_1, \ldots, \alpha'_r$ are zeros of $f - g$.

But $\deg(f - g) \leq q^{k-1}$ and our first conclussion is

$$r \leq k - 1$$

Recall $d(U, V) = 2l - 2\dim(U \cap V)$.

In conclusion

$$D \geq 2l - 2(k-1) = 2(l - k + 1)$$

According to the Singleton bound a code with $N = mk$, $l = l$, and $D = 2(l - k + 1)$ can have at most size

$$|C| \quad \leq \quad \begin{bmatrix} N - (D-2)/2 \\ l - (D-2)/2 \end{bmatrix}_q = \begin{bmatrix} m+k \\ k \end{bmatrix}_q < 4q^{mk}$$

So KK codes are nearly optimal.

Decoding

Assume $V = \langle(\alpha_1, f(\alpha_1)), \ldots, (\alpha_l, f(\alpha_l))\rangle$ is transmitted and U is received with
$\dim(U \cap V) = l - \rho$ and $U = (U \cap V) \oplus E$, where $t = \dim(E)$.

Write $r = \dim(U) = l - \rho + t$.

Let $\{(x_1, y_1), \ldots, (x_r, y_r)\}$ be a basis for U.

Assume

$$\rho + t < D/2 = l - k + 1 \tag{1}$$

Whether or not (1) holds, the receiver knows r and k and can calculate

$$\tau = \lceil (r + k)/2 \rceil$$

Decoding cont.

Assumption (1) implies $l - \rho \geq t + k$. Therefore

$$r + k = (l - \rho + t) + k = (l - \rho) + (t + k) \leq 2(l - \rho)$$

Hence,

$$r < 2\tau - k + 1 \tag{2}$$

and under assumption (1) also

$$\tau \leq l - \rho \tag{3}$$

Decoding algorithm

When U is received the receiver determines τ.
Then the receiver finds

$$Q(X,Y) = Q_X(X) + Q_Y(Y)$$

such that

1. Q_X is linearized of degree at most $q^{\tau-1}$
2. Q_Y is linearized of degree at most $q^{\tau-k}$
3. $Q(x_i, y_i) = 0$ for all $i = 1, \ldots, r$

This is doable as the number of variables is $2\tau - k + 1$ which by (2) exceeds the number of equations.

Decoding algorithm cont.

Let $\{(a_1, b_1), \ldots, (a_{l-\rho}, b_{l-\rho})\}$ be a basis for $U \cap V$.

Since all elements of U are zeros of $Q(X, Y)$
and $b_i = f(a_i)$, $i = 1, \ldots, l - \rho$ we have

$$Q(a_i, b_i) = Q(a_i, f(a_i)), \; i = 1, \ldots, l - \rho.$$

$$Q(X, f(X)) = Q_X(X) + Q_Y(X) \otimes f(X)$$
is linearized of degree at most $q^{\tau-1}$ having at least $q^{l-\rho}$ zeros.
By (3) this implies

$$Q_X(X) + Q_Y)X) \otimes f(X) = 0.$$

Kötter, Kschischang give a (non commutative) division algorithm to divide $Q_X(X)$ with $Q_Y(X)$ to obtain $f(X)$