Network Coding and Related Combinatorial Structures

Tuvi Etzion

Lecture 6

Error-Correcting Codes in Network Coding
Error-Correction for Network Coding

Outline

- Metrics for Error-Correction
- The Projective Space
- Rank-metric codes
- Lifting of Rank-metric codes
Network Coding with Errors

Min-cut can be smaller than the number of packets sent by the receiver.

$T$ packets of length $N$ are injected to the network.

$M$ packets of length $N$ over $\mathbb{F}_q$ sent, $L$ obtained.

$Y = A \cdot X + D \cdot Z$

- $Y$ size $L \times N$
- $A$ size $L \times M$
- $X$ size $M \times N$
- $D$ size $L \times T$
- $Z$ size $T \times N$

$T$ packets of length $N$ are injected to the network.
Noncoherent Network Coding

$T$ packets of length $N$ are injected to the network.

$M$ packets of length $N$ over $\mathbb{F}_q$ sent, $L$ obtained.

$Y = AX + DZ$

$Y$ size $L \times N$

$A$ size $L \times M$

$X$ size $M \times N$

$D$ size $L \times T$

$Z$ size $T \times N$

The transfer matrices $A$ and $D$ are random.
The Operator Channel

\[ M \text{ packets of length } N \text{ over } \mathbb{F}_q \text{ sent, } L \text{ obtained.} \]

\[ Y = A \cdot X + D \cdot Z \]

The row span of \( X \) represents the packets sent by the source. The specific basis that was sent is replaced by the subspace they span.
The Operator Channel

$W$ is a fixed $N$-dimensional vector space over $\mathbb{F}_q$. For simplicity we assume without loss of generality that $W = \mathbb{F}_q^n$. All transmitted and received packets are vectors of $W$. $P(W)$ is the set of all subspaces of $W$ and it is called the projective space or the projective geometry of $W$.

A code $C$ is a subset of $P(W)$. 

The Operator Channel

\( X, Y \in P(W) \)

\( \dim X \) - the dimension of \( X \).

\( X + Y = \{ x + y : x \in X, y \in Y \} \) - the sum of \( X \) and \( Y \).

\( X \cap Y = \{ 0 \} \) - \( X \) and \( Y \) have trivial intersection (disjoint).

\( X \cap Y = \{ 0 \}, X \oplus Y = X + Y \) - the direct sum of \( X \) and \( Y \).
The Operator Channel

\( X, Y \in P(W) \)

\( A_k \) - the erasure operator operates on subspaces of \( P(W) \). If \( \dim X > k \) then \( A_k(X) \) returns a randomly chosen \( k \)-dimensional subspace of \( X \). If \( \dim X \leq k \) then \( A_k(X) \) returns \( X \).

The operator channel associated with the ambient space \( W \). The input \( X \) and the output \( Y \) satisfy

\[
Y = A_k(X) \oplus E
\]

where \( k = \dim (X \cap Y) \) and \( E \) is an error space. The operator channel commits \( \rho = \dim X - k \) erasures and \( t = \dim E \) errors.
A metric $d$ on a set $V$ is a function $d: V \times V \to \mathbb{R}$ which satisfies the following three axioms:

• $d(x, y) = 0$ if and only if $x = y$ (coincidence)

• $d(x, y) = d(y, x)$ (symmetry)

• $d(x, z) \leq d(x, y) + d(y, z)$ (triangle inequality)
The subspace distance

\[ X, Y \in P_q(n) \Rightarrow d_S(X, Y) = \dim (X + Y) - \dim (X \cap Y) \]

\[ \dim (X + Y) = \dim X + \dim Y - \dim (X \cap Y) \]

\[ d_S(X, Y) = \dim X + \dim Y - 2\dim (X \cap Y) \]
\[ d_S(X, Y) = 2\dim (X + Y) - \dim X - \dim Y \]

\[ P_q(n) = P(\mathbb{F}_q^n) \]
The function \( d_S(X, Y) = \dim (X + Y) - \dim (X \cap Y) \) is a metric for the space \( P(W) \).

**Proof**

The coincidence and symmetry axioms are trivial. We have to prove the triangle inequality.

\[
d_S(X, Z) - d_S(X, Y) - d_S(Y, Z) \\
= 2(\dim (X \cap Y) + \dim (Z \cap Y) - \dim (X \cap Z) - \dim Y) \\
= 2(\dim ((X \cap Y) + (Z \cap Y)) - \dim Y) \\
+ 2(\dim (X \cap Z \cap Y) - \dim (X \cap Z)) \leq 0
\]
A minimum distance decoder for code $\mathbb{C}$ is one that takes an output $Y$ and returns a nearest codeword $X \in \mathbb{C}$ satisfying that for all $X' \in \mathbb{C}$ we have $d_S(Y, X) \leq d_S(Y, X')$.

Assume we use a code $\mathbb{C}$ with minimum distance $d_S(\mathbb{C})$ over an operator channel. Assume $X \in \mathbb{C}$ was transmitted and $Y = A_k(X) \oplus E$ was received, where $\dim E = t$. $\max\{0, \dim X - k\} = \rho$ denote the number of erasures induced by the channel. If $2(t + \rho) < d_S(\mathbb{C})$ then a minimum distance decoder of $\mathbb{C}$ will produce the transmitted subspace $X$ from the received subspace $Y$. 
A code \( \mathbb{C} \) with minimum distance \( d_S(\mathbb{C}) \) was used over an operator channel. \( X \in \mathbb{C} \) was transmitted and \( Y = A_k(X) \oplus E \) was received, where \( \dim E = t \). \( \max\{0, \dim X - k\} = \rho \) denote the number of erasures occurred. If \( 2(t + \rho) < d_S(\mathbb{C}) \) then a minimum distance decoder of \( \mathbb{C} \) will produce the transmitted subspace \( X \) from the received subspace \( Y \).

Let \( X' = A_k(X) \). From the triangle inequality \( d_S(X, Y) \leq d_S(X, X') + d_S(X', Y) \leq \rho + t \).

If \( Z \neq X \) is another codeword in \( \mathbb{C} \), then \( d_S(\mathbb{C}) \leq d_S(X, Z) \leq d_S(X, Y) + d_S(Y, Z) \)
from which it follows that \( d_S(Y, Z) \geq d_S(\mathbb{C}) - d_S(X, Y) \geq d_S(\mathbb{C}) - (\rho + t) \).

Hence, if \( 2(\rho + t) < d_S(\mathbb{C}) \) then \( \rho + t < d_S(Y, Z) \) which implies that \( d_S(Y, Z) > d_S(Y, X) \) and a minimum distance decoder will produce \( X \).
The Grassmannian

\[ P_q(n) \] is the projective space \( P(\mathbb{F}_q^n) \).

\[ G_q(n, k) \] is the set of all \( k \)-dimensional subspaces of \( P_q(n) \) (the Grassmannian).

Gaussian coefficients (\( q \)-binomial coefficient)

\[
\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\ldots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\ldots(q-1)}
\]

\[ |G_q(n, k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q \]
The Grassmannian

Theorem

\[ |G_q(n, k)| = \binom{n}{k}_q \]

Proof

There are \( \frac{q^n-1}{q-1} \) possible choices to choose the first vector as a basis for a \( k \)-dimensional subspace. For the second vector we have \( \frac{q^n-1}{q-1} - 1 = \frac{q^n-q}{q-1} \) different choices. The third vector has \( \frac{q^n-1}{q-1} - \frac{q^2-1}{q-1} = \frac{q^n-q^2}{q-1} \) possible choices and so on. The \( k \)th vector has \( \frac{q^n-q^{k-1}}{q-1} \) different choices. A total of \( \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q-1)^k} \) choices.
Now we will compute how many times a $k$-dimensional subspace $X$ was formed in this way. The first vector of $X$ can be chosen in \( \frac{q^k-1}{q-1} \) different ways, the second in \( \frac{q^k-q}{q-1} \) ways and the last one in \( \frac{q^k-q^{k-1}}{q-1} \) ways. A total of \( \frac{(q^k-1)(q^k-q) \ldots (q^k-q^{k-1})}{(q-1)^k} \) different ways. Thus, the number of different $k$-dimensional subspaces of $G_q(n,k)$ is

\[
\frac{(q^n-1)(q^n-q) \ldots (q^n-q^{k-1})}{(q^k-1)(q^k-q) \ldots (q^k-q^{k-1})} = \frac{(q^n-1)(q^{n-1}-1) \ldots (q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1) \ldots (q-1)} = \left[ n \right]_q
\]
The Grassmannian

**Theorem**

\[ q^{k(n-k)} < \binom{n}{k}_q < 4 \cdot q^{k(n-k)} \]

**Proof**

The number of \( k \)-dimensional subspaces of \( \mathbb{F}_q^n \) that occur as the row space of a matrix \( [I A] \), where \( I \) is a \( k \times k \) identity matrix and \( A \) is an arbitrary \( k \times (n-k) \) matrix over \( \mathbb{F}_q \). This proves the left side of the inequality.
The Grassmannian

**Theorem**

\[ q^{k(n-k)} < \left[ \begin{array}{c} n \\ k \end{array} \right]_q < 4 \cdot q^{k(n-k)} \]

**Proof**

\[
\left[ \begin{array}{c} n \\ k \end{array} \right]_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}
\]
\[
= q^{k(n-k)} \frac{(1 - q^{-n})(1 - q^{-n+1}) \cdots (1 - q^{-n+k-1})}{(1 - q^{-k})(1 - q^{-k+1}) \cdots (1 - q^{-1})}
\]
\[
< q^{k(n-k)} \frac{1}{(1 - q^{-k})(1 - q^{-k+1}) \cdots (1 - q^{-1})} < q^{k(n-k)} \prod_{j=1}^{\infty} \frac{1}{(1 - q^{-j})}
\]
\[
\prod_{j=1}^{\infty} \frac{1}{1-q^{-j}} \leq \prod_{j=1}^{\infty} \frac{1}{1-2^{-j}} = \frac{1}{Q_0} < 4 , \quad Q_0 \approx 0.288788095
\]
Network Coding and Related Combinatorial Structures

A SHORT BREAK
Adversarial Channel

\( T \) packets of length \( N \) are injected to the network.

\( M \) packets of length \( N \) over \( \mathbb{F}_q \) sent, \( L \) obtained.

\[
Y = A \cdot X + D \cdot Z
\]

\( Y \) size \( L \times N \)

\( A \) size \( L \times M \)

\( X \) size \( M \times N \)

\( D \) size \( L \times T \)

\( Z \) size \( T \times N \)

\( N \geq M, \quad L \geq M, \quad M \geq T \)
Coherent Network Coding

\[ Y = A \cdot X + D \cdot Z \]

- **A size** $L \times M$
- **X size** $M \times N$
- **D size** $L \times T$
- **Z size** $T \times N$

**Y size** $L \times N$

- **N \geq M, L \geq M, M \geq T**

**A is fixed and known to the receiver.**

**D and Z are arbitrarily chosen by an adversary who knows A and X.**

**T < M (T < \text{rank } A = M) \Rightarrow D \cdot Z \neq -A \cdot X**
Let $A, B$ be two $k \times m$ matrices over $\mathbb{F}_q$. The rank distance between $A$ and $B$ is defined by

$$d_R(A, B) = \text{rank} \ (A - B)$$

A $[k \times m, q, \delta]_q$ code $C$ is a linear code with dimension $q$, whose codewords are $k \times m$ matrices over $\mathbb{F}_q$ whose minimum rank distance is $\delta$. In other words this is a rank-metric code for which each two distinct codewords $A$ and $B$ satisfy $d_R(A, B) \geq \delta$.

A $[k \times m, q, \delta]_q$ code satisfies

$$q \leq \min\{k(m - \delta + 1), m(k - \delta + 1)\}$$
Lemma

\[ |\text{rank } A - \text{rank } B| \leq \text{rank } (A + B) \leq \text{rank } A + \text{rank } B. \]

Lemma

\[ d_R(A, B) = \text{rank } (A - B) \text{ is a metric for the set of } k \times m \text{ matrices over } \mathbb{F}_q. \]

Proof

The coincidence and symmetry axioms are trivial. For the triangle inequality, let \( X, Y, Z \) be \( k \times m \) matrices over \( \mathbb{F}_q \).

\[
\begin{align*}
d_R(X, Z) &= \text{rank } (X - Z) \\
&= \text{rank } ((X - Y) + (Y - Z)) \\
&\leq \text{rank } (X - Y) + \text{rank } (Y - Z) \\
&= d_R(X, Y) + d_R(Y, Z)
\end{align*}
\]
Lemma
\[ \delta_A(X, Z) = d_R(AX, AZ), \text{ where } A \text{ is of full column rank, is a metric.} \]

Proof
The coincidence and symmetry axioms are trivial. For the triangle inequality,
\[
\delta_A(X, Z) = d_R(AX, AZ) \\
\leq d_R(AX, AY) + d_R(AY, AZ) \\
= \delta_A(X, Y) + \delta_A(Y, Z)
\]

If \( A \) is not of full column rank then there exists two different matrices \( X, Z \) such that \( A(X - Z) = 0 \), i.e., \( \delta_A(X, Z) = 0 \), and the coincidence axiom cannot hold.
A code $C$ with minimum distance $\delta_A(C)$ was used over an adversarial channel. $X$ such that $AX \in C$ was transmitted and $Y = AX + DZ$ was received, where $\dim \langle Z \rangle = t$. If $2t < \delta_A(C)$ then a minimum distance decoder of $C$ will produce the transmitted matrix $X$ from the received matrix $Y$.

Since at most $t$ errors occurred we have $d_R(AX, Y) \leq t$.

If $Z \neq X$ is another codeword in $C$, then

$$2t + 1 \leq \delta_A(C) \leq d_A(X, Z) = d_R(AX, AZ) \leq d_R(AX, Y) + d_R(Y, AZ) \leq t + d_R(Y, AZ).$$

From which it follows that

$$t + 1 \leq 2t + 1 - d_R(AX, Y) \leq d_R(Y, AZ).$$

Hence, if $2t < \delta_A(C)$ then $d_R(Y, AZ) > d_R(Y, AX)$ and a minimum distance decoder will produce $X$. 
A \([k \times m, \varphi, \delta]_q\) code satisfies
\[\varphi \leq \min\{k(m - \delta + 1), m(k - \delta + 1)\}\]

There exists a \([k \times m, \varphi, \delta]_q\) code which satisfies
\[\varphi = \min\{k(m - \delta + 1), m(k - \delta + 1)\}\]

If \(A\) is an \(k \times m\) matrix then \([IA]\) is a generator matrix of a \(k\)-dimensional subspace of \(\mathbb{F}_q^{m+k}\).

If \(C\) is a \([k \times m, \varphi, \delta]_q\) code then \(C = \{\langle [I \ X] \rangle : X \in C\}\) is a code in \(G_q(m + k, k)\) with \(d_S(C) = 2\delta\).
**Rank-Metric Codes**

**Lemma**

If $A$ is an $k \times m$ matrix then $[I A]$ is a generator matrix of a $k$-dimensional subspace of $\mathbb{F}_q^{m+k}$.

The subspace $\langle [I A] \rangle$ is called the lifting of $A$.

**Theorem**

If $C$ be a $[k \times m, q, \delta]_q$ code then $C = \{ \langle [I X] \rangle : X \in C \}$ is a code in $G_q(m + k, k)$ with $d_S(C) = 2\delta$.

The code $C = \{ \langle [I X] \rangle : X \in C \}$ is the lifting of $C$. 
The injection distance

\[ X, Y \in P_q(n) \Rightarrow d_I(X, Y) = \max \{\dim X, \dim Y\} - \dim (X \cap Y) \]

\[ \dim (X + Y) = \dim X + \dim Y - \dim (X \cap Y) \]

\[ d_I(X, Y) = \dim (X + Y) - \min \{\dim X, \dim Y\} \]
Metrics in Projective Space

**Lemma**

\[ d_I(X, Y) = \max\{\dim X, \dim Y\} - \dim (X \cap Y) \]

is a metric for the space \( P(W) \).

**Proof**

The coincidence and symmetry axioms are trivial. For the triangle inequality, let \( X, Y, Z \in P(W) \) and without loss of generality assume that \( \dim X \leq \dim Z \).

\[
\begin{align*}
&d_I(X, Y) + d_I(Y, Z) - d_I(X, Z) \\
= &\max \{\dim X, \dim Y\} - \dim \{X \cap Y\} \\
&+ \max \{\dim Y, \dim Z\} - \dim \{Y \cap Z\} \\
&- \max \{\dim X, \dim Z\} + \dim \{X \cap Z\} \\
\geq &\max \{\dim X, \dim Y\} + \max \{\dim Y, \dim Z\} - \dim Z \\
&- \dim \left( (X + Z) \cap Y \right) - \dim (X \cap Z \cap Y) + \dim \{X \cap Z\}
\end{align*}
\]
**Lemma**

\[ d_I(X, Y) = \max\{\dim X, \dim Y\} - \dim (X \cap Y) \] is a metric for the space \( P(W) \).

**Proof**

For the triangle inequality, let \( X, Y, Z \in P(W) \) and without loss of generality assume that \( \dim X \leq \dim Z \).

\[
\begin{align*}
    d_I(X, Y) + d_I(Y, Z) - d_I(X, Z) &\geq \max \{\dim X, \dim Y\} + \max \{\dim Y, \dim Z\} - \dim Z \\
    &- \dim ((X + Z) \cap Y) - \dim (X \cap Z \cap Y) + \dim \{X \cap Z\} \\
    &= \max \{\dim Y, \dim Z\} - \dim Z \\
    &+ \max \{\dim X, \dim Y\} - \dim ((X + Z) \cap Y) \\
    &- \dim (X \cap Z \cap Y) + \dim \{X \cap Z\} \geq 0
\end{align*}
\]
A code $\mathbb{C}$ with minimum distance $d_I(\mathbb{C})$ was used over an adversarial channel. The codeword $\langle X \rangle \in \mathbb{C}$ was transmitted and $\langle Y \rangle$, where $Y = AX + DZ$, $\dim \langle Z \rangle = t$, was received. Let $\text{rank } X - \text{rank } A = \rho$ denote the number of erasures occurred. If $2t + \rho < d_I(\mathbb{C})$ then a minimum distance decoder for $\mathbb{C}$ will produce the transmitted subspace $\langle X \rangle$ from $\langle Y \rangle$.

Let $X' = AX$ such that $d_I(\langle X' \rangle, \langle Y \rangle) \leq t$ (clearly, $\dim \langle X' \rangle \geq \dim \langle X \rangle - \rho$).

If $\langle Z \rangle \neq \langle X \rangle$ is another codeword in $\mathbb{C}$ and $Z' = AZ$, then $d_I(\langle X \rangle, \langle Z \rangle) = \max \{ \dim \langle X \rangle, \dim \langle Z \rangle \} - \dim (\langle X \rangle \cap \langle Z \rangle) > 2t + \rho$ and if $Z' = AZ$ then $\dim \langle Z' \rangle \geq \dim \langle Z \rangle - \rho$ and $\dim (\langle X' \rangle \cap \langle Z' \rangle) \leq \dim (\langle X \rangle \cap \langle Z \rangle)$. 

Proof

Let \( X' = AX \) such that \( d_I(\langle X' \rangle, \langle Y \rangle) \leq t \) (clearly, \( \dim \langle X' \rangle \geq \dim \langle X \rangle - \rho \)).

If \( Z \neq X \) is other codeword in \( C \) and \( Z' = AZ \), then
\[
d_I(X, Z) = \max \{ \dim \langle X \rangle, \dim \langle Z \rangle \} - \dim (\langle X \rangle \cap \langle Z \rangle) > 2t + \rho
\]
and if \( Z' = AZ \) then \( \dim \langle Z' \rangle \geq \dim \langle Z \rangle - \rho \) and
\[
\dim (\langle X' \rangle \cap \langle Z' \rangle) \leq \dim (\langle X \rangle \cap \langle Z \rangle)
\]

Hence,
\[
d_I(\langle X' \rangle, \langle Z' \rangle) \geq \max \{ \dim \langle X' \rangle, \dim \langle Z' \rangle \} - \dim (\langle X' \rangle \cap \langle Z' \rangle)
\]
\[
\geq \max \{ \dim \langle X \rangle - \rho, \dim \langle Z \rangle - \rho \} - \dim (\langle X' \rangle \cap \langle Z' \rangle)
\]
\[
\geq \max \{ \dim \langle X \rangle, \dim \langle Z \rangle \} - \rho - \dim (\langle X \rangle \cap \langle Z \rangle) > 2t
\]

But,
\[
d_I(\langle X' \rangle, \langle Z' \rangle) \leq d_I(\langle Z' \rangle, \langle Y \rangle) + d_I(\langle Y \rangle, \langle X' \rangle)
\]
and hence, \( d_I(\langle Z' \rangle, \langle Y \rangle) \geq d_I(\langle X' \rangle, \langle Z' \rangle) - d_I(\langle Y \rangle, \langle X' \rangle) > t \).

Thus, the minimum distance decoder will produce \( \langle X \rangle \) from \( \langle Y \rangle \).
Three metrics

Coherent network coding - rank distance

Noncoherent network coding

At most $\ell = \rho + t$ erasures and errors - subspace distance $> 2(t + \rho)$.
At most $\rho$ erasures and at most $t$ errors - injection distance $> 2t + \rho$. 
Network Coding and Related Combinatorial Structures

END OF LECTURE 6