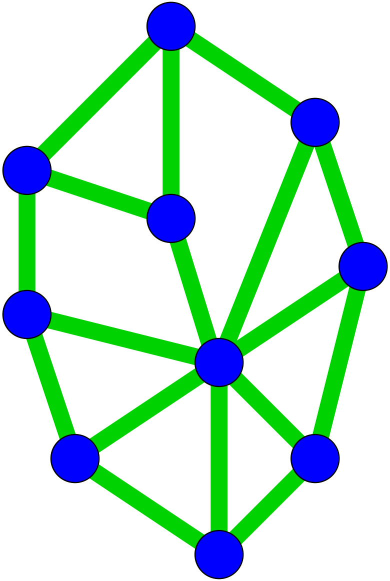
Coding for Errors and Erasures in Random Network Coding

Ralf Koetter
Technical University of Munich

joint work with
Frank R. Kschischang
University of Toronto

May 2, 2007

Random Network Coding



Random Network Coding

Consider a single unicast (one transmitter, one receiver).

1. Break a file into M fixed-length packets, each regarded as a vector over F_q, and inject these packets into the network.
2. Packets propagate through the network, possibly passing through intermediate nodes between transmitter and receiver.
3. When intermediate nodes are granted a transmission opportunity, they forward a random F_q-linear combination of packets seen so far.
4. The receiver essentially collects as many of these these randomly combined packets as possible and tries to infer what was sent.

What if there are errors?

N. Cai and R. W. Yeung, "Network coding and error correction," in *Proc. 2002 IE*
Inform. Theory Workshop, pp. 119–122, Oct. 20–25, 2002.

L. Song, R. W. Yeung, and N. Cai, "Zero-error network coding for acyclic network
IEEE Trans. on Inform. Theory, vol. 49, pp. 3129–3139, Dec. 2003.

R. W. Yeung and N. Cai, "Network error correction, part I: Basic concepts and up
bounds," *Comm. in Inform. and Systems*, vol. 6, no. 1, pp. 19–36, 2006.

R. W. Yeung and N. Cai, "Network error correction, part II: Lower bounds," *Com*
in Inform. and Systems, vol. 6, no. 1, pp. 37–54, 2006.

Z. Zhang, "Network error correction coding in packetized networks," in *Proc. 2006 IE*
Inform. Theory Workshop, Oct. 22–26, 2006.

S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard, "Resilient netwo
coding in the presence of Byzantine adversaries," in *Proc. 26th Annual IEEE Conf.*
+1in+1in *Computer Commun., INFOCOM*, (Anchorage, AK), May 6–12, 2007. (To appear.).

Random Network Coding

Let $\{p_1, p_2, \ldots, p_M\}, p_i \in F_q^N$ be the injected vectors.

In the error-free case, the receiver collects L packets $y_1, y_2, \ldots, y_L$, were

$$y_j = \sum_{i=1}^{M} h_{j,i} p_i,$$

where $h_{j,i} \in F_q$ are randomly chosen coefficients.

The number L of packets gathered is not fixed *a priori*.

Random Network Coding

Let $\{p_1, p_2, \ldots, p_M\}, p_i \in F_q^N$ be the injected vectors.

In the error-free case, the receiver collects L packets $y_1, y_2, \ldots, y_L$, were

$$y_j = \sum_{i=1}^{M} h_{j,i} p_i,$$

where $h_{j,i} \in F_q$ are randomly chosen coefficients.

The number L of packets gathered is not fixed *a priori*.

In the absence of errors:

$$y = Hp$$

where p is an $M \times N$ matrix over F_q whose rows are $p_1, p_2, \ldots, p_M$, and H is a random $L \times M$ matrix over F_q.

Random Network Coding

Let $\{p_1, p_2, \ldots, p_M\}, p_i \in F_q^N$ be the injected vectors.

In the error-free case, the receiver collects L packets $y_1, y_2, \ldots, y_L$, were

$$y_j = \sum_{i=1}^{M} h_{j,i} p_i,$$

where $h_{j,i} \in F_q$ are randomly chosen coefficients.

The number L of packets gathered is not fixed *a priori*.

In the absence of errors:

$$y = Hp$$

where p is an $M \times N$ matrix over F_q whose rows are $p_1, p_2, \ldots, p_M$, and H is a random $L \times M$ matrix over F_q.

Remark: Often p is chosen as $p = [I|A]$, so that $y = Hp = [H|HA]$ (prepend header).

Random Network Coding (cont'd)

We may also wish to model the injection of T erroneous packets $e_1, e_2, \ldots, e_t$ somewhere in the network, giving

$$y_j = \sum_{i=1}^{M} h_{j,i} p_i + \sum_{t=1}^{T} g_{j,t} e_t$$

where again $g_{j,t} \in F_q$ are random coefficients.

Random Network Coding (cont'd)

We may also wish to model the injection of T erroneous packets $e_1, e_2, \ldots, e_t$ somewhere in the network, giving

$$y_j = \sum_{i=1}^{M} h_{j,i} p_i + \sum_{t=1}^{T} g_{j,t} e_t$$

where again $g_{j,t} \in F_q$ are random coefficients.

In the presence of errors:

$$y = Hp + Ge$$

where

- p is an $M \times N$ matrix over F_q whose rows are $p_1, p_2, \ldots, p_M$,
- e is an $T \times N$ matrix over F_q whose rows are $e_1, e_2, \ldots, e_T$,
- H is a random $L \times M$ matrix over F_q,
- G is a random $L \times T$ matrix over F_q.

Remarks:

- Due to error propagation, the injection of even a single error packet has the potential to corrupt each and every received packet.
- The network topology will certainly impose structure on H and G (e.g., H may be rank-deficient due to a small min-cut between transmitter and receiver); however we will not attempt to exploit such structure.

The Key Idea

Q: Even if $e = 0$ (no errors), since H is random, what property of Hp is preserved to allow for information transmission?

The Key Idea

Q: Even if $e = 0$ (no errors), since H is random, what property of Hp is preserved to allow for information transmission?

A:

Each received packet is in the row space of p, i.e., Hp performs linear combinations of the rows of p.
In other words, *the row space of p is preserved*.

The Key Idea

Q: Even if $e = 0$ (no errors), since H is random, what property of Hp is preserved to allow for information transmission?

A:

Each received packet is in the row space of p, i.e., Hp performs linear combinations of the rows of p.
In other words, *the row space of p is preserved*.

We may therefore attempt to convey information by the selection at the transmitter of a vector space V. The transmitter conveys this selection by injection into the network of a basis for V. The receiver gathers vectors so as to be able to identify the selected space.

The Key Idea

Q: Even if $e = 0$ (no errors), since H is random, what property of Hp is preserved to allow for information transmission?

A:

Each received packet is in the row space of p, i.e., Hp performs linear combinations of the rows of p.
In other words, *the row space of p is preserved*.

We may therefore attempt to convey information by the selection at the transmitter of a vector space V. The transmitter conveys this selection by injection into the network of a basis for V. The receiver gathers vectors so as to be able to identify the selected space.

Remark: The setup is reminiscent of the noncoherent multiple antenna channel as studied, e.g., in [ZheTse02] ("Communication on the Grassmannian manifold"), only instead of working in $\mathbb{C}$ we work in F_q.

The Channel Model

Let W be an N-dimensional vector space over F_q^N. (Transmitted and received packets are elements of W.)

Let $\mathcal{P}(W)$ denote the set of all subspaces of W (sometimes called the projective geometry of W).

Definition

An *operator channel* associated with ambient space W is a channel with input and output alphabet $\mathcal{P}(W)$. The channel input V and channel output U are related as

$$U = \mathcal{H}_k(V) \oplus E$$

where $\mathcal{H}_k$ is an erasure operator, $E \in \mathcal{P}(W)$ is an arbitrary error space and $\oplus$ denotes direct sum. If $\dim(V) \geq k$, then $\mathcal{H}_k(V) = V$; otherwise $\mathcal{H}_k(V)$ acts to project V onto randomly chosen k-dimensional subspace of V.

A Metric

Let A and B be subspaces of W.

The *distance* between A and B is defined as

$$d(A, B) := \dim(A + B) - \dim(A \cap B).$$

$d(A, B)$ is equal to the the minimal number of insertions and deletions of generators that are required to transform a basis for A into a basis for B.

(Analogous to Hamming distance in classical coding theory, which is equal to the minimum number of symbol changes required to transform a vector A into a vector B.)

Codes

Definition

A *code* for an operator channel with ambient space $W \simeq F_q^N$ is a nonempty subset of $\mathcal{P}(W)$.

- The size of a code $\mathcal{C}$ is denoted $|\mathcal{C}|$.
- The minimum distance of $\mathcal{C}$ is denoted by

$$D(C) = \min_{X,Y \in \mathcal{C}, X \neq Y} d(X, Y)$$

- The maximum dimension of elements of $\mathcal{C}$ is denoted by

$$\ell(C) = \max_{X \in \mathcal{C}} \dim(X)$$

We say that C is a q-ary code of type $(N, \ell(C), \log_q |C|, D(C))$.

Minimum Distance Decoding

Definition

A *minimum distance decoder* for $\mathcal{C}$ takes the output U of an operator channel and returns a nearest codeword $V \in \mathcal{C}$, i.e., a codeword V satisfying, for all $X \in \mathcal{C}$, $d(U, V) \leq d(U, X)$.

Error-and-Erasure Correcting Capability

Theorem

Assume we use a code $\mathcal{C}$ for transmission over an operator channel. Let $V \in \mathcal{C}$ be transmitted, and let

$$U = \mathcal{H}_k(V) \oplus E$$

be received, where $\dim(E) = t$. Let $\rho = (\ell(\mathcal{C}) - k)_+$ denote the maximum number of erasures induced by the channel. If

$$2(t + \rho) < D(\mathcal{C}),$$

then a minimum distance decoder for $\mathcal{C}$ will produce the transmitted space V from the received space U.

Proof: standard application of the triangle inequality.

Remark: "erasures" (i.e., deletion of desired dimensions) cost the same as "errors" (i.e., insertion of undesired dimensions).

Coding in the Grassmann Graph

It is natural for random network coding applications to consider codes in which all codewords have the same dimension ℓ.

Definition

Let $\mathcal{P}(W, \ell)$ be the set subspaces of W of dimension ℓ (a Grassmannian). The Grassmann graph $G_{W,\ell}$ has vertex set $\mathcal{P}(W, \ell)$ with an edge joining vertices U and V if and only if $d(U, V) = 2$ (which means that $\dim(U \cap V) = \ell - 1$ or $\dim(U + V) = \ell + 1$).

The distance between any elements the Grassmann graph is an even integer. The diameter of the graph is 2ℓ.

Remark: It is well known [BroCohNeu89] that $G_{W,\ell}$ is distance-regular. The so-called *q*-Johnson association scheme arises from this graph. Virtually all techniques for bounding codes in the Hamming scheme (e.g., sphere-packing and sphere-covering concepts) apply here.

Code Rate

Let $\mathcal{C}$ be an $(N, \ell, \log_q |\mathcal{C}|, D)$ code. Transmission of a basis for a codeword requires transmission of up to $N\ell$ q-ary symbols.

Definition

The *rate* of a $(N, \ell, \log_q |\mathcal{C}, D)$ code is

$$R = \frac{\log_q |\mathcal{C}|}{N\ell}.$$

We also introduce the normalized parameters:

- the normalized weight: $\lambda = \ell/N \in [0, 1]$
- the normalized minimum distance $\delta = D/2\ell \in [0, 1]$

Examples of Codes

Example

(Classical "uncoded" network coding.)
Let $\mathcal{C}_1 \subset \mathcal{P}(W, \ell)$ be the set of spaces U having a generator matrix of the form $[I|A]$, where I is the $\ell \times \ell$ identity matrix.

This is a code of type $(N, \ell, \ell(N-\ell), 2)$ with normalized weight $\lambda = \ell/N$ and rate $R = 1 - \lambda$.

Examples of Codes

Example

(Classical "uncoded" network coding.)
Let $\mathcal{C}_1 \subset \mathcal{P}(W, \ell)$ be the set of spaces U having a generator matrix of the form $[I|A]$, where I is the $\ell \times \ell$ identity matrix.

This is a code of type $(N, \ell, \ell(N-\ell), 2)$ with normalized weight $\lambda = \ell/N$ and rate $R = 1 - \lambda$.

Example

("uncoded" network coding with strictly more codewords.)
Let $\mathcal{C}_2$ be $\mathcal{P}(W, \ell)$ itself.

This is a code of type $(N, \ell, \log_q |\mathcal{P}(W, \ell)|, 2)$ with strictly more codewords than $\mathcal{C}_1$.

Examples of Codes (cont'd)

Example

("uncoded" network coding with even more codewords)
Let $\mathcal{C}_3$ be $\bigcup_{i=1}^{\ell} \mathcal{P}(W, i)$.

Elementary Bounds

Gaussian Coefficients

For any non-negative integer i, define

$$[\![i]\!]_q := \begin{cases} 1 & \text{if } i = 0, \\ q^i - 1 & \text{if } i > 0. \end{cases},$$

and let

$$[\![i]\!]_q! := \prod_{j=0}^{i} [\![j]\!]_q.$$

Definition

The *Gaussian coefficient* $\begin{bmatrix} n \\ m \end{bmatrix}_q$ is defined as

$$\begin{bmatrix} n \\ m \end{bmatrix}_q := \begin{cases} \frac{[\![n]\!]_q!}{[\![m]\!]_q! [\![n-m]\!]_q!} & 0 \leq m \leq n \\ 0 & \text{otherwise.} \end{cases}$$

Theorem

The number of ℓ-dimensional subspaces of an N-dimensional vectors space over F_q equals $\begin{bmatrix} N \\ \ell \end{bmatrix}_q$.

Asymptotically, the Gaussian coefficient behaves as $q^{-\ell(n-\ell)}$.

Theorem

The Gaussian coefficient $\begin{bmatrix} n \\ \ell \end{bmatrix}_q$ satisfies

$$1 < q^{-\ell(n-\ell)} \begin{bmatrix} n \\ \ell \end{bmatrix}_q < 4$$

for $0 < \ell < n$.

Spheres in the Grassmann Graph

Let W be an N dimensional vector space and let $\mathcal{P}(W, \ell)$ be the set of ℓ dimensional subspaces of W.

Definition

The sphere $S(V, \ell, t)$ of radius $2t$ centered at a space V in $\mathcal{P}(W, \ell)$ is the set of all subspaces U that satisfy $d(U, V) \leq 2t$,

$$S(V, \ell, t) = \{U \in \mathcal{P}(W, \ell) | d(U, V) \leq 2t\}.$$

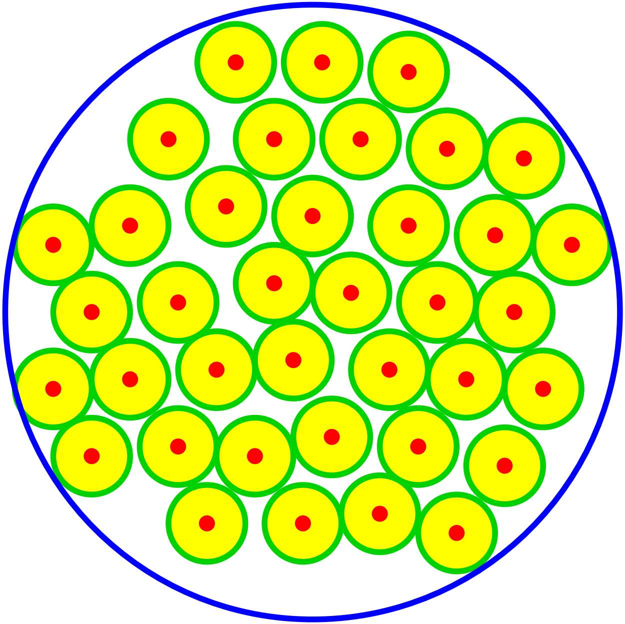
Theorem

The number of spaces in $S(V, \ell, t)$ is independent of V and equals

$$|S(V, \ell, t)| = \sum_{i=0}^{t} q^{i^2} \begin{bmatrix} \ell \\ i \end{bmatrix} \begin{bmatrix} N - \ell \\ i \end{bmatrix}$$

for $t \leq \ell$.

Sphere-Packing (Hamming) Bound



Sphere-Packing (Hamming) Bound

Let $\mathcal{C}$ be a collection of spaces in $\mathcal{P}(W,\ell)$ such that $D(\mathcal{C})$ is at least $2t$. Let $s = \lfloor \frac{t-1}{2} \rfloor$.

Theorem

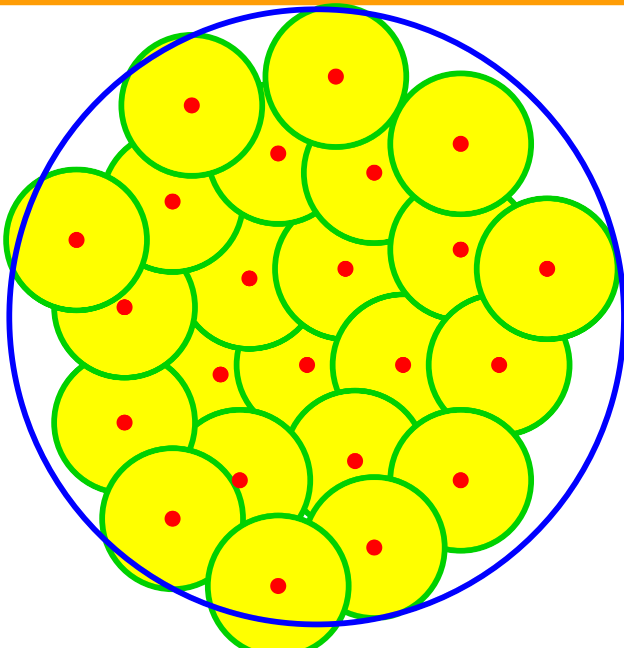
$$
\begin{aligned}
|\mathcal{C}| &\leq \frac{|\mathcal{P}(W,\ell)|}{|S(V,\ell,s)|} \\
&= \frac{\begin{bmatrix} N \\ \ell \end{bmatrix}}{|S(V,\ell,s)|} \\
&< 4q^{(\ell-s)(N-s-\ell)}
\end{aligned}
$$

In terms of normalized parameters R, λ and δ we have

$$R \leq (1-\delta/2)(1-\lambda(\frac{\delta}{2}+1)) + o(1),$$

where $o(1) \to 0$ as $N \to \infty$.

Sphere-Covering (Gilbert) Bound



Sphere-Covering (Gilbert) Bound

Theorem

There exists a code $\mathcal{C}'$ with distance $D(\mathcal{C}') \geq 2t$ such that

$$\begin{aligned} |\mathcal{C}'| &\geq \frac{|\mathcal{P}(W,\ell)|}{|S(V,\ell,t-1)|} \\ &= \frac{\begin{bmatrix} N \\ \ell \end{bmatrix}}{|S(V,\ell,t-1)|} \\ &> \frac{1}{16t} q^{(\ell-t+1)(N-t-\ell+1)} \end{aligned}$$

In terms of normalized parameters, there exists a code C' such that

$$R \geq (1-\delta)(1-\lambda(\delta+1)) + o(1).$$

Singleton Bound

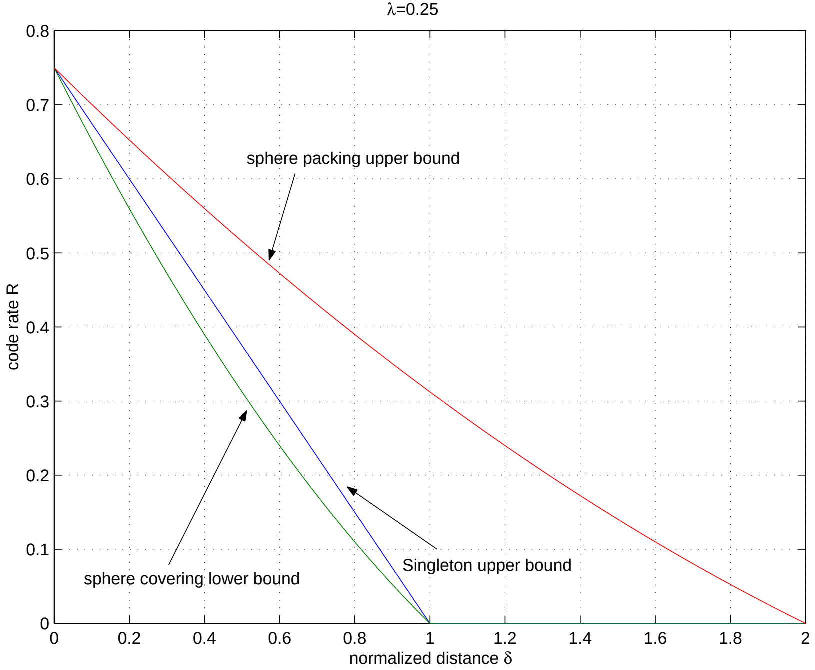
Theorem

A q-ary code $\mathcal{C} \subset \mathcal{P}(W, \ell)$ *of type* $(N, \ell, \log_q |\mathcal{C}|, D)$ *must satisfy*

$$|\mathcal{C}| \leq \begin{bmatrix} N - (D-2)/2 \\ \ell - (D-2)/2 \end{bmatrix}_q .$$

In terms of normalized parameters,

$$R \leq (1-\delta)(1-\lambda) - \frac{1}{\lambda N}(1 - \lambda + o(1))$$


λ=0.25
sphere packing upper bound
Singleton upper bound
sphere covering lower bound
code rate R
normalized distance δ
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
2

A Reed-Solomon-like Code Construction

Let F_q be a finite field and let F be an extension field.

Definition

A polynomial $L(x) \in F[x]$ is called a *linearized polynomial* with respect to F_q if

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

Linearized polynomials

If $L_1(x)$ and $L_2(x)$ are linearized polynomials, then so is $\alpha_1 L_1(x) + \alpha_2 L_2(x)$ for any $\alpha_1, \alpha_2 \in F$. The ordinary product $L_1(x)L_2(x)$ is *not* in general a linearized polynomial; however, the *composition*

$$L_1(x) \otimes L_2(x) := L_1(L_2(x))$$

does result in a linearized polynomial. Note that $L_1(x) \otimes L_2(x) \neq L_2(x) \otimes L_1(x)$ in general.

The set of linearized polynomials under $\otimes$ and $+$ forms a non-commutative ring.

Linearized polynomials (cont'd)

We may regard any extension K of F as a vector space over F_q. The map taking $\beta \in K$ to $L(\beta) \in K$ is *linear* w.r.t. F_q, i.e., for all $\beta_1, \beta_2 \in K$ and all $\lambda_1, \lambda_2 \in F_q$,

$$L(\lambda_1\beta_1 + \lambda_2\beta_2) = \lambda_1 L(\beta_1) + \lambda_2 L(\beta_2).$$

If K is large enough to contain all the zeros of $L(x)$. The zeros of $L(x)$ then correspond to the kernel of $L(x)$ regarded as a linear map, and hence they form a subspace of K. Conversely, each subspace of K corresponds to some linearized polynomial over K.

Linearized polynomials (cont'd)

We may regard any extension K of F as a vector space over F_q. The map taking $\beta \in K$ to $L(\beta) \in K$ is *linear* w.r.t. F_q, i.e., for all $\beta_1, \beta_2 \in K$ and all $\lambda_1, \lambda_2 \in F_q$,

$$L(\lambda_1\beta_1 + \lambda_2\beta_2) = \lambda_1 L(\beta_1) + \lambda_2 L(\beta_2).$$

If K is large enough to contain all the zeros of $L(x)$. The zeros of $L(x)$ then correspond to the kernel of $L(x)$ regarded as a linear map, and hence they form a subspace of K. Conversely, each subspace of K corresponds to some linearized polynomial over K.

Roughly speaking ...

linearized polynomials are to subspaces as polynomials are to points.

Encoding Procedure

Setup:

F_q is a finite field, $F = F_{q^m}$ is an extension field of F_q, regarded as a vector space of dimension m over F_q. Let $\alpha_1, \ldots, \alpha_\ell \in F$ be a set of linearly independent elements, that span a vector space A of dimension ℓ over F_q.

Encoding Procedure

Setup:

F_q is a finite field, $F = F_{q^m}$ is an extension field of F_q, regarded as a vector space of dimension m over F_q. Let $\alpha_1, \ldots, \alpha_\ell \in F$ be a set of linearly independent elements, that span a vector space A of dimension ℓ over F_q.

The User ...

... provides k elements u_0, u_1, ..., u_{k-1} in F; this is the message to be sent.

Encoding Procedure (cont'd)

The Encoder . . .

. . . forms the linearized polynomial

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

and evaluates $f(x)$ at the ℓ points $\alpha_1, \ldots, \alpha_\ell$ to form

$$\beta(i) = f(\alpha_i), i = 1, \ldots, \ell.$$

The set of pairs (α_1, β_1), (α_2, β_2), . . . , $(\alpha_\ell, \beta_\ell)$ is clearly a set of linearly independent vectors in $A \times F \simeq F_q^{\ell+m}$, and so is a basis for a vector space V of dimension ℓ. (The ambient space W is $F_q^{\ell+m}$.)

Encoding Procedure (cont'd)

The Encoder ...

...forms the linearized polynomial

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

and evaluates $f(x)$ at the ℓ points $\alpha_1, \ldots, \alpha_\ell$ to form

$$\beta(i) = f(\alpha_i), i = 1, \ldots, \ell.$$

The set of pairs (α_1, β_1), (α_2, β_2), ..., $(\alpha_\ell, \beta_\ell)$ is clearly a set of linearly independent vectors in $A \times F \simeq F_q^{\ell+m}$, and so is a basis for a vector space V of dimension ℓ. (The ambient space W is $F_q^{\ell+m}$.)

The Transmitter ...

...sends (a basis for) V over the operator channel.

Some Remarks

- Each pair α_i, β_i may be regarded as a zero of the bivariate polynomial $y - f(x)$. In fact, since $f(x)$ is linearized, every element of V is a zero of $y - f(x)$, since, for all $\lambda_1, \ldots, \lambda_\ell \in F_q$,

$$\begin{aligned}
\sum_{i=1}^{\ell} \lambda_i \beta_i - f\left(\sum_{i=1}^{\ell} \lambda_i \alpha_i\right) &= \sum_{i=1}^{\ell} \lambda_i \beta_i - \sum_{i=1}^{\ell} \lambda_i f(\alpha_i) \\
&= \sum_{i=1}^{\ell} \lambda_i (\beta_i - f(\alpha_i)) \\
&= 0
\end{aligned}$$

  which shows that $\sum_{i=1}^{\ell} \lambda_i(\alpha_i, \beta_i)$ is a zero of $y - f(x)$.
- Each distinct message polynomial gives rise to a distinct codeword, hence $|C| = q^{mk}$. Thus C is of type $(\ell + m, \ell, mk, D)$ with rate

$$R = \frac{mk}{\ell(\ell + m)} = \frac{k}{\ell} \frac{m}{m + \ell}.$$

Minimum Distance

Theorem

$$D(\mathcal{C}) = 2(\ell - k + 1)$$

Proof: Let U and V be two spaces obtained from distinct linearized polynomials $f_1(x)$ and $f_2(x)$, respectively. Suppose that $U \cap V$ has dimension a. This means it is possible to find a linearly independent elements $(\alpha'_1, \beta'_1), (\alpha'_2, \beta'_2), \dots, (\alpha'_a, \beta'_a)$ such that $f_1(\alpha'_i) = f_2(\alpha'_i) = \beta_i$. It is easy to show that $\alpha'_1, \dots, \alpha'_a$ must themselves be linearly independent. If $a \geq k$, then we would have two linearized polynomials of degree less than q^k that agree on a linearly independent points, which is only possible if the two polynomials coincide. Thus $a \leq k - 1$, so

$$d(U, V) = 2(\ell - a) \geq 2(\ell - k + 1).$$

Reed-Solomon-like Codes

This construction yields codes of type $(\ell + m, \ell, mk, 2(\ell - k + 1))$. In terms of normalized parameters, we find that

$$R = (1 - \lambda)(1 - \delta + \frac{1}{\lambda N})$$

which has the same asymptotic behavior as the Singleton bound.

Decoding

Suppose that V is sent and U, a space of dimension ℓ' is received. Let $(x_i, y_i), i = 1, \ldots, \ell'$ be a basis for U. Decoding may proceed as follows.

1. Construct a bivariate interpolating polynomial

$$Q(x, y) = \Lambda(y) + \Omega(x)$$

such that $Q(x_i, y_i) = 0$ for $i = 0, \ldots, l'$ with $\Lambda(y)$ is a monic linearized polynomial of degree q^t and $\Omega(x)$ is a linearized polynomial of degree at most $t + k - 1$, where $t = \lfloor (\ell' - k)/2 \rfloor$. [Such a polynomial can be proved to exist.]

Decoding (cont'd)

2. Note that

$$\begin{aligned} Q(x, f(x)) &= \Lambda(x) \otimes f(x) + \Omega(x) \\ &= \Lambda(y - f(x)) + Q(x, f(x)). \end{aligned}$$

If few enough errors occur, then $Q(x, f(x))$ will have many zeros (more than its degree), and so $Q(x, f(x))$ will be the zero polynomial, in which case $Q(x, y) = \Lambda(y - f(x))$ will have $y - f(x)$ as a factor.

3. $f(x)$ can be recovered via a division operation in the ring of linearized polynomials. to recover $f(x)$.

Conclusions

This paper:

Coding for random network coding

$$\Downarrow$$

Coding for operator channels

$$\Downarrow$$

Codes in the Grassmann graph

$$\Downarrow$$

Bounds, Code Constructions, Decoding Algorithms

Conclusions

This paper:

Coding for random network coding

$\Downarrow$

Coding for operator channels

$\Downarrow$

Codes in the Grassmann graph

$\Downarrow$

Bounds, Code Constructions, Decoding Algorithms

This seems to be a promising approach, with much work left to be done.