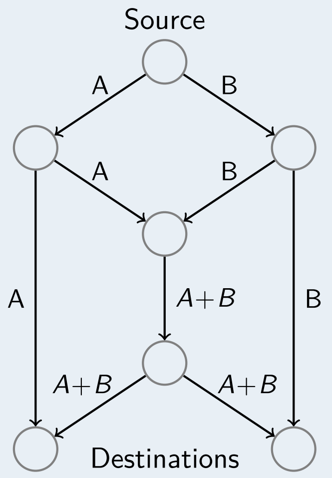
List and Probabilistic Unique Decoding of Folded Subspace Codes

Hannes Bartz, Vladimir Sidorenko

hannes.bartz@tum.de, vladimir.sidorenko@tum.de

Motivation



- The key idea of Random Linear Network Coding (RLNC) is to linearly combine ("mix") packets at the intermediate nodes

Benefit:
A higher throughput compared to routing can be achieved

Problem:
High error propagation due to linear combination of packets

Error Control in Random Linear Network Coding [1]

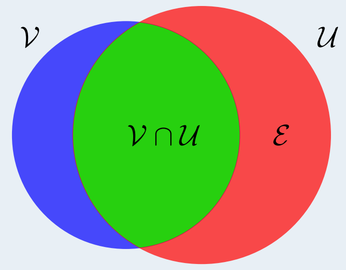
- The rowspace of the transmitted packets is preserved by the linear operations of the network
- Data can be transmitted by choosing a subspace and transmitting a basis of the subspace
- Topology and combinations don't have to be known by the transmitter and the receiver $\Rightarrow$ *non-coherent* coding
- Choosing subspaces that are separated with respect to a distance metric allows to correct errors and erasures

The Channel Model

As channel model we use the *operator channel* from [1]. Denote by $\mathbb{F}_q$ the finite field of order q and by $\mathbb{F}_{q^m}$ its extension field of degree m. Any element in $\mathbb{F}_{q^m}$ can be represented by a length m vector over $\mathbb{F}_q$.

$$\mathcal{V} \longrightarrow \boxed{\mathcal{H}_{n_t-\delta}(\mathcal{V}) \oplus \mathcal{E}} \longrightarrow \mathcal{U}$$

- **Input:** n_t-dimensional subspace $\mathcal{V}$ over $\mathbb{F}_q$
- $\mathcal{H}_{n_t-\delta}(\mathcal{V})$ returns a random $(n_t-\delta)$-dimensional subspace of $\mathcal{V}$
- γ-dimensional error space $\mathcal{E}$ (not contained in $\mathcal{V}$)
- **Output:** $(n_r = n_t - \delta + \gamma)$-dimensional subspace $\mathcal{U}$ over $\mathbb{F}_q$ $\Rightarrow$ δ deletions and γ insertions



Subspace Distance

The subspace distance between two subspaces $\mathcal{U}$ and $\mathcal{U}'$ is defined as

$$d_s(\mathcal{U},\mathcal{U}') = \dim(\mathcal{U} \oplus \mathcal{U}') - \dim(\mathcal{U} \cap \mathcal{U}')$$

Linearized Polynomials [2]

For any element $a \in \mathbb{F}_{q^m}$ and any integer i let $a^{[i]} \overset{\text{def}}{=} a^{q^i}$ be the Frobenius power of a. A nonzero polynomial of the form

$$p(x) = \sum_{i=0}^{d} p_i x^{[i]}$$

with $p_i \in \mathbb{F}_{q^m}$, $p_d \neq 0$, is called a *linearized polynomial* of q-degree $\deg_q(p(x)) = d$.

Folded Subspace Codes

Let α be a primitive element of $\mathbb{F}_{q^m}$ and let $\alpha^0, \alpha^1, \dots, \alpha^{n-1}$ be a polynomial basis of $\mathbb{F}_q^n$ with $n \le m$. Let β be a primitive element of $\mathbb{F}_{q^{n_t}}$ and let the representation of $(\beta^0, \beta^1, \dots, \beta^{n_t-1})^T$ over $\mathbb{F}_q$ form the identity matrix $\mathbf{I} \in \mathbb{F}_q^{n_t \times n_t}$. Let h be a positive integer that divides n and define $n_t = \frac{n}{h}$. For fixed integers n, k, h, an h-folded subspace code $\mathrm{FSub}[h; n, k]$ of dimension n_t is defined as

$$\begin{array}{|c|c|c|c|c|}
\beta^0 & f(\alpha^0) & f(\alpha) & \cdots & f(\alpha^{h-1}) \\
\beta^1 & f(\alpha^h) & f(\alpha^{h+1}) & \cdots & f(\alpha^{2h-1}) \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\beta^{n_t-1} & f(\alpha^{(n_t-1)h}) & f(\alpha^{(n_t-1)h+1}) & \cdots & f(\alpha^{n_t h-1})
\end{array}$$

where $f(x)$ is a *linearized polynomial* over $\mathbb{F}_{q^m}$ with $\deg_q(f(x)) < k$ and $\alpha^h \mapsto \beta$.

Interpolation-Based Decoding

The interpolation-based decoding principle consists of an *interpolation step* and a *root-finding* step. For the interpolation step, we search for a nonzero $(s+1)$-variate linearized polynomial of the form

$$Q(x, y_1, \dots, y_s) = Q_0(x) + Q_1(y_1) + \dots + Q_s(y_s) \qquad (1)$$

which satisfies for all $i \in [0, h-s], j \in [0, n_r - 1]$ and $s \le h$:

- $Q(x_j \alpha^i, y_{j,i}, y_{j,i+1}, \dots, y_{j,i+s-1}) = 0,$
- $\deg_q(Q_0(x)) < d,$
- $\deg_q(Q_\ell(y_\ell)) < d - (k-1), \ \forall \ell \in [1, s].$

A non-zero $Q(x, y_1, \dots, y_s)$ fulfilling the above interpolation constraints exists if $d \ge \left\lceil \frac{n_r(h-s+1)+s(k-1)+1}{s+1} \right\rceil$.

Theorem (Decoding Radius)

Let $Q(x, y_1, \dots, y_s) \neq 0$ fulfill the above interpolation constraints. If

$$\gamma + s\delta < s\left(n_t - \frac{k-1}{h-s+1}\right) \qquad (2)$$

then

$$P(x) \overset{\text{def}}{=} Q(x, f(x), f(\alpha x), \dots, f(\alpha^{s-1}x)) = 0. \qquad (3)$$

Normalized Decoding Radius

The *normalized decoding radius* $\tau_f = \frac{\gamma + s\delta}{n_t}$ of the approach is

$$\tau_f < s\left(1 - \frac{n_t + hm}{m(h-s+1)}R\right).$$

Root-Finding step

The task of the root finding step is to find all polynomials $f(x)$ with $\deg_q(f(x)) < k$ such that

$$P(x) \overset{\text{def}}{=} Q(x, f(x), f(\alpha x), \dots, f(\alpha^{s-1}x)) = 0. \qquad (4)$$

This can be done by solving a *linear* system of equations in at most $\mathcal{O}(k^2)$ operations in $\mathbb{F}_{q^m}$.

List Decoding Approach

- In general, the root-finding system can be underdetermined
- In this case, we obtain a *list* of roots of (4), i.e., a list of possible message polynomials
- This decoder is no polynomial-time list decoder but it provides the basis of the list with quadratic complexity

Theorem (Average List Size for Subspace Codes)

Let $\mathrm{FSub}[h; n, k]$ be a constant dimension subspace code over $\mathbb{F}_{q^m}$ and let $N = n_t + hm$ be the dimension of the ambient vector space. Let the number of insertions γ and deletions δ fulfill (2). The average list size $\overline{L}_f(\tau)$, i.e. the average number of codewords at subspace distance at most $\tau = \gamma + s\delta$ from a received n_r-dimensional subspace satisfies

$$\overline{L}(\tau) < 1 + 16(\frac{\tau}{2}+1)q^{mk+(n_r - \lfloor \frac{n_r - n_t + \tau}{2} \rfloor)(n_t + \lfloor \frac{n_r - +\tau}{2} \rfloor - N)}.$$

Probabilistic Unique Decoding

- The average list size is one for most parameters
- This allows us to use the algorithm as a probabilistic unique decoder which returns a unique solution or a decoding failure in case the list size is larger than one

Theorem (Probabilistic Unique Decoding)

Consider an h-folded subspace code $\mathrm{FSub}[h; n, k]$. Let $\mu \ge 1$ be an integer. If

$$\gamma + s\delta \le \frac{s(n_t(h-s+1)-(k-1))-\mu}{h-s+1} \qquad (5)$$

then we can find a unique solution $f(x)$ satisfying (3) with probability at least

$$1 - k\left(\frac{k}{q^m}\right)^{\mu}$$

requiring at most $\mathcal{O}(s^2 n_r^2)$ operations in $\mathbb{F}_{q^m}$.

The decoding radius can be adjusted by the choice of μ to control the decoding radius vs. failure probability tradeoff.

Simulation Results

Consider a folded subspace code with parameters $q=2$, $m=n=16$, $h=4$, $n_t=4$, $k=4$ and $s=3$.

μ	γ	δ	observed errors	failure probability	iterations
1	4	1	$5.89 \cdot 10^{-5}$	$2.44 \cdot 10^{-4}$	10^6
2	3	1	0	$1.49 \cdot 10^{-8}$	$6 \cdot 10^6$

Performance Analysis

For a fair comparison we select the code parameters such that each codeword contains the same number of symbols.

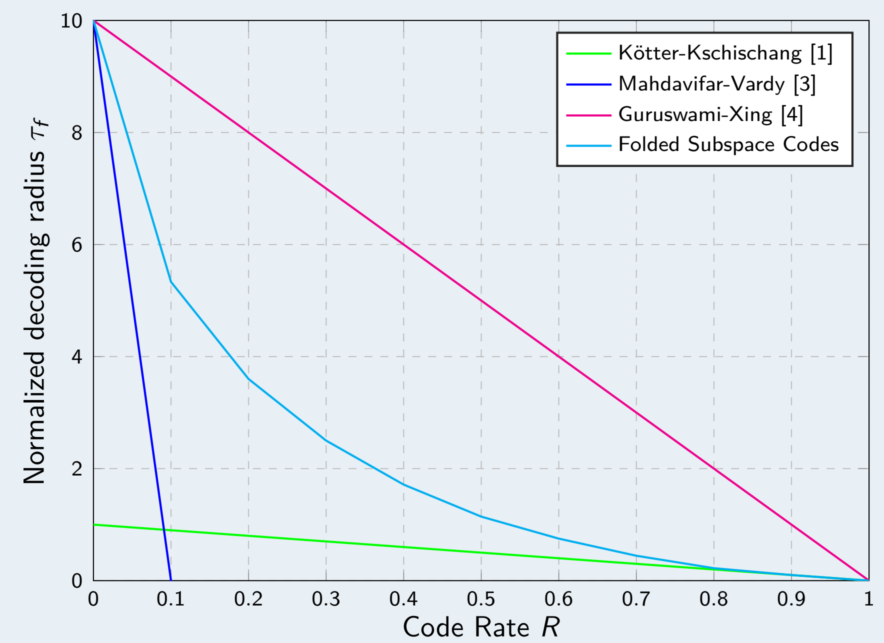


Figure 1: The normalized decoding radius $\tau_f = \frac{\gamma+s\delta}{n_t}$ vs. the rate R for $h=10$.

Comparison to other approaches

- The code by Mahdavifar and Vardy [3] only can correct errors for very small rates
- The construction by Guruswami and Xing [4] achieves the best decoding radius for all rates but puts out a very large list with high probability
- ✓ The proposed code construction can correct insertions and deletions for all code rates and returns a *unique* solution with high probability, which is a major benefit for practical applications

Summary

- Interpolation-based decoding scheme for folded subspace codes consisting of an interpolation step and a root-finding step
- Folded subspace codes are very resilient against insertions
- Upper bound on the average list size for subspace codes
- The scheme can be used as a probabilistic unique decoder that outputs a unique solution with high probability

References

[1] R. Kötter and F. R. Kschischang, "Coding for Errors and Erasures in Random Network Coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, Jul. 2008.

[2] Ø. Ore, "On a Special Class of Polynomials," *Trans. Amer. Math. Soc.*, vol. 35, pp. 559–584, 1933.

[3] H. Mahdavifar and A. Vardy, "List-Decoding of Subspace Codes and Rank-Metric Codes up to Singleton Bound," in *IEEE Trans. Int. Symp. Inf. Theory*, Jul. 2012, pp. 1488–1492.

[4] V. Guruswami and C. Xing, "List Decoding Reed–Solomon, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound," *Electr. Colloq. Comp. Complexity*, vol. 19, no. 146, 2012.

Institute for Communications Engineering

Unterstützt von / Supported by
Alexander von Humboldt Stiftung/Foundation

Technische Universität München