Equivalence for Rank-Metric and Matrix Codes with Applications to Network Coding

Katherine Morrison

Department of Mathematics
University of Nebraska

Algebraic Structure in Network Information Theory
August 17, 2011

Subspace Codes for Network Coding

Koetter and Kschischang show subspace codes are valuable for error correction of network coding.

- A subspace code is a non-empty collection C of subspaces of $\mathbb{F}_q^n$.
- Constant-dimension subspace codes: all the codewords (subspaces) have fixed dimension l.
- The subspace distance between U and V is

$$d_S(U,V) = \dim(U+V) - \dim(U \cap V)$$

Subspace Code Construction

- Matrix code: A subset $T \subseteq \mathbb{F}_q^{l \times m}$.
- Lifted matrix code: A constant-dimension subspace code where all the RREF matrices corresponding to each codeword have the same pivot locations, and the non-pivot locations are filled by the entries of a matrix from a matrix code.
  E.g. $C = \{\text{rowspan}[I|A] \ : \ A \in T\}$ for some code $T \subseteq \mathbb{F}_q^{l \times m}$.
- Silva, Kschischang, and Koetter show that the subspace distance between $U = \text{rowspan}[I|A]$ and $V = \text{rowspan}[I|B]$ is

$$d_S(U, V) = 2\,\text{rank}(A - B)$$

Subspace Code Construction Cont'd

- Rank-metric code: a block code over $\mathbb{F}_{q^m}$, where each codeword $\mathbf{x}$ is associated with a matrix $\epsilon_{\mathcal{B}}(\mathbf{x})$; row i of $\epsilon_{\mathcal{B}}(\mathbf{x})$ is the expansion of x_i w.r.t. a fixed basis $\mathcal{B}$ for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.
- Lifted rank-metric code: lifting of the matrix expansion of a rank-metric code.
- The rank-metric distance between two vectors $\mathbf{x}$ and $\mathbf{y}$ is

$$d_R(\mathbf{x}, \mathbf{y}) = \dim\langle \mathbf{x} - \mathbf{y} \rangle_{\mathbb{F}_q} = \text{rank}(\epsilon_{\mathcal{B}}(\mathbf{x}) - \epsilon_{\mathcal{B}}(\mathbf{y})).$$

Equivalence of Rank-Metric Codes

Any invertible $\mathbb{F}_{q^m}$-linear map $f : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ that preserves rank weight is called a rank-metric equivalence map.

Theorem (Berger)

The set of rank-metric equivalence maps $G_{RM}(\mathbb{F}_{q^m}^n)$ is generated by the non-zero $\mathbb{F}_{q^m}$-scalar multiplications and the linear group $\mathrm{GL}_n(\mathbb{F}_q)$. The group is isomorphic to the product $(\mathbb{F}_{q^m}^*/\mathbb{F}_q^*) \times \mathrm{GL}_n(\mathbb{F}_q)$.

Note: For $f \in G_{RM}(\mathbb{F}_{q^m}^n)$, we represent f by an ordered pair (α, A) for some $\alpha \in \mathbb{F}_{q^m}^*$, $A \in \mathrm{GL}_n(\mathbb{F}_q)$.

The rank-metric automorphism group $Aut_{RM}(C)$ of a code $C \subseteq \mathbb{F}_{q^m}^n$ is the set of rank-metric equivalence maps $f \in G_{RM}(\mathbb{F}_{q^m}^n)$ satisfying $f(C) = C$.

Gabidulin codes

- The $[n, k, n-k+1]_{q^m}$ rank-metric code $C_{k,\mathbf{g},q^m}$ with generator matrix

$$G = \begin{bmatrix} g_1, & g_2, & \dots, & g_n \\ g_1^{q^1}, & g_2^{q^1}, & \dots, & g_n^{q^1} \\ \vdots & \vdots & \vdots & \vdots \\ g_1^{q^{(k-1)}}, & g_2^{q^{(k-1)}}, & \dots, & g_n^{q^{(k-1)}} \end{bmatrix},$$

  where the entries of $\mathbf{g} = [g_1, \dots, g_n] \in \mathbb{F}_{q^m}^n$ are linearly independent over $\mathbb{F}_q$, is called a Gabidulin code.

- Gabidulin codes are q^m-ary analogues of Reed-Solomon codes that are optimal for the rank metric.

- Used in the first subspace code construction by Koetter and Kschischang; also used in the GPT public-key cryptosystem.

Rank-Metric-Automorphism Group of Gabidulin Codes

Theorem

Let $k \leq n \leq m$. Let $\mathbf{g} = [g_1, \ldots, g_n] \in \mathbb{F}_{q^m}^n$ have entries that are linearly independent over $\mathbb{F}_q$, and let $C_{k,\mathbf{g},q^m}$ be the Gabidulin code of dimension k generated by $\mathbf{g}$. Let d be the largest integer such that $\langle g_1, \ldots, g_n \rangle_{\mathbb{F}_q}$ is a vector space over $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^m}$. Then

1. *d divides $\gcd(n, m)$.*
2. *$Aut_{RM}(C_{k,\mathbf{g},q^m}) = \left\{ \left(\alpha, \epsilon_{\mathbf{g}} \left([\beta g_1, \ldots, \beta g_n] \right)^\top \right) \ : \ \alpha \in \mathbb{F}_{q^m}^*, \ \beta \in \mathbb{F}_{q^d}^* \right\}$.*

Equivalence of Matrix Codes

A matrix-equivalence map is an invertible $\mathbb{F}_q$-linear map $f : \mathbb{F}_q^{n\times m} \longrightarrow \mathbb{F}_q^{n\times m}$ that preserves rank weight.

Theorem

Let $f \in G_{Mat}(\mathbb{F}_q^{n\times m})$ be a matrix-equivalence map.
If $n \neq m$, then there exist $A \in \mathrm{GL}_n(\mathbb{F}_q)$, $B \in \mathrm{GL}_m(\mathbb{F}_q)$ such that

- $f(M) = AMB$ *for all* $M \in \mathbb{F}_q^{n\times m}$.

If $n = m$, then there exist $A, B \in \mathrm{GL}_n(\mathbb{F}_q)$ such that either

- $f(M) = AMB$ *for all* $M \in \mathbb{F}_q^{n\times m}$, *or*
- $f(M) = AM^{\top}B$ *for all* $M \in \mathbb{F}_q^{n\times m}$.

Note: When $n \neq m$,

$$G_{Mat}(\mathbb{F}_q^{n\times m}) \cong \mathrm{GL}_n(\mathbb{F}_q) \times \mathrm{PGL}_m(\mathbb{F}_q),$$

and so we can choose a representative for $f \in G_{Mat}(\mathbb{F}_q^{n\times m})$ of the form (A, B) where $A \in \mathrm{GL}_n(\mathbb{F}_q)$ and $B \in \mathrm{GL}_m(\mathbb{F}_q)$.

Matrix-Automorphism Group of Gabidulin Codes

The matrix-automorphism group $Aut_{Mat}(C)$ of a code $C \subseteq \mathbb{F}_q^{n \times m}$ is the set of matrix-equivalence maps that fix C.

Theorem

Let $k \leq n < m$ and $\mathcal{B} = \{b_1, \ldots, b_m\}$ be a basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let $\mathbf{g} = [g_1, \ldots, g_n] \in \mathbb{F}_{q^m}^n$ have entries that are linearly independent over $\mathbb{F}_q$, and let $\epsilon_{\mathcal{B}}(C_{k,\mathbf{g},q^m})$ be the matrix expansion of the Gabidulin code of dimension k generated by $\mathbf{g}$. Let d be maximal such that $\langle g_1, \ldots, g_n \rangle_{\mathbb{F}_q}$ is a vector space over $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^m}$. Then

1. *d divides $\gcd(n, m)$.*
2. *$Aut_{Mat}(\epsilon_{\mathcal{B}}(C_{k,\mathbf{g},q^m})) \supseteq$*
$$\left\{(\epsilon_{\mathbf{g}}([\alpha g_1, \ldots, \alpha g_n]), \epsilon_{\mathcal{B}}([\beta b_1, \ldots, \beta b_m])) : \alpha \in \mathbb{F}_{q^d}^*,\ \beta \in \mathbb{F}_{q^m}^*\right\}.$$

Work in Progress

- Determine if either the matrix equivalence maps provide better protection against cryptanalysis than the permutation equivalence map currently used in the GPT public-key cryptosystem.
- Use these notions of equivalence to enumerate all inequivalent self-dual matrix codes.
- Extend the notion of equivalence to subspace codes and determine the automorphism groups of various families of subspace codes.