Maximum Rank Distance Codes with Applications

Joint work with YANG Shengtian

Thomas Honold

Department of Information Science and Electronic Engineering
Zhejiang University

University of Bayreuth
July 2011

Outline

Outline

Consider $\mathbb{F}_q^{m\times n}$ w.r.t. the *rank distance* $\mathrm{d_R}$ defined by $\mathrm{d_R}(\mathbf{A},\mathbf{B}) = \mathrm{rk}(\mathbf{A}-\mathbf{B})$.
$(\mathbb{F}_q^{m\times n}, \mathrm{d_R})$ is a (translation-invariant) metric space.

Definition

An (m,n,M,d) *rank distance code* is a set $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ with $|\mathcal{C}| = M$ and $\mathrm{d_R}(\mathbf{A},\mathbf{B}) \geq d$ for distinct $\mathbf{A},\mathbf{B} \in \mathcal{C}$.

For technical reasons we assume $m \geq n$ in what follows.

Singleton bound for rank distance codes

For an (m,n,M,d) rank distance code we have $M \leq q^{m(n-d+1)}$.

Proof.

Suppose $\mathbf{A},\mathbf{B} \in \mathcal{C}$ agree in the first $n-d+1$ columns.
$\Longrightarrow \mathrm{rk}(\mathbf{A}-\mathbf{B}) \leq d-1 \Longrightarrow \mathbf{A}=\mathbf{B}$
Hence the projection map $\mathcal{C} \to \mathbb{F}_q^{m\times(n-d+1)}$ is one-to-one. $\square$

SINGLETON Systems alias GABIDULIN codes

If equality holds in the Singleton bound, then $\mathcal{C}$ is referred to as a maximum rank distance code or MRD code; more precisely:

Definition

Suppose $1 \leq k \leq n \leq m$ are integers. An (m,n,k) *maximum rank distance code (MRD code)* is a set $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ with $|\mathcal{C}| = q^{mk}$ and $\mathrm{d_R}(\mathbf{A}-\mathbf{B}) \geq n-k+1$ for distinct $\mathbf{A},\mathbf{B} \in \mathcal{C}$.

(Without the assumption $m \geq n$ we would have to write $|\mathcal{C}| = q^{\max\{m,n\}\cdot k}$ and $\mathrm{d_R}(\mathbf{A}-\mathbf{B}) \leq \min\{m,n\} - k + 1$.)

DELSARTE 1978 (and independently GABIDULIN 1985, ROTH 1991) proved the following

Theorem

Linear (m,n,k) MRD codes exist for all choices of m,n,k.

Proof.

Consider the columns of $\mathbf{A} \in \mathbb{F}_q^{m\times n}$ as coordinate vectors w.r.t. a basis $\{\alpha_1, \dots, \alpha_m\}$ of $\mathbb{F}_{q^m}/\mathbb{F}_q$.

This gives an $\mathbb{F}_q$-linear isomorphism $\mathbb{F}_q^{m\times n} \cong (\mathbb{F}_{q^m})^n$ and induces a map $C \mapsto \mathcal{C}$ from $\{$linear codes of length n over $\mathbb{F}_{q^m}\}$ to $\{m \times n$ rank distance codes over $\mathbb{F}_q\}$.

Let C be the linear code of length n over $\mathbb{F}_{q^m}$ generated by

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \dots & \alpha_n^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{k-1}} & \alpha_2^{q^{k-1}} & \dots & \alpha_n^{q^{k-1}} \end{pmatrix}$$

Then $|C| = q^{mk}$ and $\operatorname{rk}\langle c_1, \dots, c_n\rangle_{\mathbb{F}_q} \geq n - k + 1$ for every nonzero $\mathbf{c} = (c_1, \dots, c_n) \in C$.

The latter follows from $c_i = L(\alpha_i)$ for $1 \leq i \leq n$, where $L(X) = a_0X + a_1X^q + \dots + a_{k-1}X^{q^{k-1}} \in \mathbb{F}_{q^m}[X]$ is a nonzero *linearized* polynomial (Reed-Solomon type construction). $\square$

A Characteristic Property of MRD Codes

Proposition

For $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ the following are equivalent:

(i) *$\mathcal{C}$ is an (m,n,k) MRD code*

(ii) *For every $\mathbf{U} \in \mathbb{F}_q^{k\times m}$ with $\operatorname{rk} U = k$ and every $\mathbf{V} \in \mathbb{F}_q^{k\times n}$ there exists exactly one $\mathbf{G} \in \mathcal{C}$ such that $\mathbf{UG} = \mathbf{V}$.*

Viewing $\mathcal{C}$ as a set of linear transformations from $\mathbb{F}_q^m$ to $\mathbb{F}_q^n$, Part (ii) says:

> *Every linear map $g\colon U \to \mathbb{F}_q^n$, defined on a k-dimensional subspace U of $\mathbb{F}_q^m$, has a unique extension $\overline{g} \in \mathcal{C}$. ("Every k-dimensional subspace of $\mathbb{F}_q^m$ is an information subspace.")*

Compare with the case of MDS codes (where "every set of k coordinates is an information set").

Outline

Random Coding

Random $m \times n$ matrix over $\mathbb{F}_q$

A random variable $\tilde{\mathbf{G}}$ with values in $\mathbb{F}_q^{m\times n}$
Only the distribution $P\{\tilde{\mathbf{G}} = \mathbf{G}\}$, $\mathbf{G} \in \mathbb{F}_q^{m\times n}$ matters

Random linear code ensemble

$\{\mathbf{u}\tilde{\mathbf{G}} : \mathbf{u} \in \mathbb{F}_q^m\}$ Generator matrix definition
$\{\mathbf{v} \in \mathbb{F}_q^n : \tilde{\mathbf{H}}\mathbf{v}^T = \mathbf{0}\}$ Parity-check matrix definition

Examples

- $P\{\tilde{\mathbf{G}} = \mathbf{G}\} = q^{-mn}$ for all $\mathbf{G} \in \mathbb{F}_q^{m\times n}$ (equiprobable generator matrix ensemble)
- Equiprobable parity-check matrix ensemble
- Gallager's low-density parity-check (LDPC) code ensembles

Good Random Matrices

A linear code ensemble $\{\mathbf{u}\tilde{\mathbf{G}} : \mathbf{u} \in \mathbb{F}_q^m\}$ is good in the sense of the asymptotic Gilbert-Varshamov (GV) bound, provided it has the following

Fundamental property

$$P\{\mathbf{u}\tilde{\mathbf{G}} = \mathbf{v}\} = q^{-n} \qquad \forall \mathbf{u} \in \mathbb{F}_q^m \setminus \{\mathbf{0}\}, \forall \mathbf{v} \in \mathbb{F}_q^n.$$

Definition

A random $m \times n$ matrix $\tilde{\mathbf{G}}$ is said to be *good* if $\mathbf{u}\tilde{\mathbf{G}}$ is uniformly distributed over $\mathbb{F}_q^n$ for every $\mathbf{u} \in \mathbb{F}_q^m \setminus \{\mathbf{0}\}$.

Generalization

$\tilde{\mathbf{G}}$ is said to be k-*good*, $1 \leq k \leq \min\{m, n\}$, if $\mathbf{U}\tilde{\mathbf{G}}$ is uniformly distributed over $\mathbb{F}_q^{k \times n}$ for every rank-k matrix $\mathbf{U} \in \mathbb{F}_q^{k \times m}$.

Small Support Size

Example

The equiprobable generator matrix ensemble is k-good for $1 \leq k \leq \min\{m, n\}$, since

$$\#\{\mathbf{G} \in \mathbb{F}_q^{m\times n}; \mathbf{U}\mathbf{G} = \mathbf{V}\} = q^{(m-k)n}$$

for all $\mathbf{U} \in \mathbb{F}_q^{k\times m}$ with $\operatorname{rk}\mathbf{U} = k$ and all $\mathbf{V} \in \mathbb{F}_q^{k\times n}$.

> *Every linear map $g\colon U \to \mathbb{F}_q^n$, defined on a k-dimensional subspace U of $\mathbb{F}_q^m$, has the same number of (linear) extensions $\overline{g}\colon \mathbb{F}_q^m \to \mathbb{F}_q^n$.*

The support size of this ensemble is q^{mn} (“large”).

Problem

Determine the smallest support size of a k-good random $m \times n$-matrix over $\mathbb{F}_q$, and give a characterization in the extremal case.

Small Support Size—Solution

Theorem (Yang-H. 2011)

A k-good random $m \times n$-matrix $\tilde{\mathbf{G}}$ over $\mathbb{F}_q$ has support size at least $q^{\max\{m,n\}\cdot k}$. Equality holds iff $\tilde{\mathbf{G}}$ is uniformly distributed over an (m,n,k) MRD code.

Sketch of proof.

We only consider the case $k = 1$.

Suppose that $P\{\mathbf{u}\tilde{\mathbf{G}} = \mathbf{v}\} = q^{-n}$ for all $\mathbf{u} \in \mathbb{F}_q^m \setminus \{\mathbf{0}\}$, $\mathbf{v} \in \mathbb{F}_q^n$.

The case $m \leq n$

This case is easy: The support size must be at least q^n (why?), and the random $m \times n$-matrix unformly distributed over an $(m,n,1)$ MRD code gives equality.

Proof cont'd.

The case $m > n$

This case is not easy. We have based the proof on the following

Lemma

A random $m \times n$ matrix over $\mathbb{F}_q$ is good iff its transpose (a random $n \times m$ matrix over $\mathbb{F}_q$) is good.

The condition implies $P\{\mathbf{u}\tilde{\mathbf{G}}\mathbf{v}^\mathsf{T} = a\} = q^{-1}$ for all $\mathbf{u} \in \mathbb{F}_q^m \setminus \{\mathbf{0}\}$, $\mathbf{v} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$, $a \in \mathbb{F}_q$.

From this one can conclude that $\tilde{\mathbf{G}}\mathbf{v}^\mathsf{T}$ must be uniformly distributed as well (over $\mathbb{F}_q^m$).

Reason

The rational $q^m \times (q^m + q^{m-1} + \cdots + q)$ incidence matrix of the point-hyperplane design of $\mathrm{AG}(m, \mathbb{F}_q)$ has full rank q^m.

The lemma provides the key step in the proof of our theorem. □

Structure of k-good random matrices

Observation

The set of all k-good random $m \times n$-matrices over $\mathbb{F}_q$ forms a convex polytope in q^{mn}-dimensional Euclidean space.

Open Problem

Determine the vertices of this polytope.

Every (m, n, k) MRD code determines a vertex, but there are other vertices.

Outline

R_m denotes the ring of $m \times m$ matrices over $\mathbb{F}_q$ (so as a set $R_m = \mathbb{F}_q^{m\times m}$).

The space $\mathbb{F}_q^{m\times n}$ of rectangular $m \times n$ matrices over $\mathbb{F}_q$ forms an R_m-R_n bimodule relative to the action $(\mathbf{A}, \mathbf{B}) \circ \mathbf{X} = \mathbf{AXB}$ ($\mathbf{A} \in R_m$, $\mathbf{B} \in R_n$, $\mathbf{X} \in F_q^{m\times n}$).

Folklore

There is a 1-1 correspondence between right submodules of $\mathbb{F}_q^{m\times n}$ and subspaces of $\mathbb{F}_q^m$. The map which sends a right submodule $\mathcal{U}$ to the sum of all column spaces of all matrices $\mathbf{A} \in \mathcal{U}$ is such a bijection.

Definition

The *left homogeneous weight* $\mathrm{w}_\ell \colon \mathbb{F}_q^{m\times n} \to \mathbb{R}$ is uniquely defined by the following axioms:

(H1) $\mathrm{w}_\ell(\mathbf{0}) = 0$;

(H2) $\mathrm{w}_\ell(\mathbf{UX}) = \mathrm{w}_\ell(\mathbf{X})$ for all $\mathbf{X} \in \mathbb{F}_q^{m\times n}$, $\mathbf{U} \in R_m^\times$;

(H3) $\sum_{\mathbf{X}\in\mathcal{U}} \mathrm{w}_\ell(\mathbf{X}) = |\mathcal{U}|$ for all cyclic left submodules $\mathcal{U} \neq \{\mathbf{0}\}$ of $\mathbb{F}_q^{m\times n}$.

The right homogeneous weight $\mathrm{w}_\mathrm{r} \colon \mathbb{F}_q^{m\times n} \to \mathbb{R}$ is defined in an analogous fashion.

Definition

The *left homogeneous weight* $\mathrm{w}_\ell \colon \mathbb{F}_q^{m\times n} \to \mathbb{R}$ is uniquely defined by the following axioms:

(H1) $\mathrm{w}_\ell(\mathbf{0}) = 0$;

(H2) $\mathrm{w}_\ell(\mathbf{UX}) = \mathrm{w}_\ell(\mathbf{X})$ for all $\mathbf{X} \in \mathbb{F}_q^{m\times n}$, $\mathbf{U} \in R_m^\times$;

(H3) $\sum_{\mathbf{X}\in\mathcal{U}} \mathrm{w}_\ell(\mathbf{X}) = |\mathcal{U}|$ for all cyclic left submodules $\mathcal{U} \neq \{\mathbf{0}\}$ of $\mathbb{F}_q^{m\times n}$.

The right homogeneous weight $\mathrm{w}_\mathrm{r} \colon \mathbb{F}_q^{m\times n} \to \mathbb{R}$ is defined in an analogous fashion.

Remarks

- The definition makes sense for arbitrary finite modules ${}_RM$ (over a finite ring R).
- The following key property of finite modules is used in the definition: $Rx = Ry \implies R^\times x = R^\times y$.
- In the case $m \geq n$ all left submodules of $\mathbb{F}_q^{m\times n}$ are cyclic, so that (H3) holds for all left submodules $\mathcal{U}$ of $\mathbb{F}_q^{m\times n}$.

Explicit Formula for w_ℓ, w_r

$$\mathrm{w}_\ell(\mathbf{X}) = 1 - \frac{(-1)^{\operatorname{rk}\mathbf{X}}}{(q^m-1)(q^{m-1}-1)\cdots(q^{m-\operatorname{rk}\mathbf{X}+1}-1)},$$

and similarly for w_r.

From this it follows that $\mathrm{w}_\ell = \mathrm{w}_\mathrm{r} \iff m = n$.

Explicit Formula for w_ℓ, w_r

$$\mathrm{w}_\ell(\mathbf{X}) = 1 - \frac{(-1)^{\operatorname{rk}\mathbf{X}}}{(q^m-1)(q^{m-1}-1)\cdots(q^{m-\operatorname{rk}\mathbf{X}+1}-1)},$$

and similarly for w_r.

From this it follows that $\mathrm{w}_\ell = \mathrm{w}_\mathrm{r} \iff m = n$.

Observation

w_ℓ (and similarly w_r) can be scaled by a constant $\gamma > 0$ to turn it into a probability distribution on $\mathbb{F}_q^{m\times n}$. The normalized version $\overline{\mathrm{w}}_\ell = \gamma\mathrm{w}_\ell$ satisfies (H1), (H2), and $\sum_{\mathbf{X}\in\mathbb{F}_q^{m\times n}} \mathrm{w}_\ell(\mathbf{X}) = \gamma|\mathcal{U}|$ for all cyclic left submodules $\mathcal{U} \neq \{\mathbf{0}\}$ of $\mathbb{F}_q^{m\times n}$ in place of (H3).

Explicit Formula for w_ℓ, w_r

$$\mathrm{w}_\ell(\mathbf{X}) = 1 - \frac{(-1)^{\operatorname{rk}\mathbf{X}}}{(q^m-1)(q^{m-1}-1)\cdots(q^{m-\operatorname{rk}\mathbf{X}+1}-1)},$$

and similarly for w_r.

From this it follows that $\mathrm{w}_\ell = \mathrm{w}_\mathrm{r} \iff m = n$.

Observation

w_ℓ (and similarly w_r) can be scaled by a constant $\gamma > 0$ to turn it into a probability distribution on $\mathbb{F}_q^{m\times n}$. The normalized version $\overline{\mathrm{w}}_\ell = \gamma\mathrm{w}_\ell$ satisfies (H1), (H2), and $\sum_{\mathbf{X}\in\mathbb{F}_q^{m\times n}} \mathrm{w}_\ell(\mathbf{X}) = \gamma|\mathcal{U}|$ for all cyclic left submodules $\mathcal{U} \neq \{\mathbf{0}\}$ of $\mathbb{F}_q^{m\times n}$ in place of (H3).

Lemma

$\gamma = c_{mn}^{-1}$ with
$c_{mn} = \sum_{\mathbf{X}\in\mathbb{F}_q^{m\times n}} \mathrm{w}_\ell(\mathbf{X}) = q^{mn} - (-1)^m q^{m(m+1)/2} \binom{n-1}{m}_q.$

Theorem

If $m \geq n$ then the normalized left homogeneous weight $\overline{\mathrm{w}}_\ell$ defines a k-good random matrix on $\mathbb{F}_q^{m \times n}$ for $1 \leq k \leq n-1$. Similarly, if $m \leq n$ then $\overline{\mathrm{w}}_\mathrm{r}$ defines a k-good random matrix on $\mathbb{F}_q^{m \times n}$ for $1 \leq k \leq m-1$.

Idea of proof.

Since $\overline{\mathrm{w}}_\ell(\mathbf{X}) = \overline{\mathrm{w}}_\mathrm{r}(\mathbf{X}^T)$ for $\mathbf{X} \in \mathbb{F}_q^{n\times m}$, we can assume $m \geq n$ (so that every right submodule of $\mathbb{F}_q^{m\times n}$ is cyclic).

Idea of proof.

Since $\overline{\mathrm{w}}_\ell(\mathbf{X}) = \overline{\mathrm{w}}_\mathrm{r}(\mathbf{X}^T)$ for $\mathbf{X} \in \mathbb{F}_q^{n\times m}$, we can assume $m \geq n$ (so that every right submodule of $\mathbb{F}_q^{m\times n}$ is cyclic).

$\overline{\mathrm{w}}_\mathrm{r}\colon \mathbb{F}_q^{m\times n} \to \mathbb{R}$ gives rise to a k-good random matrix if and only if for every $\mathbf{B} \in \mathbb{F}_q^{k\times m}$ with $\mathrm{rk}(\mathbf{B}) = k$ and every $\mathbf{Y} \in \mathbb{F}_q^{k\times n}$ the following equation holds:

$$\sum_{\substack{\mathbf{X}\in\mathbb{F}_q^{m\times n}\\ \mathbf{BX}=\mathbf{Y}}} \overline{\mathrm{w}}_\mathrm{r}(\mathbf{X}) = q^{-kn}.$$

$\mathcal{U} = \{\mathbf{X} \in \mathbb{F}_q^{m\times n}; \mathbf{BX} = \mathbf{0}\}$ is a right submodule of $\mathbb{F}_q^{m\times n}$ of size $|\mathcal{U}| = q^{(m-k)n}$;

$\mathcal{U} \neq \{\mathbf{0}\}$ provided that $1 \leq k \leq m-1$.

Idea of proof.

Since $\overline{\mathrm{w}}_\ell(\mathbf{X}) = \overline{\mathrm{w}}_\mathrm{r}(\mathbf{X}^T)$ for $\mathbf{X} \in \mathbb{F}_q^{n\times m}$, we can assume $m \geq n$ (so that every right submodule of $\mathbb{F}_q^{m\times n}$ is cyclic).

$\overline{\mathrm{w}}_\mathrm{r} \colon \mathbb{F}_q^{m\times n} \to \mathbb{R}$ gives rise to a k-good random matrix if and only if for every $\mathbf{B} \in \mathbb{F}_q^{k\times m}$ with $\mathrm{rk}(\mathbf{B}) = k$ and every $\mathbf{Y} \in \mathbb{F}_q^{k\times n}$ the following equation holds:

$$\sum_{\substack{\mathbf{X}\in\mathbb{F}_q^{m\times n}\\ \mathbf{BX}=\mathbf{Y}}} \overline{\mathrm{w}}_\mathrm{r}(\mathbf{X}) = q^{-kn}.$$

$\mathcal{U} = \{\mathbf{X} \in \mathbb{F}_q^{m\times n}; \mathbf{BX} = \mathbf{0}\}$ is a right submodule of $\mathbb{F}_q^{m\times n}$ of size $|\mathcal{U}| = q^{(m-k)n}$;
$\mathcal{U} \neq \{\mathbf{0}\}$ provided that $1 \leq k \leq m-1$.

The proof is completed by showing that

$$\sum_{\mathbf{X}\in\mathcal{U}+\mathbf{A}} \overline{\mathrm{w}}_\mathrm{r}(\mathbf{X}) = q^{-mn}|\mathcal{U}+\mathbf{A}| = q^{-kn}$$

for every coset $\mathcal{U}+\mathbf{A}$ of every (cyclic) right submodule $\mathcal{U} \neq \{\mathbf{0}\}$ of $\mathbb{F}_q^{m\times n}$ (a strong variant of (H3)).

Example

We consider the case of binary 2×3 matrices.

Example

We consider the case of binary 2×3 matrices.

The space $\mathbb{F}_2^{2\times 3}$ contains 21 matrices of rank 1 (parametrized as $\mathbf{u}^T\mathbf{v}$ with $\mathbf{u} \in \mathbb{F}_2^2 \setminus \{\mathbf{0}\}$, $\mathbf{v} \in \mathbb{F}_2^3 \setminus \{\mathbf{0}\}$) and 42 matrices of rank 2.

Example

We consider the case of binary 2×3 matrices.

The space $\mathbb{F}_2^{2\times 3}$ contains 21 matrices of rank 1 (parametrized as $\mathbf{u}^T\mathbf{v}$ with $\mathbf{u} \in \mathbb{F}_2^2 \setminus \{\mathbf{0}\}$, $\mathbf{v} \in \mathbb{F}_2^3 \setminus \{\mathbf{0}\}$) and 42 matrices of rank 2.

The normalized left and right homogeneous weights $\overline{\mathrm{w}}_\ell$, $\overline{\mathrm{w}}_\mathrm{r}$ on $\mathbb{F}_2^{2\times 3}$ are given by the following tables:

$\mathrm{rk}(\mathbf{X})$	0	1	2
$\overline{\mathrm{w}}_\ell(\mathbf{X})$	0	$\frac{1}{42}$	$\frac{1}{84}$

$\mathrm{rk}(\mathbf{X})$	0	1	2
$\overline{\mathrm{w}}_\mathrm{r}(\mathbf{X})$	0	$\frac{1}{56}$	$\frac{5}{336}$

Example

We consider the case of binary 2×3 matrices.

The space $\mathbb{F}_2^{2\times 3}$ contains 21 matrices of rank 1 (parametrized as $\mathbf{u}^T\mathbf{v}$ with $\mathbf{u} \in \mathbb{F}_2^2 \setminus \{\mathbf{0}\}$, $\mathbf{v} \in \mathbb{F}_2^3 \setminus \{\mathbf{0}\}$) and 42 matrices of rank 2.

The normalized left and right homogeneous weights $\overline{\mathrm{w}}_\ell$, $\overline{\mathrm{w}}_\mathrm{r}$ on $\mathbb{F}_2^{2\times 3}$ are given by the following tables:

$\mathrm{rk}(\mathbf{X})$	0	1	2
$\overline{\mathrm{w}}_\ell(\mathbf{X})$	0	$\frac{1}{42}$	$\frac{1}{84}$

$\mathrm{rk}(\mathbf{X})$	0	1	2
$\overline{\mathrm{w}}_\mathrm{r}(\mathbf{X})$	0	$\frac{1}{56}$	$\frac{5}{336}$

$\overline{\mathrm{w}}_\ell$ is a probability distribution on $\mathbb{F}_2^{2\times 3}$ and satisfies (H1), (H2), but it does not yield a 1-good random 2×3 matrix over $\mathbb{F}_2$.

Example

We consider the case of binary 2×3 matrices.

The space $\mathbb{F}_2^{2\times 3}$ contains 21 matrices of rank 1 (parametrized as $\mathbf{u}^T\mathbf{v}$ with $\mathbf{u} \in \mathbb{F}_2^2 \setminus \{\mathbf{0}\}$, $\mathbf{v} \in \mathbb{F}_2^3 \setminus \{\mathbf{0}\}$) and 42 matrices of rank 2.

The normalized left and right homogeneous weights $\overline{\mathrm{w}}_\ell$, $\overline{\mathrm{w}}_\mathrm{r}$ on $\mathbb{F}_2^{2\times 3}$ are given by the following tables:

$\mathrm{rk}(\mathbf{X})$	0	1	2
$\overline{\mathrm{w}}_\ell(\mathbf{X})$	0	$\frac{1}{42}$	$\frac{1}{84}$

$\mathrm{rk}(\mathbf{X})$	0	1	2
$\overline{\mathrm{w}}_\mathrm{r}(\mathbf{X})$	0	$\frac{1}{56}$	$\frac{5}{336}$

$\overline{\mathrm{w}}_\ell$ is a probability distribution on $\mathbb{F}_2^{2\times 3}$ and satisfies (H1), (H2), but it does not yield a 1-good random 2×3 matrix over $\mathbb{F}_2$.

$\overline{\mathrm{w}}_\mathrm{r}$ defines, by Th. 11, a 1-good random matrix $\tilde{\mathbf{A}} \in \mathbb{F}_2^{2\times 3}$. This means that every coset of a right submodule $\mathcal{U}$ of $\mathbb{F}_2^{2\times 3}$ of size $|\mathcal{U}| = 8$ (which is one of the modules $\mathcal{U}_1, \mathcal{U}_2, \mathcal{U}_3$ corresponding to column spaces generated by $\binom{1}{0}$, $\binom{0}{1}$, $\binom{1}{1}$, respectively) has total weight $1/8$. For the submodules $\mathcal{U}_i$ this is obvious, since they contain the all-zero 2×3 matrix and 7 matrices of rank 1 and weight $1/56$. For the remaining cosets $\mathcal{U}_i + \mathbf{A}$ with $\mathbf{A} \notin \mathcal{U}_i$ it implies that each such coset contains 2 matrices of rank 1 and 6 matrices of rank 2.

Outline

Definition

The *right affine space of $m \times n$ matrices over* $\mathbb{F}_q$, denoted by $\mathrm{AG}_\mathrm{r}(m,n,\mathbb{F}_q)$, is the lattice of cosets (including the empty set) of right R_n-submodules of $\mathbb{F}_q^{m\times n}$. A coset $\mathbf{A}+\mathcal{U}$ is called an *r-dimensional flat (r-flat)* if $\mathcal{U} \cong \mathbb{F}_q^{r\times n}$ as an R_n-module. (Equivalently, the subspace of $\mathbb{F}_q^m$ corresponding to $\mathcal{U}$ has dimension r.)

Flats of dimension 0, 1, 2, $m-1$ are called points, lines, planes, and hyperplanes, respectively. The whole geometry (i.e. the flat $\mathbb{F}_q^{m\times n}$) has dimension m.

Left affine spaces $\mathrm{AG}_\ell(m,n,\mathbb{F}_q)$ are defined similarly.

Remark

In the *Geometry of Matrices* (after L.K. HUA and Z.X. WAN) one considers the space $\mathbb{F}_q^{m\times n}$ equipped with the collinearity relation $\operatorname{rk}(\mathbf{A}-\mathbf{B})=1$. Lines are 1-dimensional over $\mathbb{F}_q$ (and are intersections of left and right 1-flats in our sense).

Example (The plane $\mathrm{AG}_{\mathrm{r}}(2,2,\mathbb{F}_2)$)

$$
\begin{matrix}
\begin{pmatrix}0&0\\0&0\end{pmatrix} & \begin{pmatrix}1&0\\0&0\end{pmatrix} & \begin{pmatrix}0&1\\0&0\end{pmatrix} & \begin{pmatrix}1&1\\0&0\end{pmatrix}\\
\begin{pmatrix}0&0\\1&0\end{pmatrix} & \begin{pmatrix}1&0\\1&0\end{pmatrix} & \begin{pmatrix}0&1\\1&0\end{pmatrix} & \begin{pmatrix}1&1\\1&0\end{pmatrix}\\
\begin{pmatrix}0&0\\0&1\end{pmatrix} & \begin{pmatrix}1&0\\0&1\end{pmatrix} & \begin{pmatrix}0&1\\0&1\end{pmatrix} & \begin{pmatrix}1&1\\0&1\end{pmatrix}\\
\begin{pmatrix}0&0\\1&1\end{pmatrix} & \begin{pmatrix}1&0\\1&1\end{pmatrix} & \begin{pmatrix}0&1\\1&1\end{pmatrix} & \begin{pmatrix}1&1\\1&1\end{pmatrix}
\end{matrix}
$$

There are 16 points, 12 lines (3 parallel classes of size 4), and 8 MRD codes (2 parallel classes of size 4).

The 12 lines and 8 MRD codes impose on $\mathbb{F}_2^{2\times 2}$ the structure of the affine plane of order 4.

The Link with k-Good Random Matrices

Definition

Let k, m, n be positive integers with $k \leq \min\{m, n\}$. A set $\mathcal{A} \subseteq \mathbb{F}_q^{m \times n}$ is said to be *k-dense* if $\mathbf{U}\mathcal{A} = \mathbb{F}_q^{k \times n}$ for every full-rank matrix $\mathbf{U} \in \mathbb{F}_q^{k \times m}$.

As in the case of "good" we use the terms 1-*dense* and *dense* interchangeably.

Lemma

Let $\mathcal{A}$ be a nonempty subset of $\mathbb{F}_q^{m \times n}$ and $\tilde{\mathbf{A}}$ the random $m \times n$ matrix uniformly distributed over $\mathcal{A}$.

(i) *$\mathcal{A}$ is k-dense if and only if it meets every $(m-k)$-flat of $\mathrm{AG}_\mathrm{r}(m, n, \mathbb{F}_q)$ in at least one point, i.e., $\mathcal{A}$ is a blocking set with respect to $(m-k)$-flats in $\mathrm{AG}_\mathrm{r}(m, n, \mathbb{F}_q)$.*

(ii) *$\tilde{\mathbf{A}}$ is k-good if and only if $\mathcal{A}$ meets every $(m-k)$-flat of $\mathrm{AG}_\mathrm{r}(m, n, \mathbb{F}_q)$ in the same number, say λ, of points.*

The Minimum Size of Blocking Sets in $\mathrm{AG}_\mathrm{r}(m,n,\mathbb{F}_q)$

$\mu_k(m,n,\mathbb{F}_q)$ denotes the minimum size of a blocking set with respect to $(m-k)$-flats in $\mathrm{AG}_\mathrm{r}(m,n,\mathbb{F}_q)$ (respectively, the minimum size of a k-dense subset of $\mathbb{F}_q^{m\times n}$).

Theorem (The case $m \leq n$)

For $k \leq m \leq n$ we have $\mu_k(m,n,\mathbb{F}_q) = q^{kn}$, and a subset $\mathcal{A} \subseteq \mathbb{F}_q^{m\times n}$ of size q^{kn} is k-dense if and only if it is a (not necessarily linear) (m,n,k) MRD code.

The discrete version of the symmetry property of k-good random matrices is

Theorem (Left-right symmetry)

If $\mathcal{A} \subseteq \mathbb{F}_q^{m\times n}$ meets every $(m-k)$-flat of $\mathrm{AG}_\mathrm{r}(m,n,\mathbb{F}_q)$ in the same number, say λ, of points, then the same is true for the $(n-k)$-flats of $\mathrm{AG}_\ell(m,n,\mathbb{F}_q)$ (the corresponding number being $\lambda' = \lambda q^{k(n-m)}$).

MRD codes have $\lambda = 1$ (for $m \leq n$) resp. $\lambda' = 1$ (for $m \geq n$).

The Case $m > n$

Theorem

(i) $\mu_1(m, 1, q) = 1 + m(q-1)$ *for all* $m \geq 2$.

(ii) *For* $1 \leq k \leq n < m$ *we have the bounds* $q^{kn} < \mu_k(m, n, \mathbb{F}_q) < q^{km}$.

(iii) $\mu_1(3, 2, \mathbb{F}_2) = 6$;

(iv) $\mu_2(3, 2, \mathbb{F}_2) = 22$.

Notes

- $\mu_1(m, 1, q)$ is the known (JAMISON 1977, BROUWER-SCHRIJVER 1978) minimum size of a blocking set with respect to hyperplanes in the ordinary affine space $\mathrm{AG}(m, \mathbb{F}_q)$.
- The bounds in (ii) are rather weak and serve only to refute the obvious guesses "$\mu_k(m, n, \mathbb{F}_q) = q^n$" or "$\mu_k(m, n, \mathbb{F}_q) = q^m$".
- Parts (iii), (iv) required a fair amount of work (but could be done by hand).

Combinatorial Facts about $\mathrm{AG}_{\mathrm{r}}(3, 2, \mathbb{F}_2)$

- 64 points
- 112 lines (7 parallel classes of size 16)
- 28 planes (7 parallel classes of size 4)
- Planes are isomorphic to $\mathrm{AG}_{\mathrm{r}}(2, 2, \mathbb{F}_2)$.
- Two (distinct) collinear points are incident with 3 planes.
- Two non-collinear points are incident with a unique plane.

A blocking set with respect to planes of size 6

$$\begin{pmatrix}1 & 0\\ 0 & 1\\ 0 & 0\end{pmatrix},\begin{pmatrix}1 & 1\\ 1 & 0\\ 0 & 0\end{pmatrix},\begin{pmatrix}0 & 1\\ 1 & 1\\ 0 & 0\end{pmatrix},\begin{pmatrix}0 & 0\\ 1 & 0\\ 1 & 0\end{pmatrix},\begin{pmatrix}0 & 1\\ 0 & 0\\ 0 & 1\end{pmatrix},\begin{pmatrix}0 & 0\\ 0 & 0\\ 1 & 1\end{pmatrix}$$

Construction of a blocking set of size 22

Use $\mathrm{AG}_\ell(3,2,\mathbb{F}_2) \subset \mathrm{AG}(2,\mathbb{F}_8)$.

Lines of $\mathrm{AG}(2,\mathbb{F}_8)$ fall into two types:

- Lines of $\mathrm{AG}_\ell(3,2,\mathbb{F}_2)$ (three parallel classes, represented by $\mathbb{F}_8(1,0)$, $\mathbb{F}_8(0,1)$, $\mathbb{F}_8(1,1)$)
- MRD codes (six parallel classes, represented by $\mathcal{M}_i = \mathbb{F}_8(1,\alpha^i)$, $1 \leq i \leq 6$).

$\mathcal{A} = \mathcal{M}_1 \cup \mathcal{M}_2 \cup \mathcal{M}_4$ is the required blocking set.

The proof uses counting and the property that $\mathcal{A}$ meets every line of $\mathrm{AG}_\mathrm{r}(3,2,\mathbb{F}_2)$ in either 1 or 3 points.

Open Problem

Further study of the Maximal Arc Problem for $\mathrm{AG}_{\mathrm{r}}(m, n, \mathbb{F}_q)$.

Reference

S. Yang and T. Honold.
Good random matrices over finite fields.
Submitted for publication, May 2011.

Thank You