All binary MRD codes up to size 4×4

Michael Kiermaier

Institut für Mathematik
Universität Bayreuth
Germany

Conference on Applied Algebraic Geometry
Mini-symposium MS17 “Rank-Metric and Subspace Codes”
August 16, 2021
SIAM conference (held online)

joint work with Sascha Kurz and Alfred Wassermann

Goal of this talk

- Classification of all binary MRD-codes up to size 4×4.
- The full picture:
  - No restriction to quadratic sizes.
  - No restriction to linear codes.
- Summary of already known cases.
  In part using interconnections to
  - translation planes
  - (partial) spreads
- Settle the remaining cases
  by theoretical insight combined with (heavy) computation.

Outline

Definitions

- Rank distance on $\mathbb{F}_q^{m\times n}$ is $d(A,B) = \mathrm{rk}(A-B)$.
- Without restriction: $m \leq n$.
- $(\mathbb{F}_q^{m\times n}, d)$ is a metric space.
- $C \subseteq \mathbb{F}_q^{m\times n}$ is a rank-metric code.
- C $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{m\times n}$ $\implies$ C linear.
- minimum distance
  $d(C) = \min\{d(A,B) \mid A, B \in C, A \neq B\} \leq m$.
- Singleton bound: $\#C \leq q^{n(m-d+1)}$.
- Singleton bound sharp $\implies$ C MRD-code.
  (MRD = maximum rank distance)

MRD-Codes

- Singleton bound sharp $\implies$ C MRD-code.
- For distance $d = 1$, full space $\mathbb{F}_q^{m \times n}$ is trivial MRD-code.
  $\rightsquigarrow$ will assume $d \geq 2$ (so $2 \leq d \leq m \leq n$).
- MRD-codes do always exist!
  - Gabidulin codes (Delsarte 1978, Gabidulin 1985, Roth 1991)
  - generalized Gabidulin codes (Kshevetskiy, Gabidulin 2005)
  - generalized twisted Gabidulin codes (Sheekey 2016)
- $\rightsquigarrow$ Research problem: Classification of all MRD-codes.
- Needed: A notion of equivalence.

Equivalence

- Definition (state what we want!)

  $C, C' \subseteq \mathbb{F}_q^{m\times n}$ are equivalent if
  $\exists$ isometry ϕ of $(\mathbb{F}_q^{m\times n}, d)$ with $\phi(C) = C'$.

  Automorphism group

  $$\mathrm{Aut}(C) = \{\phi \text{ isometry of } (\mathbb{F}_q^{m\times n}, d) \mid \phi(C) = C\}$$

- Natural question:

  What is the isometry group $\mathrm{Aut}(\mathbb{F}_q^{m\times n}, d)$
  of the metric space ($\mathbb{F}_q^{m\times n}$,d),
  i.e. set of all distance-preserving bijections?

Isometry group of $(\mathbb{F}_q^{m\times n}, d)$

- **Theorem** (Hua 1951 (q even), Wan 1996 (q odd))

  For $m \geq 2$ and $n \geq 2$, $\mathrm{Aut}(\mathbb{F}_q^{m\times n}, d)$ consists of

  $$A \mapsto S\sigma(A)T + R$$

  and for $m = n$ (square case) additionally

  $$A \mapsto S\sigma(A^\top)T + R$$

  where $S \in \mathrm{GL}(m, q)$, $T \in \mathrm{GL}(n, q)$, $R \in \mathbb{F}_q^{m\times n}$, $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$.
- Automorphisms of the first type will be called inner.
- Automorphisms with $\sigma = \mathrm{id}$ will be called linear.

  Note: In our case $q = 2$ we have $\mathrm{Aut}(\mathbb{F}_2) = \{\mathrm{id}\}$, so all automorphisms are linear.

Subspace lattice

- Let V be a v-dimensional $\mathbb{F}_q$ vector space.
- Grassmannian $\begin{bmatrix} V \\ k \end{bmatrix}_q :=$ set of all k-dim. subspaces of V.
- Gaussian binomial coefficient

$$\#\begin{bmatrix} V \\ k \end{bmatrix}_q = \begin{bmatrix} v \\ k \end{bmatrix}_q = \frac{(q^v - 1)(q^{v-1} - 1) \cdot \ldots \cdot (q^{v-k+1} - 1)}{(q-1)(q^2-1) \cdot \ldots \cdot (q^k - 1)}$$

- Subspaces of V form a modular lattice (wrt. $\subseteq$).

Projective geometry

- projective geometry
  $\mathrm{PG}(v-1, q) = \mathrm{PG}(V) :=$ subspace lattice of V
  - Elements of $\begin{bmatrix} V \\ 1 \end{bmatrix}_q$ are points.
  - Elements of $\begin{bmatrix} V \\ 2 \end{bmatrix}_q$ are lines.
  - Elements of $\begin{bmatrix} V \\ 3 \end{bmatrix}_q$ are planes.
  - Elements of $\begin{bmatrix} V \\ 4 \end{bmatrix}_q$ are solids.

Spreads

A set $\mathcal{S} \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ is called

- a $(k-1)$-spread
  if each point is contained in exactly 1 element of $\mathcal{S}$.
- a partial $(k-1)$-spread
  if each point is contained in at most 1 element of $\mathcal{S}$.

  In this case, the points not contained in any element of $\mathcal{S}$ are called holes.

Geometrization: Lifted subspace codes

- Lifted subspace of $A \in \mathbb{F}_q^{m \times n}$ is

$$\Lambda(A) = \langle (I_m \; A) \rangle \in \begin{bmatrix} \mathbb{F}_q^{m+n} \\ m \end{bmatrix}_q,$$

  where
  - I_m is $m \times m$ unit matrix
  - $\langle \cdots \rangle$ denotes the row space.
- All $\Lambda(A)$ have trivial intersection with the special subspace

$$S = \langle e_{m+1}, \ldots, e_{m+n} \rangle \in \begin{bmatrix} \mathbb{F}_q^{m+n} \\ n \end{bmatrix}_q.$$

  where e_i is the i-th unit vector.
- Lifted subspace code of $C \subseteq \mathbb{F}_q^{m \times n}$ is

$$\Lambda(C) = \{\Lambda(A) \mid A \in C\}.$$

Lemma

Let $\mathcal{C} \subseteq \begin{bmatrix} \mathbb{F}_q^{m+n} \\ m \end{bmatrix}_q$ *and* $t = m - d + 1$. *Then*

(i) $\mathcal{C}$ *is lifted* $m \times n$ *MRD-code of distance* d $\iff$

(ii) $U \cap S = \{\mathbf{0}\}$ *for all* $U \in \mathcal{C}$ *and*
every $T \in \begin{bmatrix} \mathbb{F}_q^{m+n} \\ t \end{bmatrix}_q$ *with* $T \cap S = \{\mathbf{0}\}$
is contained in a unique element of $\mathcal{C}$.

Lemma

Let $m, n \geq 2$ *and* C, C' $m \times n$ *MRD-codes of distance* d.

(a) C *and* C' *are inner-isomorphic*
$\iff \Lambda(C) \cong \Lambda(C')$ *by a collineation in* $\mathrm{P\Gamma L}(\mathbb{F}_q^{m+n})$.

(b) $\mathrm{Aut}_{\mathrm{Inn}}(C) \cong \mathrm{Aut}_{\mathrm{P\Gamma L}}(\Lambda(C))$.

Conclusion

Instead of classifying MRD codes,
we can classify lifted MRD codes
(and benefit from the projective geometric setting).

Outline

Let $N(m, n, d)$ ($N_{\mathrm{Inn}}(m, n, d)$) be the number of all (inner) isomorphism types of $m \times n$ MRD-codes of distance d.
We want to fill the following tables:

$N_{\mathrm{Inn}}(m, n, 2)$	$n = 2$	$n = 3$	$n = 4$
$m = 2$	?(?)	?	?
$m = 3$		?(?)	?
$m = 4$			?(?)

$N_{\mathrm{Inn}}(m, n, 3)$	$n = 3$	$n = 4$
$m = 3$	?(?)	?
$m = 4$		?(?)

$N_{\mathrm{Inn}}(m, n, 4)$	$n = 4$
$m = 4$	?(?)

- For $m \neq n$, $N(m, n, d) = N_{\mathrm{Inn}}(m, n, d)$.
- For $m = n$, $N(m, n, d) \leq N_{\mathrm{Inn}}(m, n, d)$ is given in parentheses.

The case $d = m$

- Here $t = m - d + 1 = 1$.
- $\implies \Lambda(C)$ perfectly covers the points outside S.
- $\implies \Lambda(C)$ is a partial $(m-1)$-spread in $\mathrm{PG}(m+n-1, q)$, and S is the set of holes.

The subcase $d = m = n$

- Here, $\Lambda(C) \cup \{S\}$ is a $(m-1)$-spread in $\mathrm{PG}(2m-1, q)$.
- Attention:
  MRD-code $\longleftrightarrow$ spread + choice of special subspace
  $\Longrightarrow$ Single type of a spread $\mathcal{S}$ may correspond to more than 1 inner isomorphism type of MRD-codes, depending on the number of orbits of $\mathrm{Aut}(\mathcal{S})$ on $\mathcal{S}$ ($\mathcal{S}$-orbits).
- Known: $(m-1)$-spreads in $\mathrm{PG}(2m-1, q)$
  $\longleftrightarrow$ translation planes of order q^m.
- Known: Translation planes of order 4 and 8 unique, i.e. only the Desarguesian planes, which have a single $\mathcal{S}$-orbit.
  $\Longrightarrow$ $N_{\mathrm{Inn}}(2,2,2) = N_{\mathrm{Inn}}(3,3,3) = 1$ (only Gabidulin codes)

The case $d = m = n = 4$

- Dempwolff, Reifart 1983: Classification of translation planes of order 16 into 8 types.

plane	$\mathcal{S}$-orbits	#MRD-cds
Desarguesian plane	17	1
semifield plane with kernel $\mathbb{F}_4$	$16 + 1$	2
semifield plane with kernel $\mathbb{F}_2$	$16 + 1$	2
Hall plane	$12 + 5$	2
derived semifield plane	$12 + 3 + 2$	3
Dempwolff plane	$15 + 1 + 1$	3
Johnson-Walker plane	$14 + 3$	2
Lorimer-Rahilly plane	$14 + 3$	2
		17

- $\implies N_{\mathrm{Inn}}(4,4,4) = 17$
- 11 self-transpose codes (meaning $C \cong_{\mathrm{Inn}} C^{\top}$) and 3 transpose pairs of codes
  $\implies N(4,4,4) = 11 + 3 = 14$

Table update 1

$N_{\mathrm{Inn}}(m,n,2)$	$n=2$	$n=3$	$n=4$
$m=2$	1(1)	?	?
$m=3$		?(?)	?
$m=4$			?(?)

$N_{\mathrm{Inn}}(m,n,3)$	$n=3$	$n=4$
$m=3$	1(1)	?
$m=4$		?(?)

$N_{\mathrm{Inn}}(m,n,4)$	$n=4$
$m=4$	17(14)

The case $m = 2$, $n = 3$, $d = 2$

- Lifted MRD-code is partial line spread of size 8 in $\mathrm{PG}(4, 2)$.
- Classification by Gordon, Shaw and Soicher 2004:
  9 isomorphism types of such partial line spreads.
- To belong to a lifted MRD-code, the holes must form a plane (which is the special subspace).
- Only 1 type of such partial spread.
- $\implies N_{\mathrm{lnn}}(2, 3, 2) = 1$.

The case $m = 3$, $n = 4$, $d = 3$

- Done similarly in Honold, K., Kurz 2019.
- $\rightsquigarrow N_{\mathrm{lnn}}(3, 4, 3) = 37$.

The case $m = 2$, $n = 4$, $d = 2$

- Lifted MRD-code is partial line spread $\mathcal{S}$ of size 16 in $\mathrm{PG}(5, 2)$, such that the set of holes is a solid.
- A solid can be partitioned into 5 lines
  $\implies$ $\mathcal{S}$ can be extended to a spread in $\mathrm{PG}(5, 2)$.
- Classification of Mateva and Topalova 2009: 131044 isomorphism types of such spreads.
- Now:
  - For each such spread, remove all quintuples of lines forming a solid.
  - Sieve out isomorphic copies by “NetCan” (Feulner 2014).
- $\rightsquigarrow N_{\mathrm{lnn}}(2, 4, 2) = 44$.

Table update 2

$N_{\text{Inn}}(m,n,2)$	$n=2$	$n=3$	$n=4$
$m=2$	1(1)	1	44
$m=3$		?(?)	?
$m=4$			?(?)

$N_{\text{Inn}}(m,n,3)$	$n=3$	$n=4$
$m=3$	1(1)	37
$m=4$		?(?)

$N_{\text{Inn}}(m,n,4)$	$n=4$
$m=4$	17(14)

The remaining cases

- Observation
  For n and d fixed, all cases with minimum m are done.
- Plan: Recursively use $(m-1,n,d)$ to do (m,n,d).

Reduction to $m - 1$

- Let C be a binary $m \times n$ MRD-Code of distance d.
- Let C' be the subcode consisting of all codewords with the same (fixed) last row.
- After removing the last row, C' is a binary $(m-1) \times n$ MRD-code of distance d.

Resulting classification strategy

We reverse the above process.

- Loop over representatives C' of $(m-1) \times n$ MRD-codes of distance d.
- Append a zero row to all codewords of C'.
- Compute all extensions of C' to an $m \times n$ MRD-code of distance d.
  - Can be stated as an "exact cover-problem".
  - Very efficient solver "dlx" by Donald Knuth based on the "dancing links" strategy.
- In the end: Sieve out isomorphic copies.

Resulting classification strategy, cont.

Strategy applied to the remaining cases:

- 3×3, $d = 2$: success, within a few seconds CPU time.
  $\rightsquigarrow N_{\mathrm{Inn}}(3, 3, 2) = 1$
- 4×4, $d = 3$: success, withing a few hours CPU time.
  $\rightsquigarrow N_{\mathrm{Inn}}(4, 4, 3) = 1$.

  Surprising result

  The only binary, not necessarily linear 4×4 MRD-code of distance 3 is the Gabidulin code!
- 4×4, $d = 2$: success, within few days CPU time.
  However, it is based on the still missing last case:
- No chance for 3×4, $d = 2$.

Table update 3

$N_{\mathrm{Inn}}(m,n,2)$	$n=2$	$n=3$	$n=4$
$m=2$	1(1)	1	44
$m=3$		1(1)	?
$m=4$			?

$N_{\mathrm{Inn}}(m,n,3)$	$n=3$	$n=4$
$m=3$	1(1)	37
$m=4$		1(1)

$N_{\mathrm{Inn}}(m,n,4)$	$n=4$
$m=4$	17(14)

The hardest case 3×4, $d = 2$

- $\#C = 2^8 = 256$. Each of the 16 possible last rows determines a 2×4 MRD-code of size 16 (44 types).
- (remote remark:
  It is the setting of the binary q-analog of the Fano plane.)
- Look for a suitable intermediate classification goal...
- ...small enough such that it can be computed and the number of resulting cases is not too high;
- ...large enough such that the completions to full MRD-codes can be computed.
- Use the configuration of 32 matrices by fixing two last lines. (two combined 2×4 MRD-codes)
- $\rightsquigarrow$ 5.748.056 cases where the extensions to size 256 need to be computed.
- Took 254 CPU years on a computing cluster at the LRZ (Leibniz-Rechenzentrum) Munich.
- $\rightsquigarrow N_{\mathrm{Inn}}(3, 4, 2) = 33$

The last case 4×4, $d = 2$

- $\#C = 2^{12} = 4096$
- As discussed:
  Can be computed from 3×4, $d = 2$ within a few days.
- $\rightsquigarrow N_{\mathrm{Inn}}(4, 4, 2) = 9$

№	$\#\mathrm{Aut}_{\mathrm{Inn}}(C)$	linear?	transpose
1	3686400	yes	self
2	442368	yes	self
3	184320	no	self
4	86016	no	№ 5
5	86016	no	№ 4
6	76800	no	self
7	73728	yes	self
8	27648	no	self
9	18432	no	self

- $\rightsquigarrow N(4, 4, 2) = 8$

Final table update

$N_{\text{Inn}}(m,n,2)$	$n=2$	$n=3$	$n=4$
$m=2$	1(1)	1	44
$m=3$		1(1)	33
$m=4$			9(8)

$N_{\text{Inn}}(m,n,3)$	$n=3$	$n=4$
$m=3$	1(1)	37
$m=4$		1(1)

$N_{\text{Inn}}(m,n,4)$	$n=4$
$m=4$	17(14)

Thank you!

Slides can be found at

`https://www.mathe2.uni-bayreuth.de/michaelk/`