All binary MRD codes up to size $4 \times 4$

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 $4 \times 4$.
- 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

Introduction and preliminaries

The classification
Definitions

- **Rank distance** on $\mathbb{F}_q^{m\times n}$ is $d(A, B) = \text{rk}(A - B)$.
- 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 $F_q^{m \times n}$ is trivial MRD-code.
  $\sim$ 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)
- $\sim$ Research problem: Classification of all MRD-codes.
- Needed: A notion of equivalence.
Equivalence

Definition (state what we want!)

C, C' ⊆ F_q^{m×n} are equivalent if

∃ isometry φ of (F_q^{m×n}, d) with φ(C) = C'.

Automorphism group

Aut(C) = \{φ isometry of (F_q^{m×n}, d) | φ(C) = C\}

Natural question:

What is the isometry group Aut(F_q^{m×n}, d)

of the metric space (F_q^{m×n}, d),
i.e. set of all distance-preserving bijections?
Isometry group of \((\mathbb{F}_q^{m \times n}, d)\)

- **Theorem** (Hua 1951 \((q\ \text{even})\), Wan 1996 \((q\ \text{odd})\))
  
  For \(m \geq 2\) and \(n \geq 2\), \(\text{Aut}(\mathbb{F}_q^{m \times n}, d)\) 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 \(S \in \text{GL}(m, q)\), \(T \in \text{GL}(n, q)\), \(R \in \mathbb{F}_q^{m \times n}\), \(\sigma \in \text{Aut}(\mathbb{F}_q)\).

- Automorphisms of the first type will be called **inner**.
- Automorphisms with \(\sigma = \text{id}\) will be called **linear**.

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

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

$$
\# \left[ \begin{array}{c} V \\ k \end{array} \right]_q = \left[ \begin{array}{c} v \\ k \end{array} \right]_q = \frac{(q^v - 1)(q^{v-1} - 1) \cdots (q^{v-k+1} - 1)}{(q - 1)(q^2 - 1) \cdots (q^k - 1)}
$$

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

Projective geometry

- projective geometry $PG(v - 1, q) = PG(V) := $ subspace lattice of $V$
  - Elements of $\left[ \begin{array}{c} V \\ 1 \end{array} \right]_q$ are points.
  - Elements of $\left[ \begin{array}{c} V \\ 2 \end{array} \right]_q$ are lines.
  - Elements of $\left[ \begin{array}{c} V \\ 3 \end{array} \right]_q$ are planes.
  - Elements of $\left[ \begin{array}{c} V \\ 4 \end{array} \right]_q$ are solids.
Spreads

A set $S \subseteq \binom{V}{k}_q$ is called

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

In this case, the points not contained in any element of $S$ are called holes.
Geometrization: Lifted subspace codes

- **Lifted subspace** of $A \in \mathbb{F}^m_{q \times n}$ is

$$\Lambda(A) = \langle (I_m \ A) \rangle \in \left[ \mathbb{F}^{m+n}_q \right]^m_n,$$

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**

$$S = \langle e_{m+1}, \ldots, e_{m+n} \rangle \in \left[ \mathbb{F}^{m+n}_q \right]_{m \times n}.$$

where $e_i$ is the $i$-th unit vector.

- **Lifted subspace code** of $C \subseteq \mathbb{F}^m_{q \times n}$ is

$$\Lambda(C) = \{ \Lambda(A) \mid A \in C \}.$$
Lemma
Let $\mathcal{C} \subseteq \left[\mathbb{F}_q^{m+n}\right]_q$ and $t = m - d + 1$. Then

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

(ii) $U \cap S = \{0\}$ for all $U \in \mathcal{C}$ and every $T \in \left[\mathbb{F}_q^{m+n}\right]_q$ with $T \cap S = \{0\}$ is contained in a unique element of $\mathcal{C}$.

Lemma
Let $m, n \geq 2$ and $\mathcal{C}, \mathcal{C}'$ $m \times n$ MRD-codes of distance $d$.

(a) $\mathcal{C}$ and $\mathcal{C}'$ are inner-isomorphic

$\iff \Lambda(\mathcal{C}) \cong \Lambda(\mathcal{C}')$ by a collineation in $\text{PGL}(\mathbb{F}_q^{m+n})$.

(b) $\text{Aut}_{\text{Inn}}(\mathcal{C}) \cong \text{Aut}_{\text{PGL}}(\Lambda(\mathcal{C}))$.

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

Introduction and preliminaries

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

<table>
<thead>
<tr>
<th>( N_{\text{Inn}}(m, n, 2) )</th>
<th>( n = 2 )</th>
<th>( n = 3 )</th>
<th>( n = 4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( m = 2 )</td>
<td>(?(?))</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>( m = 3 )</td>
<td>(?(?))</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>( m = 4 )</td>
<td>(?(?))</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( N_{\text{Inn}}(m, n, 3) )</th>
<th>( n = 3 )</th>
<th>( n = 4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( m = 3 )</td>
<td>(?(?))</td>
<td>?</td>
</tr>
<tr>
<td>( m = 4 )</td>
<td>(?(?))</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( N_{\text{Inn}}(m, n, 4) )</th>
<th>( n = 4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( m = 4 )</td>
<td>(?(?))</td>
</tr>
</tbody>
</table>

\[ \begin{align*}
\text{For } m \neq n, \; N(m, n, d) &= N_{\text{Inn}}(m, n, d). \\
\text{For } m = n, \; N(m, n, d) &\leq N_{\text{Inn}}(m, n, d) \text{ is given in parentheses.}
\end{align*} \]
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 $\text{PG}(m + n - 1, q)$, and $S$ is the set of holes.
The subcase $d = m = n$

- Here, $\Lambda(C) \cup \{S\}$ is a $(m - 1)$-spread in $\text{PG}(2m - 1, q)$.
- Attention:
  MRD-code $\iff$ spread + choice of special subspace
  $\implies$ Single type of a spread $S$ may correspond to more than 1 inner isomorphism type of MRD-codes, depending on the number of orbits of $\text{Aut}(S)$ on $S$ ($S$-orbits).

- Known: $(m - 1)$-spreads in $\text{PG}(2m - 1, q)$
  $\iff$ 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 $S$-orbit.
  $\implies N_{\text{Inn}}(2, 2, 2) = N_{\text{Inn}}(3, 3, 3) = 1$ (only Gabidulin codes)
The case $d = m = n = 4$

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

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

\[
\Rightarrow N_{\text{Inn}}(4, 4, 4) = 17
\]

\[
\Rightarrow 11 \text{ self-transpose codes} \text{ (meaning } C \cong_{\text{Inn}} C^\top) \text{ and 3 transpose pairs of codes} \\
\Rightarrow N(4, 4, 4) = 11 + 3 = 14
\]
Table update 1

<table>
<thead>
<tr>
<th>$N_{\text{Inn}}(m, n, 2)$</th>
<th>$n = 2$</th>
<th>$n = 3$</th>
<th>$n = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m = 2$</td>
<td>1(1)</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>$m = 3$</td>
<td>?(?)</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>$m = 4$</td>
<td></td>
<td></td>
<td>?(?)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$N_{\text{Inn}}(m, n, 3)$</th>
<th>$n = 3$</th>
<th>$n = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m = 3$</td>
<td>1(1)</td>
<td>?</td>
</tr>
<tr>
<td>$m = 4$</td>
<td></td>
<td>?(?)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$N_{\text{Inn}}(m, n, 4)$</th>
<th>$n = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m = 4$</td>
<td>17(14)</td>
</tr>
</tbody>
</table>
The case \( m = 2, n = 3, d = 2 \)

- Lifted MRD-code is partial line spread of size 8 in \( \text{PG}(4, 2) \).
- 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.
- \( \implies N_{\text{Inn}}(2, 3, 2) = 1. \)

The case \( m = 3, n = 4, d = 3 \)

- Done similarly in Honold, K., Kurz 2019.
- \( \leadsto N_{\text{Inn}}(3, 4, 3) = 37. \)
The case $m = 2$, $n = 4$, $d = 2$

- Lifted MRD-code is partial line spread $S$ of size 16 in $\text{PG}(5, 2)$, such that the set of holes is a solid.
- A solid can be partitioned into 5 lines $\implies S$ can be extended to a spread in $\text{PG}(5, 2)$.
- 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).
- $N_{\text{inn}}(2, 4, 2) = 44$. 
### Table update 2

<table>
<thead>
<tr>
<th>$N_{\text{Inn}}(m, n, 2)$</th>
<th>$n = 2$</th>
<th>$n = 3$</th>
<th>$n = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m = 2$</td>
<td>1(1)</td>
<td>1</td>
<td>44</td>
</tr>
<tr>
<td>$m = 3$</td>
<td>??(?)</td>
<td>??(?)</td>
<td>??(?)</td>
</tr>
<tr>
<td>$m = 4$</td>
<td>??(?)</td>
<td>??(?)</td>
<td>??(?)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$N_{\text{Inn}}(m, n, 3)$</th>
<th>$n = 3$</th>
<th>$n = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m = 3$</td>
<td>1(1)</td>
<td>37</td>
</tr>
<tr>
<td>$m = 4$</td>
<td>??(?)</td>
<td>??(?)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$N_{\text{Inn}}(m, n, 4)$</th>
<th>$n = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m = 4$</td>
<td>17(14)</td>
</tr>
</tbody>
</table>

### 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:

- $3 \times 3, d = 2$: success, within a few seconds CPU time.
  $\rightsquigarrow N_{\text{inn}}(3, 3, 2) = 1$

- $4 \times 4, d = 3$: success, within a few hours CPU time.
  $\rightsquigarrow N_{\text{inn}}(4, 4, 3) = 1$.

Surprising result
The only binary, not necessarily linear $4 \times 4$ MRD-code of distance 3 is the Gabidulin code!

- $4 \times 4, d = 2$: success, within few days CPU time.
  However, it is based on the still missing last case:

- No chance for $3 \times 4, d = 2$. 
Table update 3

<table>
<thead>
<tr>
<th>$N_{\text{Inn}}(m, n, 2)$</th>
<th>$n = 2$</th>
<th>$n = 3$</th>
<th>$n = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m = 2$</td>
<td>1(1)</td>
<td>1</td>
<td>44</td>
</tr>
<tr>
<td>$m = 3$</td>
<td></td>
<td>1(1)</td>
<td>?</td>
</tr>
<tr>
<td>$m = 4$</td>
<td></td>
<td></td>
<td>?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$N_{\text{Inn}}(m, n, 3)$</th>
<th>$n = 3$</th>
<th>$n = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m = 3$</td>
<td>1(1)</td>
<td>37</td>
</tr>
<tr>
<td>$m = 4$</td>
<td>1(1)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$N_{\text{Inn}}(m, n, 4)$</th>
<th>$n = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m = 4$</td>
<td>17(14)</td>
</tr>
</tbody>
</table>
The hardest case $3 \times 4$, $d = 2$

- $\# C = 2^8 = 256$. Each of the 16 possible last rows determines a $2 \times 4$ 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 $2 \times 4$ MRD-codes)

- $\leadsto 5,748,056$ 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.

- $\leadsto N_{\text{inn}}(3, 4, 2) = 33$
The last case $4 \times 4, d = 2$

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

<table>
<thead>
<tr>
<th>№</th>
<th>$# \text{Aut}_{\text{Inn}}(C)$</th>
<th>linear?</th>
<th>transpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3686400</td>
<td>yes</td>
<td>self</td>
</tr>
<tr>
<td>2</td>
<td>442368</td>
<td>yes</td>
<td>self</td>
</tr>
<tr>
<td>3</td>
<td>184320</td>
<td>no</td>
<td>self</td>
</tr>
<tr>
<td>4</td>
<td>86016</td>
<td>no</td>
<td>№ 5</td>
</tr>
<tr>
<td>5</td>
<td>86016</td>
<td>no</td>
<td>№ 4</td>
</tr>
<tr>
<td>6</td>
<td>76800</td>
<td>no</td>
<td>self</td>
</tr>
<tr>
<td>7</td>
<td>73728</td>
<td>yes</td>
<td>self</td>
</tr>
<tr>
<td>8</td>
<td>27648</td>
<td>no</td>
<td>self</td>
</tr>
<tr>
<td>9</td>
<td>18432</td>
<td>no</td>
<td>self</td>
</tr>
</tbody>
</table>

- $\sim N(4, 4, 2) = 8$
## Final table update

<table>
<thead>
<tr>
<th>( N_{\text{Inn}}(m, n, 2) )</th>
<th>n = 2</th>
<th>n = 3</th>
<th>n = 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>m = 2</td>
<td>1(1)</td>
<td>1</td>
<td>44</td>
</tr>
<tr>
<td>m = 3</td>
<td></td>
<td>1(1)</td>
<td>33</td>
</tr>
<tr>
<td>m = 4</td>
<td></td>
<td></td>
<td>9(8)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( N_{\text{Inn}}(m, n, 3) )</th>
<th>n = 3</th>
<th>n = 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>m = 3</td>
<td>1(1)</td>
<td>37</td>
</tr>
<tr>
<td>m = 4</td>
<td></td>
<td>1(1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( N_{\text{Inn}}(m, n, 4) )</th>
<th>n = 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>m = 4</td>
<td>17(14)</td>
</tr>
</tbody>
</table>

Thank you!

Slides can be found at https://www.mathe2.uni-bayreuth.de/michaelk/