Unextendible Sets of Mutually Unbiased Bases (MUBs)

Markus Grassl

Markus.Grassl@mpl.mpg.de
www.codetables.de

August 10, 2015
Overview

- Mutually Unbiased Bases (MUBs) and symplectic spreads
- Unextendible MUBs
- Characterization of symplectic spreads
- Small maximal partial spread in large dimension
- Constructions & search techniques
- Computational results
Mutually Unbiased Bases (MUBs)

- orthogonal bases $\mathcal{B}^j := \{ |\psi^j_k \rangle : k = 1, \ldots, d \} \subset \mathbb{C}^d$
- basis states are “mutually unbiased”:
  
  \[ |\langle \psi^j_k | \psi^l_m \rangle|^2 = \begin{cases} 
  1/d & \text{for } j \neq l, \\
  \delta_{k,m} & \text{for } j = l.
  \end{cases} \]

- at most $d + 1$ MUBs in dimension $d$
- constructions for $d + 1$ MUBs only known for prime powers $d = p^e$
- lower bound [Klappenecker & Rötteler, quant-ph/0309120]:
  \[
  N(m \cdot n) \geq \min\{N(m), N(n)\} \geq 3 \\
  N(p_1^{e_1} p_2^{e_2} \ldots p_\ell^{e_\ell}) \geq \min_i p_i^{e_i + 1}
  \]
MUBs and Unitary Error Bases

[S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, & F. Vatan, quant-ph/0103162]

**Theorem:**
There exists \( k \) MUBs in dimension \( d \) if and only if there are \( k(d - 1) \) traceless, mutually orthogonal matrices \( U_{j,t} \in U(d, \mathbb{C}) \) that can be partitioned into \( k \) sets of commuting matrices:

\[
\mathcal{B} = \mathcal{C}_1 \cup \ldots \cup \mathcal{C}_k,
\]

where \( \mathcal{C}_j \cap \mathcal{C}_l = \emptyset \) and \( |\mathcal{C}_j| = d - 1 \)

Each of the \( k \) orthogonal bases is given by the common eigenstates of the commuting matrices in one class \( \mathcal{C}_j \).

**Ansatz:**
Use the matrices \( X^\alpha Z^\beta \) of the generalized Pauli group.
Error Basis

[A. Ashikhmin & E. Knill, Nonbinary quantum stabilizer codes, IEEE-IT 47, pp. 3065–3072 (2001)]

\[ X^\alpha := \sum_{x \in \mathbb{F}_q} |x + \alpha\rangle\langle x| \quad \text{for} \ \alpha \in \mathbb{F}_q \]

and \[ Z^\beta := \sum_{z \in \mathbb{F}_q} \omega^{\text{tr}(\beta z)} |z\rangle\langle z| \quad \text{for} \ \beta \in \mathbb{F}_q \ (\omega := \omega_p = \exp(2\pi i/p)) \]

generalized Pauli Group \( P_n \)

\[ \omega^\gamma (X^{\alpha_1} Z^{\beta_1}) \otimes (X^{\alpha_2} Z^{\beta_2}) \otimes \ldots \otimes (X^{\alpha_n} Z^{\beta_n}) =: \omega^\gamma X^\alpha Z^\beta, \]

where \( \alpha, \beta \in \mathbb{F}_q^n, \gamma \in \mathbb{F}_p \).

quotient group:

\[ \overline{P}_n := P_n / \langle \omega I \rangle \cong (\mathbb{F}_q \times \mathbb{F}_q)^n \cong \mathbb{F}_q^n \times \mathbb{F}_q^n \]
Abelian Subgroups & Symplectic Spreads

Abelian subgroup $S$:

$$(\alpha, \beta) \star (\alpha', \beta') = 0 \text{ for all } \omega \gamma(X^\alpha Z^\beta), \omega \gamma'(X^{\alpha'} Z^{\beta'}) \in S,$$

symplectic inner product $\star$ on $\mathbb{F}^n_q \times \mathbb{F}^n_q$:

$$(v, w) \star (v', w') := v \cdot w' - v' \cdot w = \sum_{i=1}^n v_i w_i' - v_i' w_i$$

maximal Abelian subgroups $\iff$ totally (symplectic) isotropic subspaces of $\mathbb{F}^{2n}_q$ (modulo the center of $\mathcal{P}_n$)

subgroups intersect in center $\iff$ symplectic spaces intersect trivially

$k$ MUBs $\iff$ partial symplectic spread of size $k$
incomplete partitioning of two-qubit Pauli matrices:

\[ C_1 = \{ I \otimes X, \ X \otimes I, \ X \otimes X \} \quad G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \]

\[ C_2 = \{ I \otimes Z, \ Z \otimes I, \ Z \otimes Z \} \quad G_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \]

\[ C_3 = \{ X \otimes Z, \ Z \otimes X, \ Y \otimes Y \} \quad G_3 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \]

This gives a set of three (real) MUBs that is strongly unextendible.

In general:

A set of MUBs from a partitioning of unitary operators is \textit{weakly unextendible} if one cannot add another eigenbasis of those unitary operators.
A set of mutually unbiased bases \( \{ \mathcal{B}^{(1)}, \ldots, \mathcal{B}^{(m)} \} \) is unextendible if there is no other basis that is unbiased with respect to all bases \( \mathcal{B}^{(j)} \).

If there is not even a single unbiased\(^a\) vector, the set of MUBs is called strongly unextendible.

A set of mutually unbiased bases constructed via eigenbases of generalized Pauli matrices is weakly unextendible if no other eigenbasis of Pauli matrices can be added.

\[ \implies \] maximal partial spreads yield weakly unextendible MUBs

---

\(^a\)A vector \( |\phi\rangle \) is unbiased to a set of vectors \( |\psi_i\rangle \) if \( |\langle \phi | \psi_i \rangle| = \text{const.} \)
Symplectic Spreads

totally isotropic subspace:

- subspace $S_i \leq \mathbb{F}_q^{2n}$ such that $S_i = S_i^*$
- symplectic self-dual code $[2n, n, d]_q$ or $(n, q^n, d)_{q^2}$
- quantum code $[[n, 0, d]]_q$

symplectic spread

collection of totally isotropic subspaces $S_i$ with trivial intersection:

- $S_i \cap S_j = \{0\}$ ($i \neq j$)
- $S_i + S_j = \mathbb{F}_q^{2n}$ ($i \neq j$)

maximal partial spread

collection of subspaces $S_i$ that cannot be enlarged
Some Known Results

- maximal size of a (complete) symplectic spread in $\mathbb{F}_q^{2n}$ is $q^n + 1$
- complete spreads exists for all prime powers $q$ and $n$
  - $n = 1$: take the lines through the origin in the affine space $\mathbb{F}_q^2$
  - $n > 1$: expand the spread in $\mathbb{F}_q^{2n}$ using a symmetric basis of $\mathbb{F}_q^n$ as matrix algebra over $\mathbb{F}_q$
- maximal partial symplectic spreads have mainly been studied for the case $n = 2$ using generalized quadrangles (e.g., by the group in Ghent)

I did not find much information on maximal partial symplectic spreads for $n > 2$. 
Defining Conditions for Symplectic Spreads

Normal Form of Generators:

\[ G_\infty = \begin{pmatrix} 0 & I \\ \end{pmatrix} \quad \text{or} \quad G_i = \begin{pmatrix} I & A_i \\ \end{pmatrix}, \quad A_i = A_i^t \text{ (symmetric)} \]

Proof:

- transitive action of symplectic group allows choice of \( G_\infty \)
- joint row span of \( G_\infty \) and \( G_i \) is the full space \( \implies G_i = (I|A_i) \)
- \( S_i = S_i^* \implies A_i \) is symmetric

Defining Conditions for Symplectic Spreads:

\[ S_i + S_j = \mathbb{F}_q^{2n} \iff \det \begin{pmatrix} I & A_i \\ I & A_j \\ \end{pmatrix} \neq 0 \iff \det(A_i - A_j) \neq 0 \]

\[ \iff (\det(A_i - A_j))^{q-1} = 1 \]
Theorem There is a maximal partial symplectic spread of size $q + 1$ for $q = 2^m$ and $n = 2$, and there is no smaller maximal partial symplectic spread.

Proof (maximality):

generators: $G_\infty = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ and $G_\alpha = \begin{pmatrix} 1 & 0 & 0 & \alpha \\ 0 & 1 & \alpha & 0 \end{pmatrix}$, $\alpha \in \mathbb{F}_q$

additional generator $G' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_{00} & x_{01} \\ x_{01} & x_{11} \end{pmatrix}$

condition: $\det \begin{pmatrix} x_{00} & x_{01} & x_{01} - \alpha \\ x_{01} & x_{11} \end{pmatrix} = x_{00}x_{11} + x_{01}^2 + \alpha^2 \neq 0$ for all $\alpha \in \mathbb{F}_q$
**Small Maximal Partial Spreads**

**Theorem** For $q$ an even prime power, the expansion of the smallest maximal partial spread of size $q^m + 1$ in $\mathbb{F}_{q^m}^4$ yields a maximal partial spread in $\mathbb{F}_q^{4m}$.

**Proof (outline)**

Let $\Gamma \in \mathbb{F}_{q^m}^{m \times m}$ be a symmetric matrix corresponding to a primitive element $\gamma$ of $\mathbb{F}_{q^m}$.

Expansions of the generators:

$$G_\infty = \begin{pmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{pmatrix}, \quad G_0 = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \end{pmatrix}, \quad \text{and}$$

$$G_{\gamma^j} = \begin{pmatrix} I & 0 & 0 & \Gamma^j \\ 0 & I & \Gamma^j & 0 \end{pmatrix}, \quad j = 0, \ldots, q^m - 2$$
Small Maximal Partial Spreads (cont.)

Lemma

Over the big field $\mathbb{F}_{q^m}$, the matrix $\begin{pmatrix} 0 & \Gamma_j \\ \Gamma_j & 0 \end{pmatrix}$ is similar to

$$A(\alpha) = \begin{pmatrix} \alpha \\ \alpha^q \\ \cdots \\ \alpha^{q^{m-1}} \end{pmatrix}, \quad \alpha = \gamma_j$$
additional generator

\[ G' = ( I \mid X ) \], where \( X \) is a symmetric \( 2m \times 2m \) matrix

conditions

\[ \det X \neq 0 \text{ and } \det \left( X - \left( \begin{array}{cc} 0 & \Gamma^j \\ \Gamma^j & 0 \end{array} \right) \right) \neq 0 \text{ for } j = 0, \ldots, q - 2 \]

\[ \iff \det (\tilde{X} - A(\alpha)) \neq 0 \text{ for } \alpha \in \mathbb{F}_{q^m} \]

\[ \iff \left( \det (\tilde{X} - A(\alpha)) \right)^{q^{-1}} = 1 \text{ for } \alpha \in \mathbb{F}_{q^m} \]

**Theorem** For \( q = 2^{m_0} \), a symmetric matrix \( \tilde{X} \), and \( A(\alpha) \) as above:

\[ \sum_{\alpha \in \mathbb{F}_{q^m}} \left( \det (\tilde{X} - A(\alpha)) \right)^{q^{-1}} = 1. \]

\[ \implies \text{The expanded spread over the subfield is maximal.} \]
Construction I: Subfield Expansion

Take a maximal partial spread in $\mathbb{F}_{q^m}^{2n}$ and expand it to obtain a partial spread in $\mathbb{F}_q^{2mn}$.

**Problem:**
A maximal partial spread over an extension field need not remain maximal when represented over a subfield:

- $q = 4 = 2^2$, $n = 3$: size 17
- $q = 9 = 3^2$, $n = 2$: size 22, 23, 24, 25, and 29

Moreover, this does not yield maximal partial spreads in $\mathbb{F}_q^{2n}$, $n$ prime.

$\implies$ Find criteria to decide when the expansion remains to be maximal.
Construction II: Extension

Given generators

\[ G_\infty = \begin{pmatrix} 0 & I \end{pmatrix}, \quad \text{and} \quad G_i = \begin{pmatrix} I & A_i \end{pmatrix} \]

find a symmetric matrix \( X \) with

\[ \det(X - A_i) \neq 0 \iff (\det(X - A_i))^{q-1} = 1 \]

\( \implies \) system of polynomial equations for the symmetric matrix \( X \)

\( \implies \) compute Gröbner basis

\( \implies \) proves maximality or provides candidates for extension
Exhaustive & Heuristic Search

exhaustive search

- graph $G$ with all symmetric matrices as vertices
- edge between $A_i$ and $A_j$ iff $\det(A_i - A_j) \neq 0$
- maximal cliques in $G$ of size $m$ correspond to maximal partial spreads of size $m + 1$ (use cliquer)

heuristic search

- start with a spread $S = \{S_\infty, S_1, \ldots, S_m\}$
- pick a symmetric matrix $A$ such that $S' \notin S$, $S'$ the row span of $( I \mid A )$
- keep those $S_i \in S$ that intersect trivially with $S'$
- compute maximal extension of this partial spread
## Computational Results

<table>
<thead>
<tr>
<th>$q^n$</th>
<th>$q$</th>
<th>$n$</th>
<th>size</th>
<th>remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>2</td>
<td>2</td>
<td>3, 5</td>
<td>complete</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>3</td>
<td>5, 9</td>
<td>complete</td>
</tr>
<tr>
<td>16</td>
<td>2</td>
<td>4</td>
<td>5, 8, 9, 11, 13, 17</td>
<td>complete</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>2</td>
<td>5, 9, 11, 13, 17</td>
<td>complete</td>
</tr>
<tr>
<td>32</td>
<td>2</td>
<td>5</td>
<td>9, ..., 15, 17, 33</td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>2</td>
<td>6</td>
<td>9, 13, ..., 47, 49, 51, 57, 65</td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>4</td>
<td>3</td>
<td>17, ..., 43, 49, 65</td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>8</td>
<td>2</td>
<td>9, 17, 21, ..., 47, 49, 51, 57, 65</td>
<td></td>
</tr>
<tr>
<td>128</td>
<td>2</td>
<td>7</td>
<td>21, ..., 31, 33, 35, 37, 39, 45, 49, 53, 57, 61, 65, 129</td>
<td></td>
</tr>
<tr>
<td>256</td>
<td>2</td>
<td>8</td>
<td>17, 28, ..., 205, 209, 211, 213, 214, 215, 225, 227, 241, 257</td>
<td>new values</td>
</tr>
<tr>
<td>256</td>
<td>4</td>
<td>4</td>
<td>17, 33, 35, ..., 205, 209, 211, 213, 214, 215, 225, 227, 241, 257</td>
<td></td>
</tr>
<tr>
<td>256</td>
<td>16</td>
<td>2</td>
<td>17, 33, 46, ..., 205, 209, 211, 213, 214, 215, 225, 227, 241, 257</td>
<td></td>
</tr>
<tr>
<td>$q^n$</td>
<td>$q$</td>
<td>$n$</td>
<td>size</td>
<td>remark</td>
</tr>
<tr>
<td>-------</td>
<td>-----</td>
<td>-----</td>
<td>--------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>2</td>
<td>5, 8, 10</td>
<td>complete</td>
</tr>
<tr>
<td>27</td>
<td>3</td>
<td>3</td>
<td>10, . . . , 20, 28</td>
<td>complete</td>
</tr>
<tr>
<td>81</td>
<td>3</td>
<td>4</td>
<td>18, . . . , 68, 70, 73, 74, 82</td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>9</td>
<td>2</td>
<td>22, . . . , 68, 70, 73, 74, 82</td>
<td></td>
</tr>
<tr>
<td>243</td>
<td>3</td>
<td>5</td>
<td>32, . . . , 120, 123, 154, 163, 244</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>5</td>
<td>2</td>
<td>13, . . . , 20, 22, 24, 26</td>
<td>complete</td>
</tr>
<tr>
<td>125</td>
<td>5</td>
<td>3</td>
<td>27, . . . , 90, 101, 126</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>7</td>
<td>2</td>
<td>14, 17, . . . , 42, 44, 48, 50</td>
<td></td>
</tr>
<tr>
<td>121</td>
<td>11</td>
<td>2</td>
<td>28, . . . , 106, 109, 110, 112, 120, 122</td>
<td>new values</td>
</tr>
<tr>
<td>169</td>
<td>13</td>
<td>2</td>
<td>40, . . . , 140, 145, 146, 148, 158, 170</td>
<td>new values</td>
</tr>
<tr>
<td>289</td>
<td>17</td>
<td>2</td>
<td>67, . . . , 238, 241, . . . , 248, 257, 258, 260, 274, 290</td>
<td>new values</td>
</tr>
<tr>
<td>361</td>
<td>19</td>
<td>2</td>
<td>82, . . . , 302, 307, . . . , 314, 325, 326, 328, 344, 362</td>
<td>new values</td>
</tr>
</tbody>
</table>
Conclusion & Outlook

- subfield expansion of spreads from larger fields
- computational results for spreads over small fields in non-quadrangle situation
- small spread of size $2^m + 1$ in $\mathbb{F}_2^{4m}$, conjectured to be of minimal size
- also: unextendible triples of MUBs in even and prime ($p \geq 7$) dimension

Further directions

- Use geometry for constructions and proofs.
- Find bounds on the smallest/largest incomplete maximal partial spreads.
- Find spreads such that the corresponding set of MUBs is unextendible.


$p^2 - p + 2$ strongly unextendible MUBs for $d = p^2$, $p \equiv 3 \text{ mod } 4$