ALCOMA 15

Algebraic Combinatorics and Applications

Kloster Banz, March 15–20, 2015

UNIVERSITÄT BAYREUTH

Maximal Partial Symplectic Spreads over Small Fields

Markus Grassl

Markus.Grassl@mpl.mpg.de

www.codetables.de

FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG
NATURWISSENSCHAFTLICHE FAKULTÄT

MAX PLANCK INSTITUTE for the science of light

March 19, 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 $\mathcal{B}^j := \{|\psi_k^j\rangle \colon k = 1, \ldots, d\} \subset \mathbb{C}^d$
- basis states are “mutually unbiased”:

$$|\langle\psi_k^j|\psi_m^l\rangle|^2 = \begin{cases} 1/d & \text{for } j \neq l, \\ \delta_{k,m} & \text{for } j = l. \end{cases}$$

- 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:

$$\mathcal{B} = \mathcal{C}_1 \cup \ldots \cup \mathcal{C}_k, \qquad \text{where } \mathcal{C}_j \cap \mathcal{C}_l = \emptyset \text{ and } |\mathcal{C}_j| = k-1$$

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 $X^{\boldsymbol{\alpha}} Z^{\boldsymbol{\beta}}$ of the generalized Pauli group

Generalized Pauli Group

Error Basis

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

$$\begin{array}{lrcll} & X^\alpha & := & \sum_{x\in\mathbb{F}_q} |x+\alpha\rangle\langle x| & \text{for } \alpha\in\mathbb{F}_q \\ \text{and} & Z^\beta & := & \sum_{z\in\mathbb{F}_q} \omega^{\operatorname{tr}(\beta z)}|z\rangle\langle z| & \text{for } \beta\in\mathbb{F}_q\ (\omega := \omega_p = \exp(2\pi i/p)) \end{array}$$

generalized Pauli Group $\mathcal{P}_n$

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

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

quotient group:

$$\overline{\mathcal{P}}_n := \mathcal{P}_n/\langle\omega I\rangle \cong (\mathbb{F}_q\times\mathbb{F}_q)^n \cong \mathbb{F}_q^n\times\mathbb{F}_q^n$$

Abelian Subgroups & Symplectic Spreads

Abelian subgroup $\mathcal{S}$:

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

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

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

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

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

k MUBs $\Longleftrightarrow$ symplectic spread of size k

Unextendible MUBs from Pauli matrices

[P. Mandayam, S. Bandyopadhyay, M. Grassl, W. K. Wootters, arXiv:1302.3709]

incomplete partitioning of two-qubit Pauli matrices:

$$\mathcal{C}_1 = \{I \otimes X,\ X \otimes I,\ X \otimes X\} \qquad G_i = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{array}\right)$$

$$\mathcal{C}_2 = \{I \otimes Z,\ Z \otimes I,\ Z \otimes Z\} \qquad G_2 = \left(\begin{array}{cc|cc} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right)$$

$$\mathcal{C}_3 = \{X \otimes Z, Z \otimes X, Y \otimes Y\} \qquad G_3 = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right)$$

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 *weakly unextendible* if one cannot add another eigenbasis of those unitary operators.

Unextendible MUBs

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.

$\Longrightarrow$ 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 $S_i = S_i^\star$
- 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:

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

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 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 $\mathbb{F}_{q^n}^2$ 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:

$$G_\infty = \left(\begin{array}{c|c} 0 & I \end{array}\right) \qquad \text{or} \qquad G_i = \left(\begin{array}{c|c} I & A_i \end{array}\right), \quad A_i = A_i^t \text{ (symmetric)}$$

Proof:

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

Defining Conditions for Symplectic Spreads:

$$S_i + S_j = \mathbb{F}_q^{2n} \iff \det\left(\begin{array}{c|c} I & A_i \\ I & A_j \end{array}\right) \neq 0 \iff \det(A_i - A_j) \neq 0$$
$$\iff (\det(A_i - A_j))^{q-1} = 1$$

Smallest Maximal Partial Spread

[M. Cimráková, S. De Winter, V. Fack, and L. Storme, 2007]

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: $G_\infty = \left(\begin{array}{cc|cc} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right)$ and $G_\alpha = \left(\begin{array}{cc|cc} 1 & 0 & 0 & \alpha \\ 0 & 1 & \alpha & 0 \end{array}\right)$, $\alpha \in \mathbb{F}_q$

additional generator $G' = \left(\begin{array}{cc|cc} 1 & 0 & x_{00} & x_{01} \\ 0 & 1 & x_{01} & x_{11} \end{array}\right)$

condition: $\det \begin{pmatrix} x_{00} & x_{01} - \alpha \\ x_{01} - \alpha & x_{11} \end{pmatrix} = x_{00}x_{11} + x_{01}^2 + \alpha^2 \neq 0$ 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 $\Gamma \in \mathbb{F}_q^{m\times m}$ be a symmetric matrix corresponding to a primitive element γ of $\mathbb{F}_{q^m}$.

expansion of the generators:

$$G_\infty = \left(\begin{array}{cc|cc} 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{array}\right), \quad G_0 = \left(\begin{array}{cc|cc} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \end{array}\right), \quad \text{and}$$

$$G_{\gamma^j} = \left(\begin{array}{cc|cc} I & 0 & 0 & \Gamma^j \\ 0 & I & \Gamma^j & 0 \end{array}\right), \quad j = 0, \ldots, q^m - 2$$

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

$$A(\alpha) = \left(\begin{array}{cccc|cccc} & & & & \alpha & & & \\ & & & & & \alpha^q & & \\ & & & & & & \ddots & \\ & & & & & & & \alpha^{q^{m-1}} \\ \hline \alpha & & & & & & & \\ & \alpha^q & & & & & & \\ & & \ddots & & & & & \\ & & & \alpha^{q^{m-1}} & & & & \end{array}\right), \quad \alpha = \gamma^j$$

Small Maximal Partial Spreads (cont.)

additional generator

$G' = \left(\begin{array}{c|c} I & X \end{array} \right)$, where X is a symmetric $2m \times 2m$ matrix

conditions

$\det X \neq 0$ and $\det\left(X - \begin{pmatrix} 0 & \Gamma^j \\ \Gamma^j & 0 \end{pmatrix} \right) \neq 0$ for $j = 0, \ldots, q-2$

$\iff \det\bigl(\tilde{X} - A(\alpha)\bigr) \neq 0$ for $\alpha \in \mathbb{F}_{q^m}$

$\iff \Bigl(\det\bigl(\tilde{X} - A(\alpha)\bigr)\Bigr)^{q-1} = 1$ for $\alpha \in \mathbb{F}_{q^m}$

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

$$\sum_{\alpha \in \mathbb{F}_{q^m}} \Bigl(\det\bigl(\tilde{X} - A(\alpha)\bigr)\Bigr)^{q-1} = 1.$$

$\Longrightarrow$ The expanded spread over the subfield is maximal.

Construction $\mathbb{I}$: 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.

$\Longrightarrow$ Find criteria to decide when the expansion remains to be maximal.

Construction II: Extension

Given generators

$$G_\infty = \left(\begin{array}{c|c} 0 & I \end{array}\right), \quad \text{and} \quad G_i = \left(\begin{array}{c|c} I & A_i \end{array}\right)$$

find a symmetric matrix X with

$$\det(X - A_i) \neq 0 \Longleftrightarrow (\det(X - A_i))^{q-1} = 1$$

$\Longrightarrow$ system of polynomial equations for the symmetric matrix X

$\Longrightarrow$ compute Gröbner basis

$\Longrightarrow$ proves maximality or provides candidates for extension

Exhaustive & Heuristic Search

exhaustive search

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

heuristic search

- start with a spread $\mathcal{S} = \{S_\infty, S_1, \ldots, S_m\}$
- pick a symmetric matrix A such that $S' \notin \mathcal{S}$, S' the row span of $\left(\begin{array}{c|c} I & A \end{array} \right)$
- keep those $S_i \in \mathcal{S}$ that intersect trivially with S'
- compute maximal extension of this partial spread

Computational Results

q^n	q	n	size	remark
4	2	2	$3, 5$	complete
8	2	3	$5, 9$	complete
16	2	4	$5, 8, 9, 11, 13, 17$	complete
16	4	2	$5, 9, 11, 13, 17$	complete
32	2	5	$9, \ldots, 15, 17, 33$	
64	2	6	$9, 13, \ldots, 47, 49, 51, 57, 65$	
64	4	3	$17, \ldots, 43, 49, 65$	
64	8	2	$9, 17, 21, \ldots, 47, 49, 51, 57, 65$	
128	2	7	$21, \ldots, 31, 33, 35, 37, 39, 45, 49, 53, 57, 61, 65, 129$	
256	2	8	$17, 28, \ldots, 205, 209, 211, 213, 214, 215, 225, 227, 241, 257$	
256	4	4	$17, 33, 35, \ldots, 205, 209, 211, 213, 214, 215, 225, 227, 241, 257$	
256	16	2	$17, 33, 46, \ldots, 205, 209, 211, 213, 214, 215, 225, 227, 241, 257$	new values

Computational Results (cont.)

q^n	q	n	size	remark
9	3	2	$5, 8, 10$	complete
27	3	3	$10, \ldots, 20, 28$	complete
81	3	4	$18, \ldots, 68, 70, 73, 74, 82$	
81	9	2	$22, \ldots, 68, 70, 73, 74, 82$	
243	3	5	$32, \ldots, 120, 123, 154, 163, 244$	
25	5	2	$13, \ldots, 20, 22, 24, 26$	complete
125	5	3	$27, \ldots, 90, 101, 126$	
49	7	2	$14, 17, \ldots, 42, 44, 48, 50$	
121	11	2	$28, \ldots, 106, 109, 110, 112, 120, 122$	new values
169	13	2	$40, \ldots, 140, 145, 146, 148, 158, 170$	new values
289	17	2	$67, \ldots, 238, 241, \ldots, 248, 257, 258, 260, 274, 290$	new values
361	19	2	$82, \ldots, 302, 307, \ldots, 314, 325, 326, 328, 344, 362$	new values

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

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.
  $\Longrightarrow$ [András Szántó, arXiv:1502.05245] using matrix algebras:
  $p^2 - p + 2$ strongly unextendible MUBs for $d = p^2$, $p \equiv 3 \bmod 4$