Problems on spherical codes motivated by quantum information theory

William J. Martin

Department of Mathematical Sciences
and
Department of Computer Science
Worcester Polytechnic Institute

Workshop on Coding and Information Theory
Center of Mathematical Sciences and Applications
April 12, 2018
Mutually Unbiased Bases (MUBs)

We seek orthonormal bases $\mathcal{B}_1, \ldots, \mathcal{B}_k$ in $\mathbb{R}^d$ or $\mathbb{C}^d$ (that is, 

$$\langle b, b' \rangle = \begin{cases} 
1 & \text{if } b = b'; \\
0 & \text{if } b \neq b'. 
\end{cases}$$

for $b$ and $b'$ in the same basis)

such that

$$|\langle b, b' \rangle| = 1/\sqrt{d}$$

for vectors $b \in \mathcal{B}_i$ and $b' \in \mathcal{B}_j$ when $i \neq j$. 

William J. Martin  
Quantum Information Theory
Independent Quantum Measurements (Schwinger, ’60)

- We assume here von Neumann measurements of a $d$-state quantum system
- Each measurement is an orthonormal basis
- A pair of measurements $\mathcal{B}$ and $\mathcal{B}'$ are independent (or unbiased relative to one another) if, for each $b' \in \mathcal{B}'$, the coefficients $\alpha_j$ in
  \[
  b' = \sum_{b_j \in \mathcal{B}} \alpha_j b_j
  \]
  all have the same absolute value: $|\alpha_j| = d^{-1/2}$
- For applications such as quantum state tomography [Ivanović, ’81; Wootters & Fields, ’89] and quantum cryptography [Bennett & Brassard, ’84], we want the maximum possible number $k$ of pairwise (“mutually”) unbiased bases $\mathcal{B}_1, \ldots, \mathcal{B}_k$.
- We say we have $k$ MUBs in dimension $d$
There can be at most $d + 1$ MUBs in $\mathbb{C}^d$

Rather than LP bound [Delsarte, Goethals & Seidel ’75], let’s use [Szántó, ’16]:

- **Maximal Abelian subalgebra**: all matrices with $B_j$ as an eigenbasis denoted by $A_j$
- $A_j \cap A_\ell = \langle I \rangle$
- Under Hilbert-Schmidt inner product $\langle M, N \rangle = \text{Tr}(M^\dagger N)$, elements of $A_j$ orthogonal to $I$ are orthogonal to elements of $A_\ell$ orthogonal to $I$
- packing orthogonal $(d - 1)$-subspaces into a $d^2 - 1$ dimensional space of matrices, so $k \leq d + 1$
Build $d + 1$ MUBs in $\mathbb{C}^d$ when $d = q^m$, a prime power

People have used Weil sums, planar functions [Klappenecker & Roetteler '03] [Roy & Scott, '07] [Godsil & Roy '09]
I learned this from Bill Kantor.

Entries will be indexed by elements of $V = \mathbb{F}_q^m$.
A function $\varphi : V \to \mathbb{F}$ is bent if for each nonzero $u \in V$, the function $\psi : v \mapsto \varphi(u + v) - \varphi(v)$ evenly covers $\mathbb{F}$.

$$|\psi^{-1}(a)| = q^{m-1} \quad (a \in \mathbb{F}).$$
Build $d + 1$ MUBs in $\mathbb{C}^d$ when $d = q^m$, a prime power

**Hypothesis:** We suppose that $S$ is a set of functions $V \rightarrow \mathbb{F}$, including the zero function, such that the difference of any two is bent.

Let $\zeta$ be a primitive $q^{th}$ root of unity in $\mathbb{C}$.

Equip $\mathbb{C}^d$ with its usual Hermitian inner product $(\cdot, \cdot)$. Write the standard basis for $\mathbb{C}^d$ as $\{e_v | v \in V\}$.

Let $\mathcal{F}_\infty = \{\langle e_v \rangle | v \in V\}$.

For $f \in S$, let

$$\mathcal{F}_f = \left\{ \langle \sum_{v \in V} \zeta^{a \cdot v + f(v)} e_v \rangle | a \in V \right\}.$$ 

and let

$$\mathbb{F}^S = \{\mathcal{F}_f : f \in S\} \cup \{\mathcal{F}_\infty\}.$$ 

**Theorem:** $\mathbb{F}^S$ is a set of MUBs in $\mathbb{C}^d$. 
Best Known Sets For Other Dimensions

Very little is known.

- For $d = 6$, can we achieve $k \geq 4$?
- For $d = p_1^{r_1} \cdots p_s^{r_s}$, above construction, with tensor products gives
  \[ k \geq 1 + \min \{ p_1^{r_1}, \ldots, p_s^{r_s} \} \]
- Goal: $k = \Omega(n)$
Real MUBs: Linear Programming Bound

**Theorem** [Delsarte, Goethals & Seidel, '75]: At most \( \frac{d}{2} + 1 \) mutually unbiased bases in \( \mathbb{R}^d \).

Linear programming on finite sets in projective space using Jacobi polynomials.
View each basis as an orthoplex, with two unit vectors per line.

- Allowable inner products \( \{ \pm 1, \pm \frac{1}{\sqrt{d}}, 0 \} \)
- Regardless of structure (imprimitivity), we can have at most \( d(d + 2)/2 \) lines with these angles
Q-Polynomial (Co-Metric) Association Schemes

Here we apply polynomials entrywise to a Gram matrix, e.g.

\[ G = [g_{ij}]_{i,j} \implies G^2 = [g_{ij}^2]_{i,j} \]

\(X\) a spherical code with \(s + 1\) inner products, Gram matrix \(G\).

**Defn:** \(X\) is an \(s\)-class \(Q\)-polynomial association scheme if the vector space

\[ \text{span}\{G^0 = J, G^1 = G, G^2, \ldots, G^s\} \]

is closed under matrix multiplication.

An association scheme is *imprimitive* if this matrix algebra contains

\[ J \oplus J \oplus \cdots \oplus J \]

**Thm** [LeCompte, WJM, Owens, ’10] Every set of real mutually unbiased bases yields a 4-class \(Q\)-polynomial association scheme with two imprimitivity systems ("Q-bipartite" and "Q-antipodal").
Real MUBs are Association Schemes

\( X \) a spherical code with \( s + 1 \) inner products, Gram matrix \( G \).

**Defn:** \( X \) is an \( s \)-class \( Q \)-polynomial association scheme if the vector space

\[
\text{span} \left\{ G^0 = J, G^1 = G, G^2, \ldots, G^s \right\}
\]

is closed under matrix multiplication.

**Thm** [LeCompte, WJM, Owens, ’10] Every set of real mutually unbiased bases yields a 4-class \( Q \)-polynomial association scheme with two imprimitivity systems (“\( Q \)-bipartite” and “\( Q \)-antipodal”). Conversely, every 4-class \( Q \)-polynomial association scheme with two imprimitivity systems arises from a set of \( k \) MUBs.
Kerdock Codes: only known way to reach $\frac{d}{2} + 1$ MUBs

View binary vectors as $\pm 1$-vectors in $\mathbb{R}^d$.

- Here $d = 4^m$. First-order Reed-Muller code has $2d$ codewords with inner products $\pm d$ and zero.
- Piece together $d$ cosets — all contained in the second-order Reed-Muller code — so that inner products between cosets are all $\pm 2^m$.
- This Kerdock code gives $\frac{d}{2} + 1$ orthoplexes, which can be viewed as mutually unbiased bases.

\[
\begin{array}{c|cccc}
  i & 0 & 2^{2m-1} \mp 2^{m-1} & 2^{2m-1} & 2^{2m} \\
  \hline
  A_i & 1 & 2^m(2^{2m-1} - 1) & 2^{2m+1} - 2 & 1
\end{array}
\]
Best Known Sets for Other Dimensions

Two mutually unbiased bases in $\mathbb{R}^d$: equivalent to existence of a Hadamard matrix.

In order to have $k \geq 3$ real MUBs, we require $d = 4t^2$ for some $t$.

<table>
<thead>
<tr>
<th>$t$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$d$</td>
<td>4</td>
<td>16</td>
<td>36</td>
<td>64</td>
<td>100</td>
<td>144</td>
</tr>
<tr>
<td>$k$</td>
<td>3</td>
<td>9</td>
<td>3</td>
<td>33</td>
<td>2-3</td>
<td>7-73</td>
</tr>
</tbody>
</table>
**Linked Simplices**

**Defn:** Two full-dimensional simplices in $\mathbb{R}^d$ are *linked* if inner products between vectors in distinct simplices take on just two values:

$$\langle b, b' \rangle \in \{\xi, \zeta\}$$

**Q:** What is the maximum number of pairwise linked simplices in $\mathbb{R}^d$? (E.g., the cube gives two in $\mathbb{R}^3$.)

**Theorem** [Kodalen ’17]: Linked simplices are equivalent to linked systems of symmetric designs [Cameron ’74]

Kodalen shows how to build sets of mutually unbiased bases and sets of equiangular lines from linked simplices.
Equiangular Lines

- How many lines can we form through the origin in $\mathbb{R}^d$ or $\mathbb{C}^d$ such that the angle between any two lines is the same? (Unit vectors spanning the lines have inner product with constant modulus.)
- Icosahedron: six lines in $\mathbb{R}^3$
- Jaap Seidel’s thesis in 1948 touched on this question [Haantjes '48]
Bound for Real Equiangular Lines

[Lemmens & Seidel ’73] Attribute to Gerzon:

\[ |X| \leq \frac{d(d + 1)}{2} \]

Achieved seldom:

- \( d = 2 \) hexagon
- \( d = 3 \) icosahedron
- \( d = 7 \) let \( S_8 \) act on \((-3, -3, 1, 1, 1, 1, 1, 1)\) to obtain 28 vectors in codimension one
- \( d = 23 \) two-graph attached to Conway sporadic finite simple group gives 276 lines

If achieved again, then \( d + 2 \) must be odd square. Open: \( d = 79 \).
Peter Neumann proved that the cosine must be \( 1/n \) for some odd integer \( n \) when \( |X| > 2d \).
deCaen’s Construction

For $d = 3 \cdot 2^{2t-1} - 1$, [de Caen ’00] finds $k = \frac{2}{9}(d + 1)^2$ equiangular lines in $\mathbb{R}^d$.

His Gram matrix is selected from the association of the Kerdock code!
Connections: Two-Graphs and Frames

Real equiangular lines are connected to:

- regular two-graphs (Graham Higman, Donald Taylor)
- equiangular tight frames ("ETFs")
Complex Equiangular Lines (SIC-POVMs)

Let $N(d)$ denote the max size of a set of equiangular lines in $\mathbb{C}^d$.

**Theorem** [Delsarte, Goethals, Seidel '78]

$$N(d) \leq d^2$$

Here are the general techniques to obtain exactly $d^2$ lines in $\mathbb{C}^d$:

- [S. Hoggar '81, '98]: 64 lines in $\mathbb{C}^8$ from a 4-dimensional quaternionic polytope
- [Jedwab & Wiebe '14]: Elegant solutions in dimensions $d = 2, 3, 8$ from Hadamard matrices
- Various authors: “Zauner method”
Some Nice Constructions of Less Than $d^2$ Lines

- [König '95, '99]: Characters of abelian groups restricted to $(\nu, k, 1)$-difference sets (rediscovered several times)
- [Godsil & Roy '12]: line systems from relative difference sets
- [Greaves, et al. '14]/[Jedwab & Wiebe '14]: equiangular lines from MUBs
- equiangular tight frame constructions
Sets of Quadratic Size

Recall that the upper bound is $N(d) \leq d^2$

- The König construction gives
  \[ N(d) \geq d^2 - d + 1 \]
  for $d = p^r + 1$ ($p$ prime)

- Converting MUBs to equiangular lines (Greaves, et al., Jedwab & Wiebe) gives
  \[ N(d) = \Theta(d^2) \]
  for many other dimensions $d$. 
Equiangular Lines from Difference Sets

Let $G$ be a finite abelian group. A *character* of $G$ is a group homomorphism

$$\chi : G \rightarrow \mathbb{C}^*$$

**Example:** For $G = \mathbb{Z}_7$ we have seven distinct characters, $\chi_a$ ($0 \leq a < 7$) given by

$$\chi_a(b) = \omega^{ab}$$

where $\omega$ is any primitive complex $7^{th}$ root of unity.

The quadratic residues in $\mathbb{Z}_7$ form a difference set $D = \{1, 2, 4\}$:

$1-2 = 6$, $1-4 = 4$, $2-1 = 1$, $2-4-5$, $4-1 = 3$, $4-2 = 2$. 
Lines from Difference sets

The quadratic residues in \( \mathbb{Z}_7 \) form a difference set \( D = \{1, 2, 4\} \) with parameters \( (7, 3, 1) \).

The corresponding characters \( \chi_1, \chi_2, \chi_4 \) give us 7 vectors by arranging them in a \( 3 \times 7 \) array and transposing:

\[
\begin{align*}
\chi_1 &= [1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6] \\
\chi_2 &= [1, \omega^2, \omega^4, \omega^6, \omega, \omega^3, \omega^5] \\
\chi_4 &= [1, \omega^4, \omega, \omega^5, \omega^2, \omega^6, \omega^3]
\end{align*}
\]

With \( \omega = e^{2\pi i/7} \), we have

\[
X = \{(1, 1, 1), (\omega, \omega^2, \omega^4), (\omega^2, \omega^4, \omega), (\omega^3, \omega^6, \omega^5), \\
(\omega^4, \omega, \omega^2), (\omega^5, \omega^3, \omega^6), (\omega^6, \omega^5, \omega^3)\}
\]

which span 7 equiangular lines.
Lines from Difference sets

The quadratic residues in $\mathbb{Z}_7$ form a difference set $D = \{1, 2, 4\}$ with parameters $(7, 3, 1)$.

The corresponding characters $\chi_1, \chi_2, \chi_4$ give us 7 vectors by arranging them in a $3 \times 7$ array and transposing:

With $\omega = e^{2\pi i/7}$

\[
\begin{align*}
\chi_1 &= [1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6], \\
\chi_2 &= [1, \omega^2, \omega^4, \omega^6, \omega, \omega^3, \omega^5], \\
\chi_4 &= [1, \omega^4, \omega, \omega^5, \omega^2, \omega^6, \omega^3]
\end{align*}
\]

This gives us a configuration of 7 vectors in $\mathbb{C}^3$

\[
X = \{(1, 1, 1), (\omega, \omega^2, \omega^4), (\omega^2, \omega^4, \omega), (\omega^3, \omega^6, \omega^5), \ldots\}
\]

which span 7 equiangular lines.
Lines from Difference sets

The quadratic residues in \( \mathbb{Z}_7 \) form a difference set \( D = \{1, 2, 4\} \) with parameters \((7, 3, 1)\).

The corresponding characters \( \chi_1, \chi_2, \chi_4 \) give us 7 vectors by arranging them in a \( 3 \times 7 \) array and transposing:

\[
\begin{align*}
\chi_1 &= \begin{bmatrix} 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 \end{bmatrix} \\
\chi_2 &= \begin{bmatrix} 1 & \omega^2 & \omega^4 & \omega^6 & \omega & \omega^3 & \omega^5 \end{bmatrix} \\
\chi_4 &= \begin{bmatrix} 1 & \omega^4 & \omega & \omega^5 & \omega^2 & \omega^6 & \omega^3 \end{bmatrix}
\end{align*}
\]

With \( \omega = e^{2\pi i/7} \), this gives us a configuration of 7 vectors in \( \mathbb{C}^3 \):

\[
X = \{(1, 1, 1), (\omega, \omega^2, \omega^4), (\omega^2, \omega^4, \omega), (\omega^3, \omega^6, \omega^5), (\omega^4, \omega, \omega^2), (\omega^5, \omega^3, \omega^6), (\omega^6, \omega^5, \omega^3)\}
\]

which span 7 equiangular lines.
**Zauner’s Conjecture**

**Conjecture** (G. Zauner, 1999) SIC-POVMs exist in all dimensions $d$. Moreover, in each dimension $d$, there is a “fiducial” vector (a common eigenvector of all operators in some specific abelian subgroup of the Heisenberg-Weyl group) whose orbit under the Heisenberg-Weyl group has size $d^2$ and forms a SIC-POVM.
Zauner’s Conjecture

From a computational viewpoint, the conjecture seems to work!

“Numerical” examples of SIC-POVMs have been found to high precision in dimensions 2–151 inclusive; also 168, 172, 195, 199, 228, 259, 323, 844, 1299, 2208.

Exact analytic solutions have been found (mostly by Gröbner basis techniques) in dimensions 2–21 inclusive; also 24, 28, 30, 31, 35, 37, 39, 43, 48, 120, 124, 323.

So what’s holding us up?
Zauner’s Conjecture

Grassl and Scott [’09] summarize the then-known solutions in a 16-page paper (with a 206-page supplement).

10a

```
+.22518226652570929642141251166452065139e+0+.00000000000000000000000000000000e+0i
+.21281603496476162944277495061557615214e+0-.40237284916732874563473284735309371005e+0i
-.21720278822783363199467134228877846622e+0-.18622981416764427112589459112712078191e+0i
-.51186787757437419182346233108536956517e+0-.20193083833839869879387871188726235885e+0i
+.22442550671357785217047122140058220692e+0+.89342732314492811955925446460812908910e-1i
-.57441100401303718997024481250379823169e-1+.43602390662541867781420316780629349457e-1i
-.3751184613293444963656039170690317437e+0+.38737288942425228592216149700713646394e-2i
+.23853605695729570773167018546354663503e+0+.24876881139569911111619017146256733837e+0i
-.12452009916996958884871674848680344535e+0-.45778017329246117075131294765879160859e-1i
-.1183323937374801892958514297444494320e+0-.52798999543319862645855198551278721702e-1i
```

Fiducial vector for numerical example in $\mathbb{C}^{10}$. 
Zauner’s Conjecture

Second part of Grassl-Scott supplement gives exact solutions.

Fiducial vector for analytic example in $\mathbb{C}^{10}$ requires some preliminary definitions of constants.
Zauner’s Conjecture

Second part of Grassl-Scott supplement gives exact solutions.

Here is the \textbf{first entry} of the fiducial vector for the example in $\mathbb{C}^{10}$.

An exact fiducial vector can take up over a 1000 pages!
The Whole Talk in One Slide

Thank you for listening!

- Find, as many as you can, equiangular lines in $\mathbb{C}^d$ (unit vectors whose inner products have constant modulus). Find $d^2$, if possible.
- Find, as many as you can, equiangular lines in $\mathbb{R}^d$ (unit vectors whose inner products have constant absolute value). Find $\binom{d+1}{2}$, if possible.
- Find, as many as you can, orthonormal bases in $\mathbb{C}^d$ where unit vectors from distinct bases have inner products with constant modulus. Find $d + 1$, if possible.
- Find, as many as you can, orthonormal bases in $\mathbb{R}^d$ where unit vectors from distinct bases have inner products with constant absolute value. Find $\frac{d}{2} + 1$, if possible.