

---

Magma 2006

Technische Universität Berlin

July 30 – August 2, 2006

---

**M A G M A**  
C O M P U T E R • A L G E B R A

# Finding Equiangular Lines in Complex Space

Markus Grassl

31.07.2006



Institut für Algorithmen und Kognitive Systeme  
Fakultät für Informatik, Universität Karlsruhe (TH)  
Germany

# Overview

- The problem
- Some background
- Weyl-Heisenberg and Jacobi Groups
- Finding some solutions
- Modular computations

# The Problem: Equiangular Lines in Complex Space

## The General Problem

Find  $m$  normalized vectors  $\{\mathbf{v}_1, \dots, \mathbf{v}_m\} \subset \mathbb{C}^d$  such that the modulus of the inner product between any pair of vectors is constant, i. e.

$$|\langle \mathbf{v}_i | \mathbf{v}_j \rangle|^2 = \begin{cases} 1 & \text{for } i = j, \\ c & \text{for } i \neq j \end{cases}$$

## Special Case

Find  $d^2$  normalized vectors  $\{\mathbf{v}_1, \dots, \mathbf{v}_{d^2}\} \subset \mathbb{C}^d$  such that the modulus of the inner product between any pair of vectors is constant, i. e.

$$|\langle \mathbf{v}_i | \mathbf{v}_j \rangle|^2 = \begin{cases} 1 & \text{for } i = j, \\ 1/(d+1) & \text{for } i \neq j \end{cases}$$

## Some Background (I)

### Complex Spherical 2-Designs

The integral of any degree-two polynomial over the complex sphere in  $\mathbb{C}^d$  can be computed as finite average, i. e.

$$\frac{1}{\mu(\mathbb{C}S^{d-1})} \int_{g \in \mathbb{C}S^{d-1}} f(g) d\mu(g) = \frac{1}{m} \sum_{i=1}^m f(\mathbf{v}_i)$$

if  $m = d^2$  and the vectors  $\mathbf{v}_i$  are equiangular lines.

### Banach Spaces [König & Tomczak-Jaegermann 94]

The projection constant

$$\lambda(E) = \sup_{X \supseteq E} \inf_P \{ \|P\| : P: X \rightarrow E \text{ is linear projection onto } E \}$$

of a complex  $d$ -dimensional normed space  $E$  is maximal iff a set of  $d^2$  equiangular lines exists.

## Some Background (II)

### Quantum Information: SIC-POVMs

- generalized quantum measurement (POVM) with  $d^2$  rank-one elements  
 $E_j = \Pi_j/d$  with  $\Pi_j = |\phi_j\rangle\langle\phi_j|$
- The  $d^2$  elements form a basis of  $\mathbb{C}^{d \times d}$ .  
 $\implies$  “informationally complete”, i.e., reconstruction of a quantum state  $\rho$  is possible
- expectation values  $p_j = \text{tr}(\rho E_j)$  “maximally independent”:

$$\text{tr}(\Pi_j \Pi_k) = |\langle\phi_j|\phi_k\rangle|^2 = \frac{1}{d+1} \quad \text{for } j \neq k,$$

$\implies$  “symmetric”

- applications in quantum cryptography as well

# Weyl-Heisenberg Group

- Generators:  $H_d := \langle X, Z \rangle$

where  $X := \sum_{j=0}^{d-1} |j+1\rangle \langle j|$  and  $Z := \sum_{j=0}^{d-1} \omega_d^j |j\rangle \langle j|$

$$(\omega_d := \exp(2\pi i/d))$$

- Relations:

$$(\omega_d^c X^a Z^b) (\omega_d^{c'} X^{a'} Z^{b'}) = \omega_d^{a'b - b'a} (\omega_d^{c'} X^{a'} Z^{b'}) (\omega_d^c X^a Z^b)$$

- Basis:

$$H_d / \zeta(H_d) = \{X^a Z^b : a, b \in \{0, \dots, d-1\}\} \cong \mathbb{Z}_d \times \mathbb{Z}_d$$

trace-orthogonal basis of all  $d \times d$  matrices

# Jacobi Group (or Clifford Group)

- automorphism group of the Heisenberg group  $H_d$ , i.e.

$$\forall T \in J_d : T^\dagger H_d T = H_d$$

- the action of  $J_d$  on  $H_d$  modulo phases corresponds to the symplectic group  $SL(2, \mathbb{Z}_d)$ , i.e.

$$T^\dagger X^a Z^b T = \omega_d^c X^{a'} Z^{b'} \quad \text{where} \quad \begin{pmatrix} a' \\ b' \end{pmatrix} = \tilde{T} \begin{pmatrix} a \\ b \end{pmatrix}, \quad \tilde{T} \in SL(2, \mathbb{Z}_d)$$

$\implies$  homomorphism  $J_d \rightarrow SL(2, \mathbb{Z}_d)$

- $J_d$  is generated by the discrete Fourier transform and a diagonal matrix “with quadratic phases” (depends on  $d$  odd or even)

# Zauner's Conjecture

[G. Zauner, Dissertation, Universität Wien, 1999]

## Conjecture:

For every dimension  $d \geq 2$  there exists a SIC-POVM whose elements are the orbit of a rank-one operator  $E_0$  under the Heisenberg group  $H_d$ .

What is more,  $E_0$  commutes with an element  $T$  of the Jacobi group  $J_d$ .

The action of  $T$  on  $H_d$  modulo the center has order three.

support for this conjecture:

- algebraic solutions by [Zauner 99, Appleby 05] for  $d = 2, 3, 4, 5, 7, 19$  (only prime powers)
- numerical evidence by [Renes et al. 04] for  $d \leq 45$
- our algebraic solutions for  $d = 6, 8, 9, 10, 11, 12, 13, 15$  [Grassl 04–06]

# Constructing SIC-POVMs

## Ansatz 1:

SIC-POVM that is the orbit under  $H_d$ , i.e.,

$$|\phi_{a,b}\rangle := X^a Z^b |\phi_0\rangle$$

$$|\langle \phi_{a,b} | \phi_{a',b'} \rangle|^2 = \begin{cases} 1 & \text{for } (a,b) = (a',b'), \\ 1/(d+1) & \text{for } (a,b) \neq (a',b') \end{cases}$$

$$|\phi_0\rangle = \sum_{j=0}^{d-1} (x_{2j} + ix_{2j+1}) |j\rangle,$$

( $x_0, \dots, x_{2d-1}$  are real variables,  $x_1 = 0$ )

$\implies$  polynomial equations for  $2d - 1$  variables, but already too complicated for  $d = 6$

## Constructing SIC-POVMs (cntd.)

### Ansatz 2:

SIC-POVM that is the orbit under  $H_d$ ,

additionally:

$|\phi_0\rangle$  lies in a (degenerate)  $\ell$ -dimensional eigenspace of some  $T \in J_d$

$$|\phi_0\rangle = \sum_{j=0}^{\ell-1} (x_{2j} + ix_{2j+1}) |b_j\rangle,$$

where  $|b_j\rangle$ ,  $j = 1, \dots, \ell$  is the basis of that eigenspace

$\implies$  reduced number of variables

$\implies$  better chances to compute algebraic solutions

## Strategy Supported by MAGMA

1. Find a suitable non-trivial automorphism  $T \in J_d$  with a small eigenspace.
  - use the homomorphism  $J_d \rightarrow SL(2, \mathbb{Z}_d)$
  - use the conjugacy classes of  $SL(2, \mathbb{Z}_d)$
2. Construct the system of polynomial equations.
3. Try to solve the resulting system of polynomial equations.
4. Construct number field which contains some solutions.
5. Find a real subfield.
6. Compute automorphisms of solutions.

**Example:  $d = 6$** 

here:  $d = 6$ ,  $\ell = 3$ , i.e., only 5 variables

⇒ algebraic solutions computed using MAGMA

- 144 complex solutions for the real variables  
⇒ only the real solutions are valid
- in total 96 “different” such SIC-POVMs, but all these SIC-POVMs are related by complex conjugation or a global basis change

## Example: $d = 12$

solutions in number field  $\mathbb{Q}(\sqrt{2}, \sqrt{13}, \theta_1, \theta_2, i, \omega_3)$  of degree 64 generated by

$$\theta_1 := \sqrt{\sqrt{13} - 1}, \quad \theta_2 := \sqrt{\sqrt{13} + 3}, \quad i^2 = -1, \quad \omega_3 := \exp 2\pi i/3$$

Coordinates of the (not normalized) initial vector  $|\psi_{12}\rangle = \sum_{i=1}^{12} v_i |i\rangle$

$$v_1 = 16$$

$$v_2 = \left( ((\sqrt{26} + \sqrt{2} - \sqrt{13} - 1)\theta_1 + (\sqrt{26} - 5\sqrt{2} - 2\sqrt{13} + 10))\theta_2 \right. \\ \left. + ((-\sqrt{26} - 3\sqrt{2} + 2\sqrt{13} + 6)\theta_1 + (4\sqrt{2} - 4)) \right) i \\ + ((-\sqrt{13} - 1)\theta_1 + (\sqrt{26} - 5\sqrt{2}))\theta_2 + (\sqrt{26} + 3\sqrt{2})\theta_1 + 4$$

$$v_3 = ((4\sqrt{2} - 8)\theta_1 - 4\sqrt{26} - 4\sqrt{2} + 4\sqrt{13} + 4)i$$

$$v_4 = (((4\sqrt{2} - 4)\theta_1 - 4\sqrt{2} + 8)\theta_2 + (8\sqrt{2} - 8))i + (-4\theta_1 - 4\sqrt{2})\theta_2 + 8$$

$$\begin{aligned}
v_5 &= (-2\sqrt{26} - 6\sqrt{2})\theta_1 - 8 \\
v_6 &= \left( ((\sqrt{26} - \sqrt{2} - \sqrt{13} + 1)\theta_1 + (2\sqrt{2} - 4))\theta_2 \right. \\
&\quad \left. + ((-2\sqrt{2} + 4)\theta_1 + (2\sqrt{26} + 2\sqrt{2} - 2\sqrt{13} - 2)) \right) i \\
&\quad + ((-\sqrt{13} + 1)\theta_1 + 2\sqrt{2})\theta_2 + 2\sqrt{2}\theta_1 + 2\sqrt{13} + 2 \\
v_7 &= (16\sqrt{2} - 16)i \\
v_8 &= \left( ((\sqrt{26} + \sqrt{2} - \sqrt{13} - 1)\theta_1 + (\sqrt{26} - 5\sqrt{2} - 2\sqrt{13} + 10))\theta_2 \right. \\
&\quad \left. + ((\sqrt{26} + 3\sqrt{2} - 2\sqrt{13} - 6)\theta_1 - 4\sqrt{2} + 4) \right) i \\
&\quad + ((-\sqrt{13} - 1)\theta_1 + (\sqrt{26} - 5\sqrt{2}))\theta_2 + (-\sqrt{26} - 3\sqrt{2})\theta_1 - 4 \\
v_9 &= -4\sqrt{2}\theta_1 - 4\sqrt{13} - 4 \\
v_{10} &= (((4\sqrt{2} - 4)\theta_1 - 4\sqrt{2} + 8)\theta_2 + (-8\sqrt{2} + 8))i + (-4\theta_1 - 4\sqrt{2})\theta_2 - 8 \\
v_{11} &= ((2\sqrt{26} + 6\sqrt{2} - 4\sqrt{13} - 12)\theta_1 - 8\sqrt{2} + 8)i \\
v_{12} &= \left( ((\sqrt{26} - \sqrt{2} - \sqrt{13} + 1)\theta_1 + (2\sqrt{2} - 4))\theta_2 \right. \\
&\quad \left. + ((2\sqrt{2} - 4)\theta_1 - 2\sqrt{26} - 2\sqrt{2} + 2\sqrt{13} + 2) \right) i \\
&\quad + ((-\sqrt{13} + 1)\theta_1 + 2\sqrt{2})\theta_2 - 2\sqrt{2}\theta_1 - 2\sqrt{13} - 2
\end{aligned}$$

## General Approach

1. Use a suitable symmetry group  $G \subset U(d)$  (abstract error group<sup>a</sup>).
2. Find  $T \in U(d) \setminus G$  with  $G^T = G$  and  $T$  not proportional to identity.
3. Use a generic vector in an eigenspace of  $T$  as fiducial vector

$$|\phi_0\rangle = \sum_{j=0}^{\ell-1} (x_{2j} + ix_{2j+1}) |b_j\rangle.$$

4. The SIC-POVM is the projective orbit under  $G$ , i.e.

$$\{g |\phi_0\rangle \langle \phi_0| g^{-1} : g \in G\}.$$

5. Try to solve the resulting system of polynomial equations over  $\mathbb{R}$ .

---

<sup>a</sup>[[Klappenecker & Rötteler, quant-ph/0010082](#)]

# Modular Computations

## Solving polynomial equations using Gröbner bases

- “standard” Buchberger algorithm over cyclotomic/number field
- additional variable for field extension  
⇒ computations over  $\mathbb{Q}$
- use linear algebra for reduction (F4 in Magma) ⇒ modular techniques

## Reconstructing Gröbner bases [E. Arnold 03]

- compute Gröbner bases mod  $p_i$
- if all primes  $p_i$  are “lucky”, reconstruction is possible

successfully applied for  $d = 10$  with 65 primes, modulus 504 digits, solutions in number field of degree 192

# Some Group Covariant SIC-POVMS

group	$d$	unitary automorphism	number of SIC-POVMS
$H_6$	6	order 3	$48 + 48$
$H_8$	8	order 6	64
$H_9$	9	order 3	$216 + 216$
$H_{10}$	10	order 3	$240 + 240$
$H_{11}$	11	order 3	$440 + 440$
$H_{12}$	12	order 3	384
$H_{13}$	13	order $\geq 3$	not yet computed
$H_{15}$	15	order $\geq 3$	not yet computed
SmallGroup(36, 11)	6	order 3	$24 + 24$
SmallGroup(64, 78)	8	order 1	16

for  $d \geq 10$ , the classification is incomplete