Gröbner bases and cocyclic Hadamard matrices

Álvarez, Armario, Falcón, Frau and Gudiel

University of Seville

5th Workshop on Real and Complex Hadamard Matrices and Applications

Outline

Hadamard cocyclic ideals

Hadamard ideals - Kotsireas, Koukouvinos, Seberry (2006)

Hadamard cocyclic ideals

Hadamard ideals - Kotsireas, Koukouvinos, Seberry (2006)
Polynomial equations $\longleftrightarrow$ Hadamard matrices with 1 and 2-circulant core

Hadamard cocyclic ideals

Hadamard ideals - Kotsireas, Koukouvinos, Seberry (2006)
Polynomial equations $\longleftrightarrow$ Hadamard matrices with 1 and 2-circulant core

G is a group of order $4t$, a *cocycle* ψ over G is a mapping $\psi : G \times G \to \langle -1 \rangle$ satisfying $\psi(1,1) = \psi(g,1) = \psi(1,g) = 1,\ g \in G$ and the cocycle equation:

$$\psi(g_i, g_j)\ \psi(g_i g_j, g_k) \psi(g_i, g_j g_k)\ \psi(g_j, g_k) = 1, \quad g_i, g_j, g_k \in G. \qquad (1)$$

Pros & Cons

Pros

- Faster Hadamard test

Pros & Cons

Pros

- Faster Hadamard test
- Search performed in terms of a basis of cocyles

$$\{\text{coboundaries}\} \cup \{\text{inflation}\} \cup \{\text{transgression}\}$$

Pros & Cons

Pros

- Faster Hadamard test
- Search performed in terms of a basis of cocyles

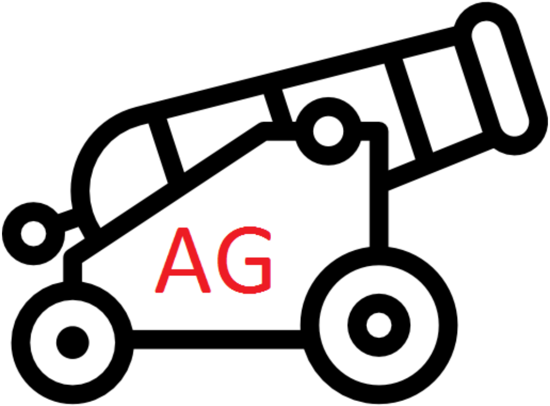
$$\{\text{coboundaries}\} \cup \{\text{inflation}\} \cup \{\text{transgression}\}$$

Cons

- $\{$ Cocyclic Hadamard Matrices $\} \subset \{$ Hadamard Matrices $\}$

The idea

Use the Algebraic Geometry artillery (namely Gröbner basis techniques) to determine both the cardinality and the elements of the set $\mathcal{H}_G$ of cocyclic Hadamard matrices over a multiplicative finite group G of $4t$ elements.



First (naive) approach

$\mathbb{Q}[X_G]$ be the polynomial ring over $\{X_G\} = \{x_{i,j} \colon\ g_i, g_j \in G\}$

First (naive) approach

$\mathbb{Q}[X_G]$ be the polynomial ring over $\{X_G\} = \{x_{i,j} \colon \ g_i, g_j \in G\}$

Theorem

The set $\mathcal{H}_G$ can be identified with the set of zeros of the zero-dimensional ideal $I_G = I_G^1 + I_G^2 + I_G^3 + I_G^4 \subset \mathbb{Q}[X_G]$, where

$$\begin{cases} I_G^1 = \langle\, x_{i,j}^2 - 1 \colon \ i,j \in G \,\rangle \\ I_G^2 = \langle\, x_{i,j}x_{ij,k} - x_{j,k}x_{i,jk} \colon \ i,j,k \in G \,\rangle \\ I_G^3 = \langle\, x_{1,j} - 1, x_{i,1} - 1 \colon \ i,j \in G \setminus \{1\} \,\rangle \\ I_G^4 = \langle\, \sum_{j \in G} x_{i,j} \colon \ i \in G \setminus \{1\} \,\rangle \end{cases}$$

Complexity

Set of polynomials defining I_G:

$$O(t^3) \text{ polynomials of degree up to 2 over } O(t^2) \text{ variables}$$

Complexity

Set of polynomials defining I_G:

$$O(t^3) \text{ polynomials of degree up to 2 over } O(t^2) \text{ variables}$$

Lakshman and Lazard (1991) $\longrightarrow 2^{O(t^2)}$!!

Complexity

Set of polynomials defining I_G:

$$O(t^3) \text{ polynomials of degree up to 2 over } O(t^2) \text{ variables}$$

Lakshman and Lazard (1991) $\longrightarrow 2^{O(t^2)}$!!

Open computer algebra system for polynomial computations SINGULAR
`CocGM`(t, G, opt)

Complexity

Set of polynomials defining I_G:

$$O(t^3) \text{ polynomials of degree up to 2 over } O(t^2) \text{ variables}$$

Lakshman and Lazard (1991) $\longrightarrow 2^{O(t^2)}$!!

Open computer algebra system for polynomial computations SINGULAR
`CocGM(`t, G, opt`)`
http://personales.us.es/raufalgan/LS/hadamard.lib

$$\begin{cases} G = 1 \Rightarrow \mathbb{Z}_t \times \mathbb{Z}_2^2, G = 2 \Rightarrow D_{4t} \\ opt = 1 \Rightarrow \sharp\mathcal{H}_G, opt = 2 \Rightarrow \mathcal{H}_G \end{cases}$$

Complexity

Set of polynomials defining I_G:

$$O(t^3) \text{ polynomials of degree up to 2 over } O(t^2) \text{ variables}$$

Lakshman and Lazard (1991) $\longrightarrow 2^{O(t^2)}$!!

Open computer algebra system for polynomial computations SINGULAR
`CocGM`(t, G, opt)
http://personales.us.es/raufalgan/LS/hadamard.lib

$$\begin{cases} G = 1 \Rightarrow \mathbb{Z}_t \times \mathbb{Z}_2^2, G = 2 \Rightarrow D_{4t} \\ opt = 1 \Rightarrow \sharp\mathcal{H}_G, opt = 2 \Rightarrow \mathcal{H}_G \end{cases}$$

$$t \leq 3$$

Basis of normalized cocycles

Fixed a representative cocycle ρ, and a basis for normalized cocycles **B**.
$\mathbb{Q}[X]$ be the polynomial ring over $\{X\} = \{x_i \colon\ i \in \{1, \ldots, k\}\}$

Basis of normalized cocycles

Fixed a representative cocycle ρ, and a basis for normalized cocycles **B**.
$\mathbb{Q}[X]$ be the polynomial ring over $\{X\} = \{x_i : \ i \in \{1, \ldots, k\}\}$

Theorem

*(Álvarez et al.)[2008] The matrix M_ψ is Hadamard if and only if the vector of coordinates $(x_1, \ldots, x_k)_{\mathbf{B}}$ of ψ with regards to **B** satisfies the following system of $4t-1$ equations and k unknowns*

$$\left\{ \begin{array}{lcl} (m_{2,1}^1)^{x_1} \ldots (m_{2,1}^k)^{x_k} + \ldots + (m_{2,4t}^1)^{x_1} \ldots (m_{2,4t}^k)^{x_k} & = & 0 \\ & \vdots & \\ (m_{4t,1}^1)^{x_1} \ldots (m_{4t,1}^k)^{x_k} + \ldots + (m_{4t,4t}^1)^{x_1} \cdots (m_{4t,4t}^k)^{x_k} & = & 0 \end{array} \right. \tag{2}$$

□

Theorem

The set $\mathcal{H}_G^\rho$ can be identified with the set of zeros of the following zero-dimensional ideal of $\mathbb{Q}[X]$.

$$J_G := \langle\, x_i^2 - x_i : \ i \in \{1, \ldots, k-m\}\,\rangle + \langle \sum_{h=1}^{4t} s_{l,h}(X) : \ l \in \{1, \ldots 4t-1\}\,\rangle.$$

$s(l,h)$ is defined in terms of paths and intersections, and $\deg(s_{l,h}) \leq 2$.

Theorem

The set $\mathcal{H}_G^\rho$ can be identified with the set of zeros of the following zero-dimensional ideal of $\mathbb{Q}[X]$.

$$J_G := \langle\, x_i^2 - x_i :\ i \in \{1, \ldots, k-m\}\,\rangle + \langle\, \sum_{h=1}^{4t} s_{l,h}(X) :\ l \in \{1, \ldots 4t-1\}\,\rangle.$$

$s(l,h)$ is defined in terms of paths and intersections, and $\deg(s_{l,h}) \leq 2$.

Now, Lakshman and Lazard $\Longrightarrow 2^{O(t)}$

Theorem

The set $\mathcal{H}_G^\rho$ can be identified with the set of zeros of the following zero-dimensional ideal of $\mathbb{Q}[X]$.

$$J_G := \langle\, x_i^2 - x_i \colon\ i \in \{1, \ldots, k-m\}\,\rangle + \langle \sum_{h=1}^{4t} s_{l,h}(X) \colon\ l \in \{1, \ldots 4t-1\}\,\rangle.$$

$s(l,h)$ is defined in terms of paths and intersections, and $\deg(s_{l,h}) \leq 2$.

Now, Lakshman and Lazard $\Longrightarrow 2^{O(t)}$

`CocGB`(t, G, opt)

Theorem

The set $\mathcal{H}_G^{\rho}$ can be identified with the set of zeros of the following zero-dimensional ideal of $\mathbb{Q}[X]$.

$$J_G := \langle\, x_i^2 - x_i :\ i \in \{1, \ldots, k-m\}\,\rangle + \langle\, \sum_{h=1}^{4t} s_{l,h}(X) :\ l \in \{1, \ldots 4t-1\}\,\rangle.$$

$s(l,h)$ is defined in terms of paths and intersections, and $\deg(s_{l,h}) \leq 2$.

Now, Lakshman and Lazard $\Longrightarrow 2^{O(t)}$

$\texttt{CocGB(}t, G, opt\texttt{)}$

$$\begin{cases} G = 1 \Rightarrow \mathbb{Z}_t \times \mathbb{Z}_2^2, G = 2 \Rightarrow D_{4t} \\ opt = 1 \Rightarrow \sharp\mathcal{H}_G, opt = 2 \Rightarrow \mathcal{H}_G \end{cases}$$

Theorem

The set $\mathcal{H}_G^\rho$ can be identified with the set of zeros of the following zero-dimensional ideal of $\mathbb{Q}[X]$.

$$J_G := \langle x_i^2 - x_i : \; i \in \{1, \ldots, k-m\} \rangle + \langle \sum_{h=1}^{4t} s_{l,h}(X) : \; l \in \{1, \ldots 4t-1\} \rangle.$$

$s(l,h)$ is defined in terms of paths and intersections, and $deg(s_{l,h}) \leq 2$.

Now, Lakshman and Lazard $\Longrightarrow 2^{O(t)}$

`CocGB(`t, G, opt`)`

$$\begin{cases} G = 1 \Rightarrow \mathbb{Z}_t \times \mathbb{Z}_2^2, G = 2 \Rightarrow D_{4t} \\ opt = 1 \Rightarrow \sharp\mathcal{H}_G, opt = 2 \Rightarrow \mathcal{H}_G \end{cases}$$

$$t \leq 7, \; D_{4t}$$

Fine tuning: $\mathbb{Z}_t \times \mathbb{Z}_2^2$

Fine tuning: $\mathbb{Z}_t \times \mathbb{Z}_2^2$

Diagrammatic properties:

$$\left|\begin{array}{ccccccc} - & - & - & \times & \times & \times & - \\ - & - & \times & - & \times & - & \times \\ - & - & - & - & \times & - & - \\ \times & \times & - & - & \times & - & - \end{array}\right|$$

$\texttt{CocAH}(t, col, dist, H)$

Fine tuning: $\mathbb{Z}_t \times \mathbb{Z}_2^2$

Diagrammatic properties:

$$\left| \begin{array}{ccccccc} - & - & - & \times & \times & \times & - \\ - & - & \times & - & \times & - & \times \\ - & - & - & - & \times & - & - \\ \times & \times & - & - & \times & - & - \end{array} \right|$$

$\texttt{CocAH}(t, col, dist, H)$

$$\begin{cases} \text{col: parity of columns} \\ \text{dist: sum of each row} \\ \text{H: fixed values of some coordinates} \end{cases}$$

Fine tuning: $\mathbb{Z}_t \times \mathbb{Z}_2^2$, example

$t = 31$

Fine tuning: $\mathbb{Z}_t \times \mathbb{Z}_2^2$, example

$t = 31$

col: $0, 4, 2, 4, 2, 2, 2, 2, 0, 2, 2, 0, 4, 2, 2$

Fine tuning: $\mathbb{Z}_t \times \mathbb{Z}_2^2$, example

$t = 31$

col: $0, 4, 2, 4, 2, 2, 2, 2, 0, 2, 2, 0, 4, 2, 2$

dist: $12, 18, 18, 12$

Fine tuning: $\mathbb{Z}_t \times \mathbb{Z}_2^2$, example

$t = 31$

col: $0, 4, 2, 4, 2, 2, 2, 2, 0, 2, 2, 0, 4, 2, 2$

dist: $12, 18, 18, 12$

$H = 14, 15, 21, 24, 29$

Fine tuning: $\mathbb{Z}_t \times \mathbb{Z}_2^2$, example

$t = 31$

col: $0, 4, 2, 4, 2, 2, 2, 2, 0, 2, 2, 0, 4, 2, 2$

dist: $12, 18, 18, 12$

$H = 14, 15, 21, 24, 29$

$$10F6F96990660F6666F06609969F6F0$$

Fine tuning: D_{4t}

Fine tuning: D_{4t}

$\texttt{CocDH}(t, col, dist, H)$

Fine tuning: D_{4t}

$\texttt{CocDH}(t, col, dist, H)$

$$\begin{cases} \text{dist: number of new intersections in each row [2,t]} \\ \text{H: fixed values of some coordinates} \end{cases}$$

Fine tuning: D_{4t}, example

$t = 31$

Fine tuning: D_{4t}, example

$t = 31$

dist $1, 1, 2, 2, 3, 3, 2, 3, 0, 1, 0, 4, 2, 2, 3, 2, 3, 2, 2, 0, 0, 3, 1, 1, 2, 1, 3, 2, 2, 3$

Fine tuning: D_{4t}, example

$t = 31$

dist $1, 1, 2, 2, 3, 3, 2, 3, 0, 1, 0, 4, 2, 2, 3, 2, 3, 2, 2, 0, 0, 3, 1, 1, 2, 1, 3, 2, 2, 3$

$H = \underline{5}, \underline{6}, \underline{17}, \underline{36}, \underline{48}, 63, 64, \underline{84}, \underline{95}, 115, \underline{117}$

Fine tuning: D_{4t}, example

$t = 31$

dist $1, 1, 2, 2, 3, 3, 2, 3, 0, 1, 0, 4, 2, 2, 3, 2, 3, 2, 2, 0, 0, 3, 1, 1, 2, 1, 3, 2, 2, 3$

$H = \underline{5}, \underline{6}, \underline{17}, \underline{36}, \underline{48}, 63, 64, \underline{84}, \underline{95}, 115, \underline{117}$

$$21172424E984E2E3FC6B06D5527CA70$$

Future work

Future work

Improve the quality of the helping information

to get better results !

Thank you and farewell !!!