An Asymptotic Approach to the Hadamard Conjecture

Rod Canfield

erc@cs.uga.edu

Department of Computer Science

University of Georgia

W80

(Waterloo Workshop in Computer Algebra)

May 28, 2011

Acknowledgements

Eugene Zima, Ilias Kotsireas
Department of Physics & Computer Science
Wilfrid Laurier University
the C(omputer) A(lgebra) R(esearch) G(roup) Laboratory

Past Co-authors: Jason Gao, Catherine Greenhill,
Brendan McKay, Bob Robinson
Host institution: Australia National University

Collaborators: Warwick de Launey & David A. Levin

NSA Mathematical Sciences Program

HAPPY BIRTHDAY, HERB!

Main Definitions

An $n \times t$ matrix over $\{\pm 1\}$ is a partial Hadamard matrix provided the rows are pairwise orthogonal.

Definition: $H_{nt} :=$ the # of $n \times t$ partial Hadamard matrices

Example. One of the matrices counted by H_{58}:

$$\begin{array}{cccccccc} + & + & + & + & + & + & + & + \\ + & + & + & + & - & - & - & - \\ + & + & - & - & + & + & - & - \\ + & - & + & - & + & - & + & - \\ - & - & + & + & + & + & - & - \end{array}$$

Example illustrates: $n \geq 3 \ \& \ H_{nt} \neq 0 \implies 4|t$

The Problem

Find an asymptotic formula for H_{nt} valid along certain infinite sequences of pairs (n, t).

The Problem

Find an asymptotic formula for H_{nt} valid along certain infinite sequences of pairs (n,t).

Theorem (de Launey & Levin, 2010) Let (n,t) be an infinite sequence of pairs satisfying $4|t$ and $t \geq n^{12+\epsilon}$. Then along this sequence

$$H_{nt} \sim \frac{2^{nt+(n-1)^2}}{(2\pi t)^{d/2}}, \quad d = \binom{n}{2}.$$

The Problem

Find an asymptotic formula for H_{nt} valid along certain infinite sequences of pairs (n, t).

Theorem (de Launey & Levin, 2010) Let (n, t) be an infinite sequence of pairs satisfying $4|t$ and $t \geq n^{12+\epsilon}$. Then along this sequence

$$H_{nt} \sim \frac{2^{nt+(n-1)^2}}{(2\pi t)^{d/2}}, \quad d = \binom{n}{2}.$$

A Fourier-analytic approach to counting partial Hadamard matrices

Cryptography and Communications 2(2010) pp 307–334.

The Hadamard Conjecture

The HADAMARD CONJECTURE states that there exist square Hadamard matrices of size $t \times t$ for $t \in \{1, 2, 4, 8, 12, 16, 20, \ldots\}$.

Various constructions have been found

$t = 668$ is the first undecided value

$t = 428$ was decided in 2004

Outline of Talk

Circle Method Estimates
Progress on Latin rectangles
The Generating Function
The primary and secondary regions

The Circle Method

$$
\begin{aligned}
a_n &= [z^n] f(z) \\
&= \frac{1}{2\pi i} \oint_{|z|=r} \frac{f(z)}{z^{n+1}} dz \\
&= \frac{1}{2\pi r^n} \int_{-\pi}^{+\pi} \frac{f(re^{i\theta})}{e^{ni\theta}} d\theta \\
&= \frac{1}{2\pi r^n} \left[\int_{-\delta}^{+\delta} \cdots \; + \; \int_{\delta \le |\theta| \le \pi} \cdots \right]
\end{aligned}
$$

Latin Rectangles

Another two-parameter asymptotic counting problem

How many $k \times n$ Latin rectangles are there ?

Erdos & Kaplansky	1946	$k = O(\log n)^{3/2-\epsilon})$
Yamamoto	1951	$k = o(n^{1/3})$
Stein	1978	$k = o(n^{1/2})$
Godsil & McKay	1990	$k = o(n^{6/7})$

$$(n!)^k \left(\frac{(n)_k}{n^k}\right)^n \left(1 - \frac{k}{n}\right)^{-n/2} e^{-k/2}$$

Main Symbols

$$\begin{array}{cc} n & \text{the height of the pHm} \\ t & \text{the width} \\ d & = \binom{n}{2} \text{ the dimension of an integral} \\ \delta & \text{defines primary/secondary regions.} \end{array}$$

y and $Z(y)$

Given vector y of height n

$$y = \begin{bmatrix} \vdots \\ y_j \\ \vdots \end{bmatrix} \quad \in \quad \{\pm 1\}^n,$$

define the vector of inner products, $Z(y)$, by

$$Z(y) = \begin{bmatrix} \vdots \\ y_j y_k \\ \vdots \end{bmatrix} \quad \in \quad \{\pm 1\}^d.$$

Example of $Z(y)$

$$
\begin{array}{cccccccc}
+ & + & + & + & - & - & - & - \\
+ & + & - & - & + & + & - & - \\
+ & - & + & - & + & - & + & - \\
- & - & + & + & + & + & - & -
\end{array}
$$

$$
\downarrow
$$
$$
Z
$$
$$
\downarrow
$$

$$
\begin{array}{cccccccc}
+ & + & - & - & - & - & + & + \\
+ & - & + & - & - & + & - & + \\
- & - & + & + & - & - & + & + \\
+ & - & - & + & + & - & - & + \\
- & - & - & - & + & + & + & + \\
- & + & + & - & + & - & - & +
\end{array}
$$

H_{nt} as a constant term

Define $M = M_n = \{Z(y) : y \in \{\pm 1\}^n\}$; $|M| = 2^{n-1}$

$$
\begin{aligned}
H_{nt} &= 2^t \quad \times \quad \#\{(\vec{m}_1, \ldots, \vec{m}_t) : \vec{m}_k \in M \ \& \ \textstyle\sum_k \vec{m}_k = \vec{0}\} \\
&= 2^t \quad \times \quad [x_{12}^0 \cdots x_{n-1n}^0] \left(\textstyle\sum_{\vec{m} \in M} \prod_{jk} x_{jk}^{m_{jk}} \right)^t
\end{aligned}
$$

H_{nt} as an Integral

Let $x_{jk} = e^{i\lambda_{jk}}$ and define

$$\psi(\lambda) = \frac{1}{|M|} \sum_{\vec{m} \in M} e^{i\lambda \cdot \vec{m}}.$$

Then,

$$H_{nt} = 2^t \times [x_{12}^0 \cdots x_{n-1n}^0] \left(\sum_{\vec{m} \in M} \prod_{jk} x_{jk}^{m_{jk}} \right)^t$$

$$= \frac{2^{nt}}{(2\pi)^d} \times \int_{-\pi}^{+\pi} \cdots \int_{-\pi}^{+\pi} \psi(\lambda)^t d\lambda.$$

Primary/Secondary

Let $\Lambda = \{\lambda : |\psi(\lambda)| = 1\}$, and $4|t$.

$$H_{nt} = \frac{2^{nt}}{(2\pi)^d} \left[2^{(n-1)^2} \int_{B_\delta} \psi(\lambda)^t d\lambda + \int_{R_\delta} \psi(\lambda)^t d\lambda \right]$$

$$B_\delta = \{\lambda : |\lambda_{jk}| \leq \delta\}$$

$$R_\delta = [-\pi, +\pi]^d \cap \{\mathrm{dist}(\lambda, \Lambda) \geq \delta\}.$$

Primary Integral

Assuming $n\delta \longrightarrow 0$,

$$\psi(\lambda)^t = \exp\left(-(t/2) \parallel \lambda \parallel^2 + O(tn^3\delta^3)\right).$$

$$\int_{-\delta}^{+\delta} \exp\left(-(t/2)x^2\right) \quad = \quad \sqrt{\frac{2\pi}{t}} \left(1 + O(e^{-t\delta^2/2})\right).$$

Provided $tn^3\delta^3 \longrightarrow 0$, $de^{-t\delta^2/2} \longrightarrow 0$,

$$\int_{B_\delta} \psi(\lambda)^t = \left(\frac{2\pi}{t}\right)^{d/2} (1 + o(1)).$$

Secondary Integral

de Launey and Levin prove that for any k, $1 \leq k \leq n$,

$$|\psi(\lambda)|^2 \;\leq\; \frac{1}{2} + \frac{1}{2} \prod_{\substack{j=1 \\ j \neq k}}^{n} \cos 2\lambda_{jk}$$

This gives

$$\left| \int_{R_\delta} \psi(\lambda)^t \right| \;\leq\; (2\pi)^d \, e^{-ct\delta^2}$$

Combining the Two

$$H_{nt} = \frac{2^{nt}}{(2\pi)^d}\left[2^{(n-1)^2}\int_{B_\delta}\psi(\lambda)^t d\lambda + \int_{R_\delta}\psi(\lambda)^t d\lambda\right]$$

$$H_{nt} = \frac{2^{nt}}{(2\pi)^d}\left[2^{(n-1)^2}\left(\frac{2\pi}{t}\right)^{d/2}(1+o(1)) + O(1)(2\pi)^d\, e^{-ct\delta^2}\right]$$

$$H_{nt} = 2^{nt}\left[2^{(n-1)^2}(2\pi t)^{-d/2}(1+o(1)) + O(1)\, e^{-ct\delta^2}\right]$$

The assumptions: $tn^3\delta^3 \to 0$, $de^{-t\delta^2/2} \to 0$.

For sec. $= o($prim.$)$, $t\delta^2 = \Omega(d\log t)$

The de Launey Levin Theorem

$$H_{nt} \; = \; 2^{nt} \left[2^{(n-1)^2} (2\pi t)^{-d/2} (1 + o(1)) \; + \; O(1) e^{-ct\delta^2} \right]$$

We arrive at deLauney and Levin's formula,

$$H_{nt} \; \sim \; \frac{2^{nt+(n-1)^2}}{(2\pi t)^{d/2}},$$

obtained under the assumption that

$$\delta = \sqrt{\frac{n^2 \log t}{t}}$$

satisfies $tn^3\delta^3 \to 0$ and $de^{-t\delta^2/2} \to 0$.