An Asymptotic Approach to the Hadamard Conjecture

Rod Canfield

erc@cs.uga.edu

Department of Computer Science

University of Georgia

Warwick's Conference

May 16, 2011

Words From Fiction

I knew I had been appointed from outside the Royal Aircraft Establishment as a new broom to do a bit of sweeping. I hope I did it with sympathy and understanding, because the problem of the aging civil servant engaged in research is not an easy one. There comes a time when the research worker . . . becomes detached from all reality. He tends to lose interest in the practical application of his work . . . and turns more and more to the ethereal realms of mathematical theory; as bodily weakness gradually puts an end to physical adventure he turns readily to the adventure of the mind, to the purest realms of thought where in the nature of things no unpleasant consequences can follow if he makes a mistake.

No Highway   a novel by Nevil Shute

Thanks

Collaborators: Warwick de Launey, David Levin, Brendan McKay

Organizing & Sponsoring: CCR La Jolla

Definition

Let n, t be positive integers.
An $n \times t$ partial Hadamard matrix
is an $n \times t$ matrix over $\{-1, +1\}$
whose rows are orthogonal.

We let H_{nt} equal the number of such matrices.

Theorem

Let $\epsilon > 0$. Then,

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

along any infinite sequence of (n, t) with $4|t$ and $t > n^{12+\epsilon}$.

Warwick de Launey & David Levin
A Fourier-analytic Approach to Counting Partial Hadamard Matrices
Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences
Volume 2 (2010) pages 307–334.

The Circle Method

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

Stirling's Formula

$$\frac{1}{n!} = [z^n]e^z = \frac{1}{2\pi i}\oint_{|z|=r} \frac{\exp(z)}{z^{n+1}}\,dz = \frac{1}{2\pi}\int_{-\pi}^{+\pi} \frac{\exp(re^{i\theta})}{r^n e^{ni\theta}}\,d\theta$$

$$= \frac{e^r}{2\pi r^n}\Big[\int_{-\delta}^{+\delta} \exp\left((r-n)i\theta - (1/2)r\theta^2 + O(r|\theta|^3)\right)d\theta$$

$$+O(1)\int_{\delta\le|\theta|\le\pi} \exp\left(-cr\theta^2\right)d\theta\Big]$$

$$= \frac{e^n}{2\pi n^n}\left[\sqrt{\frac{2\pi}{n}}\,(1+o(1))\,.\right]$$

W. K. Hayman

A generalisation of Stirling's formula

Journal für die reine und angewandte Mathematik

vol 196 (1956) 67–95.

Integer Matrices

Let $ms = nt$ and $M(m,n;s,t)$ be the number of $m \times n$ matrices over the integers w/ row, col sums s and t; then,

$$M(m,n;s,t) = [x_1^s \cdots x_m^s y_1^t \cdots y_n^t] \prod_{\substack{1 \le j \le m \\ 1 \le k \le n}} (1 - x_j y_k)^{-1}$$

$$= \frac{1}{(2\pi)^{m+n}} \frac{(1-r^2)^{-mn}}{r^{sm+tn}}$$

$$\times \int_{-\pi}^{\pi} \cdots \int_{-\pi}^{\pi} \frac{\prod_{j,k} \left(1 - \lambda(e^{i(\theta_j+\phi_k)} - 1)\right)^{-1}}{\exp(is \sum_j \theta_j + it \sum_k \phi_k)}$$

where $\lambda = \frac{r^2}{1-r^2}$

Saddlepoint Equations

$$\left(1 - \lambda(e^{i(\theta_j+\phi_k)} - 1)\right)^{-1}$$

$$= \exp\left(i\lambda(\theta_j + \phi_k) - (1/2)\lambda(1+\lambda)(\theta_j + \phi_k)^2 + \cdots\right)$$

Equations: (1) $\lambda n = s$, (2) $\lambda m = t$
So, λ is the average entry

Primary Region $\mathcal{R}$

$$
\begin{aligned}
|\overline{\theta} + \overline{\phi}| &\leq (1+\lambda)^{-1}(mn)^{-1/2+\epsilon} \\
|\hat{\theta}_j| &\leq (1+\lambda)^{-1}(n)^{-1/2+\epsilon}, 1 \leq j \leq m \\
|\hat{\phi}_k| &\leq (1+\lambda)^{-1}(m)^{-1/2+\epsilon}, 1 \leq k \leq n
\end{aligned}
$$

$$
\exp\left(-(1/2)\lambda(1+\lambda)\sum_{jk}(\theta_j + \phi_k)^2\right)
$$

$$
4\pi\frac{\sqrt{mn}}{2}\left(\frac{2\pi}{Amn}\right)^{-1/2}\left(\frac{2\pi}{An}\right)^{-(m-1)/2}\left(\frac{2\pi}{Am}\right)^{-(n-1)/2}
$$

$A = \lambda(1+\lambda)$.

An Integration Lemma

Separate pdf file

Secondary

$\mathcal{A} : \cos(\theta_j + \phi_k) \leq \cos\delta$ for at least $(1/3)\min(mn^\epsilon, m^\epsilon n)$ pairs.
For $X \subseteq (-\pi, \pi]$, $N_\theta(X), N_\phi(X)$ count $j : \theta_j \in X$, $k : \phi_k \in X$.
$\mathcal{R}(\ell) : N_\theta([(\ell - 4)\delta, (\ell + 4)\delta]) \geq m - m^\epsilon$,
and $N_\phi([(-\ell - 4)\delta, (-\ell + 4)\delta]) \geq n - n^\epsilon$.
$U = \bigcup_{\ell=0}^{N-1} \mathcal{R}(\ell)$.

$$\begin{aligned} \mathcal{A} \cup U &= [-\pi, \pi]^{m+n} \\ \int_{\mathcal{A}} |F| &= O(e^{-n}) I_0 \\ \int_{U \cap \mathcal{R}^c} |F| &= O(e^{-n^\epsilon}) I_0. \end{aligned}$$

A Deduction

Conjecture: for $m, n \to \infty$

$$M(m,n;s,t) = \frac{\binom{n+s-1}{s}^m \binom{m+t-1}{t}^n}{\binom{mn+\lambda mn-1}{\lambda mn}}$$

$$\times \quad \exp\left(\frac{1}{2} + o(1)\right)$$

Orthogonal Arrays

$0, 1$ matrices with n columns, $q2^k$ distinct rows
Each k-pattern appears q times in any k-set of columns

$$N(n, k) = \sum_q N(n, k, q)$$

is the number of order k correlation-immune Boolean functions of n variables

$$H_{nn} = 2^n n! N(n-1, 2, n/4), n > 2$$

Gen. Func.

$\mathcal{I}_k = \{S \in 2^{[n]} \ : \ |S| \leq k\}$
$M = \sum_{j=0}^{k} \binom{n}{j}$ variables $\{x_S \ : \ S \in \mathcal{I}_k\}$

$$F(x) = \prod_{\alpha \in \{\pm 1\}^n} \left(1 + \prod_{S \in \mathcal{I}_k} x_S^{\alpha_S} \right),$$

where

$$\alpha_S = \prod_{j \in S} \alpha_j$$

$$N(n,k,q) = \text{ constant term in } x_{\emptyset}^{-q2^k} F(x)$$

Results

$$N(n,k) \sim 2^{2^n+Q-k}(2^{n-1}\pi)^{-(M-1)/2}$$

$$M = \sum_{j=0}^{k} \binom{n}{j} \quad \text{and} \quad Q = \sum_{j=1}^{k} j \binom{n}{j}$$

$$1 \leq k \leq \left(\frac{\log 2}{6} - \varepsilon \right) \frac{n}{\log n}$$

Denisov

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	$k = o(n^{6/7})$

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

Integral Formula

With $d = \binom{n}{2}$,

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

$$\psi_n(\lambda) = 1 + \sum_{G \in \mathcal{M}_{\mathrm{even}}(n)} \prod_{jk} \frac{(i\lambda_{jk})^{\mu_{jk}(G)}}{\mu_{jk}(G)!}$$