

3. I risultati “classici”

Hadamard avrebbe voluto realizzare altre matrici di ordine superiore a 12 e 20 e diverso da potenze di 2 con una tecnica analoga, ma non ci riuscì.

Con i due nuovi interi 12 e 20 e con il metodo di Sylvester, l'insieme di interi che sono numeri di Hadamard si ampliava, contenendo quelli del tipo

$$2^k, \quad 12 \cdot 2^k \quad \text{e} \quad 20 \cdot 2^k \quad (k = 0, 1, 2, \dots).$$

Hadamard sospettava che la sua costruzione si potesse in qualche modo generalizzare. Ciò avvenne cinque anni più tardi ad opera del padovano Umberto Scarpis, che per primo sviluppò l'intuizione di Hadamard.

Scarpis pubblicò infatti nel 1898 il lavoro:

«*Sui determinanti di valore massimo*»

Rendiconti del Reale Istituto Lombardo di Scienze e Lettere, (2), 31 (1898), 1441-1446.

Nota. Eliahou ringrazia per avergli inoltrato copia di questo lavoro Andrea Montoli, allora studente di dottorato a Milano in cotutela a Calais, poi vincitore di un posto di Ricercatore a Padova, dove non ha preso servizio avendo nel frattempo ottenuto un posto migliore; è ora professore associato a Milano.

Una descrizione della vita e delle opere di Scarpis si trova nell'articolo del nostro compianto collega Maurizio Emaldi:

“*Campi finiti: piccola nota storica*”

MatematicaMente, Pubblicazione della sezione veronese della MATHESIS, N.143 (2009).

Scarpis fu presidente della sezione bolognese della Mathesis.

Chi era allora Scarpis e che contributo diede alle matrici di Hadamard?

Nato a Padova nel 1861, laureato in matematica a Padova nel 1884 avendo tra i suoi maestri Gregorio Ricci Curbastro e Francesco Flores D'Arcais, Umberto Scarpis insegnò nei ginnasi di varie città e poi al Liceo Minghetti di Bologna. Fu libero docente di algebra all'Università di Bologna, dove morì il 27 dicembre 1921.

Il merito di Scarpis riguardo alle matrici di Hadamard fu quello di avere per primo fatto intervenire i numeri primi nelle costruzioni di tali matrici.

TEOREMA (Scarpis, 1898) *Se $n-1$ è un numero primo e se esiste una matrice di Hadamard di ordine n , allora ne esiste anche una di ordine $(n-1)n$.*

La dimostrazione di Scarpis si ispira alla costruzione di Hadamard della matrice di ordine 12, facendo uso di permutazioni cicliche.

I risultati di Sylvester e Scarpis forniscono un collegamento tra le matrici di Hadamard ed i numeri primi di Mersenne.

Se $n = 2^k$ ($k \geq 1$) sappiamo da Sylvester che n è un numero di Hadamard.

Il teorema di Scarpis assicura che, se $2^k - 1$ è un numero primo, anche $(2^k - 1)2^k$ è un numero di Hadamard; ad esempio:

$$(2^5 - 1)2^5 = 992 \quad \text{e} \quad (2^7 - 1)2^7 = 16.256$$

Se $2^k - 1$ è un numero primo, allora k deve essere primo. I numeri $2^k - 1$ con k primo sono i numeri di Mersenne. Per $k = 2, 3, 5, 7$ tali numeri sono primi, ma per $k = 11$ no:

$$2^{11} - 1 = 2047 = 23 \times 89.$$

Nel 2012 erano noti 47 numeri primi di Mersenne ed il più grande numero primo noto era:

$$2^{43.112.609} - 1$$

che ha 13 milioni di cifre.

scoperto nel 2008

Non si sa se di tali numeri ce ne è una infinità.

Dopo poco più di 30 anni, l'americano Gilman mostrò che una delle due ipotesi del teorema di Scarpis è automaticamente verificata.

TEOREMA (Gilman, 1930) *Se n è multiplo di 4 e $n-1$ è un numero primo, allora esiste una matrice di Hadamard di ordine n .*

In altri termini, se $n = p + 1$ (con p primo) è multiplo di 4, allora n è un numero di Hadamard. Di tale teorema si ha solo l'“abstract” di un articolo negli atti di un convegno tenuto a Cleveland nel 1930, dal titolo:

«On the Hadamard determinant theorem and orthogonal determinants»

Bulletin Amer. Math. Soc. 37 (1931), 30-31.

Gilman non pubblicò mai questo risultato, probabilmente perché poco dopo uscì un lavoro di Raymond Paley che lo migliorava molto. L'idea innovatrice cui si accenna nell'abstract è quella di usare i quadrati del campo con p elementi, dove $p = n - 1$.

Vale la pena dare alcuni cenni biografici su Raymond Paley.

Questo giovane matematico, cui avevano preconizzato un grande avvenire, nacque nel 1907 a Londra. Fu riconosciuto come il più brillante allievo a Cambridge della coppia Hardy & Littlewood. Fu autore con Norbert Wiener, uno dei padri della cibernetica, di un celebrato teorema di analisi armonica, co-autore con Littlewood di un teorema di analisi complessa e collaborò con Zygmund sulle serie di Fourier. Morì a 26 anni, sotto una slavina a 2.800 metri di altitudine nelle Rocky Mountains canadesi durante una escursione invernale in solitaria.

La sua costruzione che generalizza quella di Gilman usa i quadrati dei campi finiti e si trova nel lavoro: "*On orthogonal matrices*", J. Math. and Physics. 12 (1933), 311–320.

TEOREMA (Paley, 1933) *Se n è multiplo di 4 e $n-1$ oppure $n/2 - 1$ sono potenze di numeri primi, allora esiste una matrice di Hadamard di ordine n .*

Accenniamo alla costruzione di Paley. Le costruzioni sono in realtà due, simili ma diverse tra loro, a seconda che $n - 1 = p^k$ oppure $n/2 - 1 = p^k$. Noi vedremo la prima costruzione, essendo la seconda un po' più complicata.

o meno di isomorfismi

Ricordiamo che esiste un unico campo F_q con $q = p^k$ elementi (campo di Galois), estensione del campo F_p , di dimensione k come spazio vettoriale su F_p .

Gli elementi non nulli di F_q sono radici del polinomio:

$$X^{q-1} - 1 = (X^{(q-1)/2} - 1)(X^{(q-1)/2} + 1).$$

Le radici di $X^{(q-1)/2} - 1$ sono dei quadrati, le radici di $X^{(q-1)/2} + 1$ non lo sono.

Se $a \in F_q$, il suo *carattere quadratico* $\chi(a)$ è posto pari a 0, 1 o -1, a seconda che a sia 0, oppure sia un quadrato o non lo sia.

Fissato F_q , con $q = p^k$, si definisce la *matrice di Jacobsthal* $q \times q$ associata (in onore di Ernst Jacobsthal (1882-1965), allievo di Frobenius e Schur, inventore della successione di numeri J_n definiti per induzione da: $J_0 = 0$, $J_1 = 1$ e $J_n = J_{n-1} + 2J_{n-2}$), che viene denotata con Q .

La matrice Q ha le righe e le colonne indiciate dagli elementi di F_q .

Il coefficiente di posto (a,b) ($a, b \in F_q$) è: $\chi(a-b)$.

La matrice Q soddisfa a: $QQ^T = qI_q - \underline{e}\underline{e}^T$

dove $\underline{e}^T = [1, 1, \dots, 1]$, per cui $\underline{e}\underline{e}^T$ è la matrice con tutti i coefficienti uguali ad 1.

Se $n - 1 = q$, Q è anti-simmetrica ($Q + Q^T = O$), se $n/2 - 1 = q$, Q è simmetrica.

Nel caso in cui $n-1 = q$, Paley prova che la matrice di Hadamard cercata è:

$$H_n = I_n + \begin{bmatrix} 0 & \underline{e}^T \\ -\underline{e} & Q \end{bmatrix}$$

Infatti:

$$H_n \cdot H_n^T = \left(I_n + \begin{bmatrix} 0 & \underline{e}^T \\ -\underline{e} & Q \end{bmatrix} \right) \cdot \left(I_n + \begin{bmatrix} 0 & -\underline{e}^T \\ \underline{e} & Q^T \end{bmatrix} \right) =$$

$$I_n + \begin{bmatrix} 0 & \underline{0}^T \\ \underline{0} & Q+Q^T \end{bmatrix} + \begin{bmatrix} n-1 & \underline{0}^T \\ \underline{0} & \underline{e}\underline{e}^T + QQ^T \end{bmatrix} =$$

$$\begin{bmatrix} n & \underline{0}^T \\ \underline{0} & I_{n-1} + Q + Q^T + \underline{e}\underline{e}^T + (n-1)I_{n-1} - \underline{e}\underline{e}^T \end{bmatrix} = nI_n$$

NB $Q\underline{e} = \underline{0} \Leftrightarrow \underline{e}^T Q^T = \underline{0}^T$
 perché in ogni riga di Q
 ci sono tanti 1 quanti -1,
 perché F_q ha tanti quadrati
 quanti non quadrati!

ESEMPIO DI COSTRUZIONE DI PALEY PER $n = 8 = 7 + 1$.

Il campo F_7 ha i 7 elementi: 0, 1, 2, 3, 4, 5, 6, di cui 1, 2 e 4 sono quadrati, mentre 3, 5 e 6 non lo sono, quindi si ha:

$$\chi(a) = 0 \quad , \quad \chi(1) = \chi(2) = \chi(4) = 1 \quad , \quad \chi(3) = \chi(5) = \chi(6) = -1 \quad .$$

La matrice di Jacobsthal 7x7 associata e la matrice di Hadamard 8x8 sono:

$$Q = \begin{array}{c|ccccccc} & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 0 & 0 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 0 & -1 & -1 & 1 & -1 & 1 \\ 2 & 1 & 1 & 0 & -1 & -1 & 1 & -1 \\ 3 & -1 & 1 & 1 & 0 & -1 & -1 & 1 \\ 4 & 1 & -1 & 1 & 1 & 0 & -1 & -1 \\ 5 & -1 & 1 & -1 & 1 & 1 & 0 & -1 \\ 6 & -1 & -1 & 1 & -1 & 1 & 1 & 0 \end{array} \quad H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \end{bmatrix}$$

E' facile provare tramite i risultati “classici” sopra ricordati che tutti multipli di 4 fino a 100 sono numeri di Hadamard, **tranne il 92**.

Sylvester \rightarrow 4 8 16 32 64 } 24 40 48 80 96

Hadamard \rightarrow 12 20

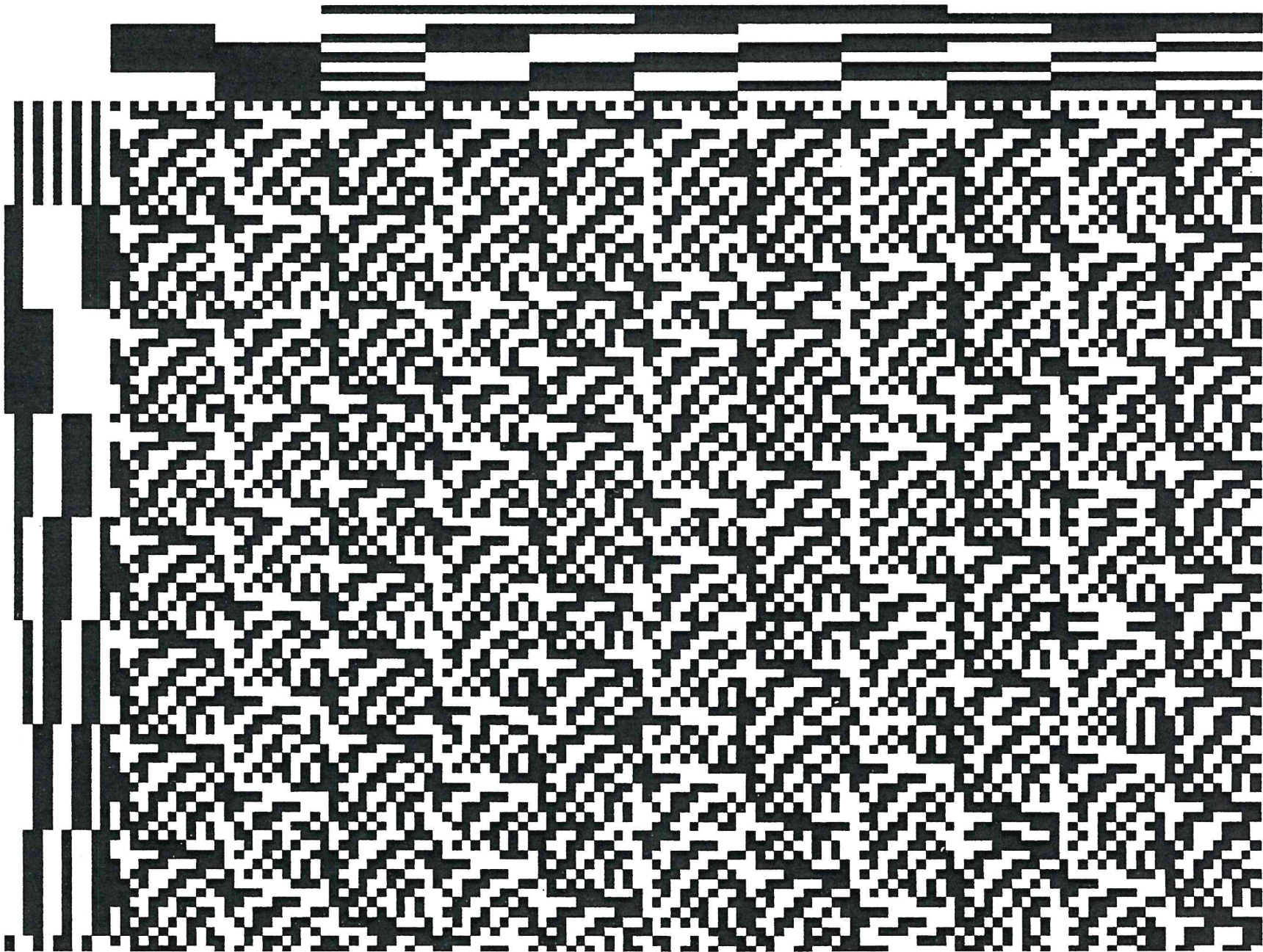
Scarpis $\rightarrow 7 \cdot 8 = 56$ e anche $11 \cdot 12 = 132$, $19 \cdot 20 = 380$, $23 \cdot 24 = 552$, $31 \cdot 32 = 992$,
 $47 \cdot 48 = 2.256$, $79 \cdot 80 = 6.320$

Gilman → 44 60 68 72 84 88

Paley I → 28

Paley II → 36 52 76 100

SCACCHIERA 132 x 132 OTTENUTA CON LA COSTRUZIONE DI SCARPIS



4. Alcuni sviluppi con l'avvento dei computers

Dopo Paley, ci vollero 30 anni perché anche il 92 cedesse sotto gli assalti dei matematici.

Ciò avvenne nel 1962 ad opera di Baumert, Golomb e Hall nel lavoro:

"Discovery of an Hadamard matrix of order 92"

Bull. Amer. Math. Soc. 68 (3), 237–238

usando una costruzione del 1944 di Williamson e servendosi dell'aiuto di un computer. Quindi:

tutti i multipli di 4 fino a 100 sono numeri di Hadamard.

Per i numeri >100 la situazione attestata nel 2012 da S. Eliahou è la seguente:

- i multipli di 4 ≤ 1.000 che non si sa se sono numeri di Hadamard sono

668 716 892 ;

l'ultimo a cadere nel 2008 sotto i colpi di D.Z. Dokovic è stato il 764

- i multipli di 4 tra 1.000 e 2.000 che non si sa se sono numeri di Hadamard

1.132 1.244 1.436 1.676 1.772 1.916 1.948 1.964 ;

l'ultimo a cadere nel 2012 sotto i colpi di Kotsireas, Dokovic e Golubitsky è 1.004

I seguenti risultati si trovano nell'articolo recente di Balonin, Doković e Karbovskiy:

"Construction of symmetric Hadamard matrices of order $4v$ for $v = 47, 73, 113$ "

Special Matrices, 6 (2018), 11–22.

- il più piccolo multiplo di 4 per cui non si conosceva l'esistenza di matrici di Hadamard simmetriche di quell'ordine era $188 = 4 \cdot 47$.
- matrici di Hadamard simmetriche di ordine 116, 156, 172 erano state costruite solo nel 2015 e 2017.
- per effettuare le costruzioni di matrici di Hadamard simmetriche, i tre autori hanno usato programmi appositi fatti girare su due PC che nel caso più favorevole hanno preso 5 minuti, mentre nel caso più sfavorevole hanno preso 5 giorni.

La tecnica usata è detta “*Propus array*” che utilizza matrici 4 x 4 a blocchi $v \times v$ (ricordano la matrice 12 x 12 di Hadamard) del tipo:

$$H = \begin{bmatrix} -C_1 & C_2P & C_3P & C_4P \\ C_3P & PC_4 & C_1 & -PC_2 \\ C_2P & C_1 & -PC_4 & PC_3 \\ C_4P & -PC_3 & PC_2 & C_1 \end{bmatrix}$$

dove i blocchi C_i sono opportune matrici circolanti $v \times v$ ed il blocco P è la matrice di permutazione che ha 1 sulla contro-diagonale.

La matrice H è di Hadamard se: $C_1C_1^T + C_2C_2^T + C_3C_3^T + C_4C_4^T = 4v I_v$.

L'estrema complicazione sta nello scegliere opportunamente le matrici C_i .

5. Applicazioni

C'è un libro dedicato interamente alle applicazioni delle matrici di Hadamard:

Kathy Horadam: "*Hadamard matrices and their applications*", Princeton Univ. Press, 2007.

Ecco alcuni settori in cui le matrici di Hadamard hanno trovato applicazioni:

- codici correttori d'errori per trasmissioni di immagini da sonde spaziali (Mariner)
- crittografia
- comunicazioni digitali radio-amatoriali
- telefonia mobile
- stima della varianza in statistica
- in spettrometria .

Per chi volesse saperne di più in generale:

R. Craigen and H. Kharaghani, «*Hadamard matrices and Hadamard designs*», in Handbook of Combinatorial Designs, Chapman & Hall, Boca Raton, 2007.