Constructions and Applications of Hadamard and Weighing Matrices

Assaf Goldberger[1] Yossi Strassler[2] Giora Dula[3]

[1] Tel-Aviv University assafg@post.tau.ac.il

[2] Dan Yishay danyishay@gmail.com

[3] Netanya Accademic College giora@netanya.ac.il

Rutgers March 8th 2018

content

- The work of Sylvester Walsh and Hadamard.
- Application to error correcting codes and to quantum random access codes.
- Payley and Williamson constructions and weighing matrices.
- The work of Koukouvinos and Seberry and of Harada and Munemasa on applications of Weighing Matrices.
- Further review of results (time permitting).
- Suppost and Shaddow geometries.

James Joseph Sylvester Matrices

- define the Sylvester matrices inductively

$$H_1 = \begin{pmatrix} 1 \end{pmatrix}, H_2 = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} H_{2^{n+1}} = \begin{pmatrix} H_{2^n} & H_{2^n} \\ H_{2^n} & -H_{2^n} \end{pmatrix}$$

- H_{2^n} have the properties:
  - H_{2^n} is a symmetric matrix.
  - 1) $H_{2^n} H_{2^n}^T = H_{2^n}^T H_{2^n} = 2^n I_{2^n}$.
  - 2) every two distict rows or distinct columns have half of their digits identical and half opposite to the other.
  - 3) det $H_{2^n} = 2^{n2^{n-1}}$ is the biggest possible value of determinants (volume of a complex parallelepiped) of the same dimension matrices with $|a_{i,j}| \leq 1$.

the Walsh matrices

- define the Walsh matrices $F_{n\times 2^n}(\mathbb{Z}_2) = F_n$ inductively

$$F_1 = \begin{pmatrix} 0 & 1 \end{pmatrix}, F_2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} F_{n+1} = \begin{pmatrix} 0_{1\times 2^n} & 1_{1\times 2^n} \\ F_n & F_n \end{pmatrix}$$

- the k^{th} column of F_n, $1 \leq k \leq 2^n$ is the diadic expansion of $k-1$.
- two non identical rows of F_n agree in 2^{n-1} position and differ in 2^{n-1} position.
- $F_n^T F_n$ is a square $2^n \times 2^n$ matrix. Applying componentwise $i \to 1-2i$ on $F_n^T F_n$ gives the Sylvester matrix.
-

$$H_4 = F_2^T F_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \quad (1)$$

Hadamard linear error correcting codes

- Any vector of n bits is a message. A message is a row of F_n^T. Two different messages are different rows of F_n^T.
- encipher each message m as the product of m with the "generating" matrix F_n. Any two distinct messages give two distinct rows in H_{2^n}, and have 2^{n-1} different digits.
- Any mistake in the enciphering and transmitting of messages by less then 2^{n-1} can be recoverd
- The Sylvester-Walsh-Hadamard linear error correcting code of type $[2^n, n, 2^{n-1}]_2$ is a linear map encipher: $(\mathbb{Z}_2)^n \to (\mathbb{Z}_2)^{2^n}$ so that the Hamming distance between any two messages is 2^{n-1}.
- The punctured Hadamard code is of type $[2^{n-1}, n, 2^{n-2}]_2$ and has as a generating matrix the right half of the matrix F_n.

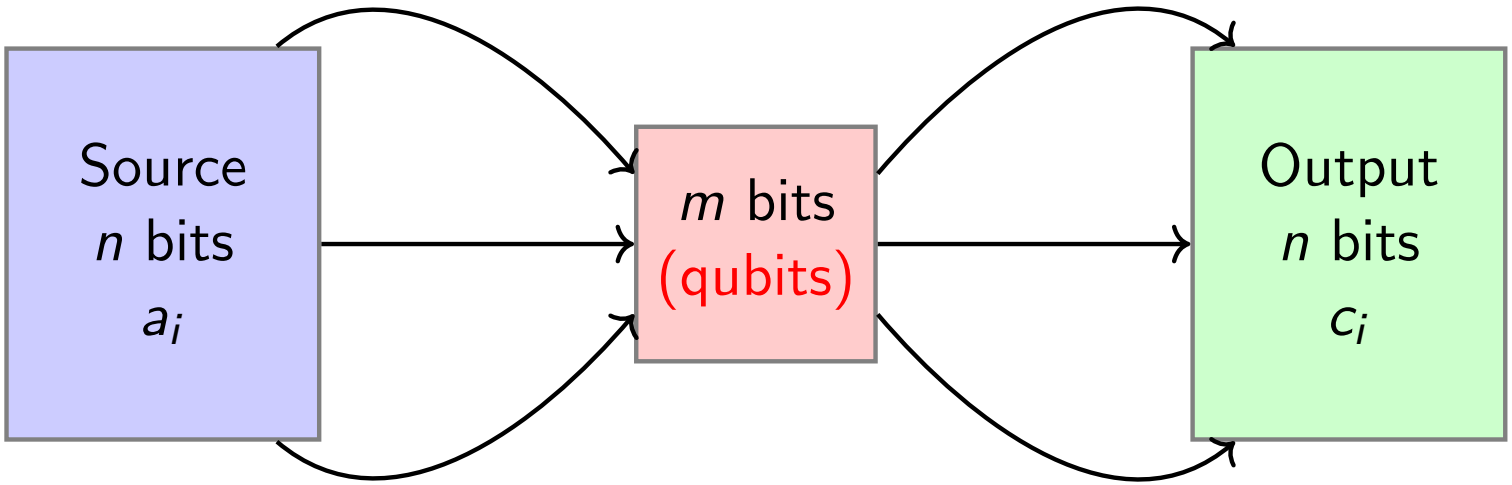
The work of Jacques Hadamard

- Hadamard asked, given a dimension n which square $n \times n$ matrices with $|a_{i,j}| \leq 1$ will have the biggest possible determinant.
- He was able to prove that any such H will satisfy that $HH^T = H^T H = nI_n$, will have $det(H) = n^{\frac{n}{2}}$. He proved that except for the Sylvester matrices of dimensions 1 and 2, any such other H_n must satisfy that $n\%4 = 0$.
- he made the famous conjecture that H_{4k} exist for all natural k. This conjecture is still open.
- A solution for the previous smallest unknown case of n=428 was announced by Kharaghani and Tayfeh-Rezaie in June 2004. the smallest order for which the existence of an Hadamard matrix is in doubt is currently 668.
- Hadamard also found H_{12} and H_{20}.

Applications of Hadamard matrices

- The probe Mariner 9 was sent by NASA to Mars, and sent home to earth on May 1971 photograph pictures taken for Mars. Transmission took a long time and was susceptible to errors and NASA chose to encipher the messages using the punctured Hadamard code.
- Any Hadamard (not necessarily Sylvester type) matrix can be used for error correcting (not linear) code. Take H_n and the adjunct matrix $[H, -H]$. Any (not necessarily linear) map from the set of cardinality $2n$ to the different rows of H and of $-H$ is a code.
- The difference between two messages is at least $\frac{n}{2}$. so that if there is less then $\frac{n}{4}$ corrupted bits the original message can be recovered.
- The Walsh code is a particular linear case where $H = F_n^T F_n$.

(Quantum) Random Access Codes



$$\forall i \; Prob(c_i = a_i) \geq p > 0.5$$

$$m \geq (1 - H(p))n$$

$$H(p) = -p \log_2(p) - (1 - p) \log_2(1 - p)$$

e.g. 2 bits $\rightarrow$ 1 qubit $\rightarrow$ 2 bits

$$p = \cos^2(\pi/8) \approx 0.85$$

QRAC and MUB's

- in QRAC one can work with qdits (=bases in $\mathbb{C}^d$).
- Two bases $\{e_i\}, \{f_j\}, 1 \leq i, j \leq d$ of $\mathbb{C}^d$ are mutually unbiased(MUB) if $\forall i, j | < e_i, f_j > |^2 = \frac{1}{d}$.
- In QRAC, one wants to work with MUB's.
- If $\{e_i\}$ is chosen to be the standard basis, $\{f_j\}$ must be chosen to be the rows of a normalized complex Hadamard matrix.
- Hadamard's proof that for H_n to exist it must hold that $n\%4 = 0$ is only valid for real Hadamard matrices.
- For all n there exists a (complex) H_n called the Fourier matrix.

Construction of Payley's matrices

- Suppose that $p \neq 2$ is a prime , and that q is a power of p. Denote $GF(q)$ the field with q elements. For $a \in \mathbb{G}F(q)$ define the Legendre symbol by

$$\left(\frac{a}{q}\right) = \begin{cases} 0 & a = 0 \\ 1 & a \neq 0 \quad \exists b, b^2 = a \\ -1 & a \neq 0 \quad \nexists b, b^2 = a \end{cases}$$

- Define the set $GF^+ = GF(q) \cup \{\infty\}$ and a square matrix C_{q+1} by

$$C_{i,j} = \begin{cases} \left(\frac{i-j}{q}\right) & i, j \in GF(q) \\ 0 & i = j = \infty \\ 1 & i = \infty \quad j \neq \infty \\ \left(\frac{-1}{q}\right) & j = \infty \quad i \neq \infty \end{cases}$$

Payley's Hadamard matrices

- C satisfies that $CC^T = C^T C = qI_{q+1}$.
- the diagonal terms in C equal 0, the off diagonal terms are ± 1.
- A matrix D_n with terms in $\{\pm 1, 0\}$ such that $DD^T = D^T D = (n-1)I_n$ is called a conference matrix.
- for $q\%4 = 1$ C is symmetric and for $q\%4 = 3$ C is antisymmetric.
- For $q\%4 = 3$ the matrix $C + I$ is a Payley's Hadamard matrix.
- For $q\%4 = 1$ the block matrix

$$\begin{pmatrix} C+I & C-I \\ C-I & -C-I \end{pmatrix}_{2q+2}$$

is the Payley's Hadamard matrix.

weighing matrices

- Denote $\mu_2^* = \{0, \pm 1\}$. $W \in \mathbb{M}_n(\mu_2^*)$ is called a weighing matrix $W(n, w)$ if it satisfies $WW^T = W^T W = wI_n$. n is called the order and w the weight of W.
- Thus Hadamard matrices are $W(n, n)$ matrices and conference matrices are $W(n, n-1)$ matrices. We saw above that Payley's construction is to form $W(n, n)$ from $W(k, k-1)$.
- The following are $W(2, w), 1 \leq w \leq 2$

$$\left(\begin{array}{c|cc} I_2 & 1 & 1 \\ & 1 & - \end{array}\right)$$

- The following are $W(3, w), 1 \leq w \leq 3$

$$\left(I_3 \;\middle|\; \mathrm{None} \;\middle|\; \mathrm{None}\right)$$

- The following are $W(4, w), 1 \leq w \leq 4$

$$\left(\begin{array}{cccc|cccc|cccc|cccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & - & 0 & 0 & 1 & 0 & 1 & - & 1 & - & 1 & - \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & - & 0 & 1 & 1 & 1 & - & - \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & - & - & - & 1 & 0 & 1 & - & - & 1 \end{array}\right)$$

more open problems in weighing matrices

- The existence of $W(4k, 4k)$ is the Hadamard conjecture but also for $w < n$ the existence of $W(n, w)$ is open in general.
- Until 1998 the smallest order weighing matrix that was not known to exist was $W(17, 9)$. In [OM] some of those matrices were found.
- The next weighing matrix whose existance was open after their work was $W(23, 16)$, which was found by our group.
- Other problems in this subject are to find an (anti)symmetric $W(n, w)$. These are considered different problems. Our group found a symmetric $W(23, 16)$.

The work of Koukouvinos and Seberry [KS] on weighing matrices and their application

- A Chemical balance is a two pan balance with no bias. Suppose given n object with true weights $t_j, 1 \leq j \leq n$. Suppose using the pan m times, each time putting few objects on the left hand and few on the right, and measuring the balanced results $b_i, 1 \leq i \leq m$. Let $W_{m \times n}$ be the matrix (weighing design) that describes the experiment where $w_{i,j} = 1$ if in the i^{th} experiment the j^{th} object was placed on the left hand, $w_{i,j} = -1$ if the j^{th} object was placed on the right hand and $w_{i,j} = 0$ if the j^{th} object did not participate.
- One would expect the equality $b = Wt$. Assume also that there are errors caused in the measurements expressed in an error vector $e = e_m$ which is a random variable with mean value 0 and covariance $\sigma^2 I_m$, then the true equality becomes $b = Wt + e$.

The work of Koukouvinos and Seberry [KS] continued

- In Theorem 6 they prove that for $n \leq m$, chosing the matrix W to consist of n columns of a Hadamard matrix of order m would give an optimal design for the chemical weighing experiment, meabing that the error e will be minimal.
- In the case that there is a restriction on the weighing pan, and it is not possible to weigh more than w objects simultanously, then it follows that the optimal weighing design becomes a weighing matrix as defined above $W(m, w)$
- Another usage of weighing matrices is for optical multiplexing, which essentially is the previous setup, except that t_j measures intensity of light from the j^{th} source of light, and $w_{i.j} = 1, 0, -1$ if in the i^{th} experiment called mask, the j^{th} source is transmitting absorbing or reflecting light.
- They also found some new weighing matrices.

The work of Harada and Munemassa [HM] on weighing matrices and their application

- Given a weighing matrix $W(n, w)$ and an integer m dividing w, interpret any element as an elements of $\mathbb{Z}_m$, then each row of W defines and element in $\mathbb{Z}_m^n$, and all of W defines the span of all rows, which is a submodule of $\mathbb{Z}_m^n$. All rows are still pairwise perpendicular and non zero. Using the definition $WW^t = wI = 0$ it follows that for every prime p which divides m rank $(W \otimes \mathbb{Z}_p) \leq n/2$; so that the rows of W span a true submodule of $\mathbb{Z}_m^n$.
- Any submodule of $\mathbb{Z}_m^n$ is called a code. The code generated by W is self orthogonal because every word is prpendicular to any other. It can serve as a generating matrix for a linear process encoding messages of length $rank(W)$ over $\mathbb{Z}_m$ to messages of length n.
- Known classifications of orthogonal codes are used in this paper to find some new weighing matrices.

Hadamard equivalence

- A monomial matrix (signed permutation) is a permutation matrix whose non zero elements are ± 1. The set of all monomial matrices is denoted $Mon(n, n)$.
- An Hadamard operation on a matrix A, is applying signed paermutations, one on the rows and one on the columns.
- Two matrices are Hadamard equivalent if one is obtained from the other by an Hadamard operation.
- An open problem is to find if two $W(n, w)$ are Hadamard equivalent or to classify all the possible classses for $W(n, w)$.
- All Hadamard matrices of order n with $n \leq 12$ have one Hadamard equivalence class. There are 5 Hadamard equivalence classess of Hadamard matrices of order 16, 3 for n=20 and 60 for n=24

Results of Eliyahu and Kervaire and of Craigen

- Shalom Eliyahu and Michel Kervaire solved Hadamard conjecture modulo 32 [EK].
- They proved that for every $n \in \mathbb{N}$ there is a ± 1 matrix H_{4n} so that $HH^T = 4nI_{4n}\%32$.
- Craigen [C] solved Hadamard conjecture for $2^t p$ given a prime p, for sufficiently large t.
- For every prime p, there is a number t such that there is a Hadamard matrix of order $2^t p$, where $t \leq 2N$ where N is the number of 1 digits in the binary expansion of p, and $t \leq 4\lceil \frac{1}{6} log_2(\frac{p-1}{2}) \rceil + 2$.

Extension of Payley's construction to weighing matrices

- Given a set of $n \times n$ matrices $G_i, 1 \leq i \leq m$, the set is called amicable [W] if $\forall i, j, 1 \leq i, j \leq m$ it holds that $G_i G_j^T = G_j G_i^T$ or equivalently $G_i G_j^T$ is symmetric.
- The set will be called antiamicable if $\forall i, j, 1 \leq i, j \leq m$ it holds that $G_i G_j^T = -G_j G_i^T$ or equivalently $G_i G_j^T$ is antisymmetric.
- A set of μ_2^* matrices will be called disjoint if $\forall i, j, 1 \leq i \neq j \leq m$, the Hadamard (componentwise) product of G_i and G_j is the zero matrix and $\sum_{i=1}^{m} G_i$ is a ± 1 matrix.
- Loosely speaking being disjoint means that the supports of those matrices form a decomposition of all the entries of the square matrix of length m.

Extension of Payley's construction to weighing matrices-contined

- Payley construction for the case $q = 1\%4$ can be extended to the construction of weighing matrices as follows. Given disjoint matrices $A \in W(n, w_1)$ and $B \in W(n, w_2)$, if A and B are amicable, then the matrix

$$\begin{pmatrix} A+B & A-B \\ A-B & -A-B \end{pmatrix}_{2n}$$

  is in $W(2n, 2(w_1 + w_2))$,
- If A and B are antiamicable, the matrix $A + B$ is in $W(n, w_1 + w_2)$.
- These two constructions become the Payley Hadamard matrices, because in the $q = 1\%4$ case it holds that I commutes with C defined above, and for $q = 3\%4$ I still commutes with C which is antisymmetric and thus the pair is also antiamicable.

More relationship between Hadamard and weighing matrices

- Four square $n \times n$ ± 1 matrices A, B, C and D are called of Williamson type if they satisfy the equation $AA^T + BB^T + CC^T + DD^T = 4tI_t$ and are amicable.
- [Xi] found more relationship between Hadamard and weighing matrices. He considered four $n \times n$ matrices of Williamson type which satisfy some additional commutativity conditions.
- Then there exist two disjoint $W(2n, n)$ matrices and 4 disjoint $W(4n, n)$ matrices.
- There is a family of natural numbers N defined so that there exist two disjoint $W(2N, N)$ matrices and 4 disjoint $W(4N, N)$ matrices.
- There is a number m defined so that there is an Hadamard $4nm$ matrix.

Williamson construction

- The usage of Payley's construction yielded Hadamard matrices up to order 88.
- The Payley Hadamard matrices is the densest known family of Hadamard matrices.
- In 1962 a Hadamard matrix of order 92 was found by Baumert, Golomb, and Hall using the Williamson construction.
- The construction in [BH] is now called Baumert Hall construction of Williamson type Hadamard matrices.

Baumert Hall construction of Williamson type Hadamard matrices

- Define the quaternionic group consisting of $G = \pm\{1, i, j, k\}$ with the product of the quaternions.
- There is a presentation of G into $GL(\mathbb{R}, 4)$ given by mapping $1, i, j$ and k to the matrices,

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

  respectively.
- Given A, B, C and D of Williamson type the matrix $H = \begin{pmatrix} A & -B & C & D \\ B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}$ can be presented using the kronecker tensor product $H = 1 \otimes A + i \otimes B + j \otimes C + k \otimes D$. .

Baumert Hall construction of Williamson type Hadamard matrices-continued

- Then H is an Hadamard matrix of order $n = 4t$.
- There is a prentation of $\mathbb{S}^0 \hookrightarrow GL(\mathbb{R}, 2)$ by

$$\overline{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \overline{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

.

- Using the above define the following square $2t$ matrices $\alpha = \overline{1} \otimes A + \overline{-1} \otimes B, \beta = \overline{1} \otimes A - \overline{-1} \otimes B, \gamma = \overline{1} \otimes C + \overline{-1} \otimes D$, $\delta = \overline{1} \otimes C - \overline{-1} \otimes D$.
- Applying the above construction with $\alpha, \beta, \gamma, \delta$ replacing A, B, C, D respectively, gives an Hadamard matrix of order $2n$.
- Repeating this process gives a family of Hadamard matrices of orders $2^k n$.

(back) circulant matrices

- Define a permutation on $\mathbb{Z}_n$ by $\sigma : x \to x + 1\%n$. Let P be the permutation matrix acting on the set $\{1, \cdots n\}$ by σ.
- A matrix A is called circulant if it satisfies that $PAP^T = A$. This means that the terms of A are fixed on the diagonals $\%n$ that are parallel to the main diagonal.
- A is called back circulant if it satisfies that $PAP = A$, meaning that the terms are fixed on the backdiagonals $\%n$.
- Let R is the permutation matrix with 1 digits on the back diagonal and 0 digits elsewhere, or equivalently constructed like P above from the permutation $i \to (n+1) - i, \forall i, 1 \leq i \leq n$.
- If A is circulant then AR and RA are back circulant and if A is back circulant then AR and RA are circulant.

Goethals and Seidel construction of Williamson type Hadamard matrices

- Given 4 circulant square ± 1 $n \times n$ matrices A, B, C and D such that $AA^T + BB^T + CC^T + DD^T = 4nI_n$ then the following matrix is an Hadamard matrix.

$$\begin{pmatrix} A & BR & CR & DR \\ -BR & A & -D^TR & -C^TR \\ -CR & D^TR & A & -B^TR \\ -DR & -C^TR & B^TR & A \end{pmatrix}$$

- Similarly to the Payley construction, the constructions in [BH] and in [GS] can be extended to weighing matrices.

Classifying Hadamard equivalence classes of some weighing matrices

- Chan Rodger Sebery classification. [CRS] classified (up to Hadamard equivalence) all weighing matrices of weight $w \leq 5$ and all weighing matrices of order $n \leq 11$. They used what is called in Assaf's paper [G] the support geometry.
- Harada Munemasa classification [HM] they classify all weighing matrices of order $n \leq 15$, $n = 17$ and all $W(16, w), w = 6, 9, 12$ and $W(18, 9)$. For example they found 11891 classes of $W(18, 9)$
- In [S] Strassler found all equivalence classes of circulant weighing matrices of weight 9. This appeared later in [AAMS]. It turns out that the order must be a multiple of either 13 or 24.
- In [AES] all Circulant Weighing Matrices of Weight 16 and Odd Order are classified. It turns out that the order must be an odd multiple of either 21 or 31.

online sites of open and solved problem

There are on line sites with tables of open or of recently found results. The book Handbook of Combinatorial Designs edited by Chales J Colbourn and by Jefferry H. Dinitz has 89 sections in its second edition. [SD].
The site of Akihiro Munemassa [SM] has a link to new unpublished weighing matrices

A page from [SD]

Figure: Table of (un)known weighing matrices

n =68, 72, and all subsequent even numbers, but is unresolved for $n = 70$. In places "$\ldots 2k, (2k+1)\ldots$" is used to indicate that all even orders in the indicated range are known, while all odd orders are unresolved; similarly, "$\ldots 4k, (4k+2)\ldots$" indicates that orders $\equiv 0 \pmod 4$ are known but those $\equiv 2 \pmod 4$ are unresolved.

2.85 **Table** $W(n, w)$, $w = a^2 \leq 256$ (all n admissible).

w	n
1	1...
4	4,6,7,8,10...
9	10,12...
16	16,18,20,21,22,(23),24,(25),26,(27),28,(29),30...
25	26,28,30...34,(35)...$2k$, $(2k+1)$...54...
36	36,38,40,42,44,(45)...$2k$,$(2k+1)$...56,(57,58,59),60,(61),62,63,64,(65),66,(67), 68,(69),70,(71),72...
49	50,52,54,56,57,(58,59),60,(61,62,63),64,(65,66,67),68,(69,70,71),72,(73,74,75),76, (77),78,(79),80,(81,82,83),84,(85,86,87),88,(89,90,91),92,(93,94,95),96,(97)...$2k$, $(2k+1)$...104...114, (115), 116, 117, 118, (119), 120, 121, 122, (123), 124, 125, 126, (127), 128, 129, 130, (131), 132...138, (139), 140, 141, 142, (143), 144...150, (151), 152...
64	64,66,68,70,72,73,74,(75)...$2k$, $(2k+1)$...116...
81	82,84,(86),88,90,91,92,(93,94,95),96,(97,98,99),100,(101,102,103),104,(105,106, 107),108,109,110,(111),112,(113,114,115),116,117,118,(119),120,121,122,(123), 124,(125),126,127,128,(129),130...
100	100,(102),104,(106),108,110,112,(113)...$2k$, $(2k+1)$...186

our contribution to the subject

- In the last 3 years our group was able to solve 6 weighing matrices stated as open in the handbook. 5 of those are publishable.
- These are the $W(23, 16)$ and symmetric $W(14, 9)$ which were solved by the mathod we called the shadow geometry,
- Symmetric $W(23, 16)$ which was solved by the method we called code invariant,
- $W(25, 18)$, $W(27, 16)$ and $W(29, 16)$ which were solved by a method we called tiling design.

Weight 16 is fully resolved

- We remark that after we solved the symmetic $W(14, 9)$ we found out that it was actually solved long ago in the paper by Chan Rodger and Seberry [CRS] and we wrote to the handbook asking to remove this result.
- Also we remark that in the method of tiling design we found a $W(23, 16)$ that is not Hadamard equivalent to the $W(23, 16)$ found by the geometry method.
- For a given weight $w = k^2$, it is known that $W(n, w)$ exists for sufficiently large n. Therefore, there can be only finitely many open cases. In the table (Figure 1), all open cases are surrounded in parentheses. Looking at the table, we see that today the case of weight 16 is fully resolved.

The shadow geometry method

- Today we would like to discuss the shadow geometry method, and will deonstrate it using an example.
- The following $W(7,4)$ (from Wikipedia) was found long ago:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & -1 & 0 & -1 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 & -1 & -1 \\ 0 & 1 & -1 & 0 & 0 & 1 & -1 \\ 0 & 1 & 0 & -1 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 & -1 & 1 & 0 \end{pmatrix}$$

$W(7,4)$ as an An example

- Let us take the absolute value componentwise and get the matrix we call the support geometry PG defined by $\forall 1 \leq i,j \leq n, PG_{i,j} = w_{i,j}^2$.
- We define the shadow geometry by $\forall 1 \leq i,j \leq n, DG_{i,j} = 1 - PG_{i,j}$.

$$DG = J - PG = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Support and Shaddow geometries

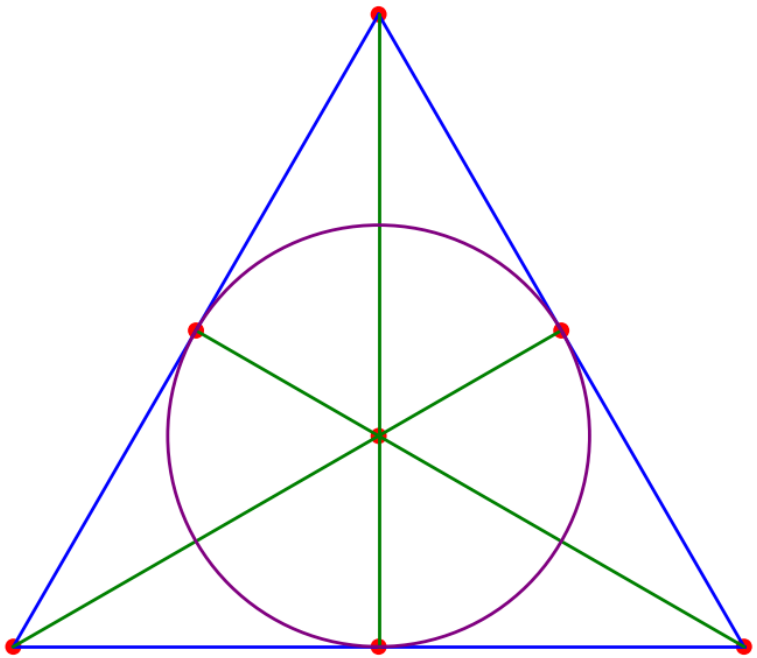
- The reason for the name geometry is that for DG this is an incidence matrix between a geometry with 7 points and 7 lines (The Fano Plane).
- There are also the dual geometries, induced by the transpoe matrices.
- We also remark thet generally, there might be several different rows having the 1 digits in the same columns, so that the collection of lines is in fact a multisetL.
- We call DG the Shaddow Geometry and PG the supposrt Geometry.

philology of the word geometry

- As in the PG every line is determined by its points, the same holds for DG. In this case, DG is the incidence matrix of the well known Fano plane (Figure 2)
- Take a prime p and $q = p^n$ and $F = GF(q^n)$. Denote $\mathbb{F}P$ The projective plane of F.
- $\mathbb{F}P$ has $\frac{q^3-1}{q-1} = q^2 + q + 1$ lines and points. Any line has $q + 1$ points, and every point is included in $q + 1$ lines. Every two lines intersect at a single point, and every two points lie in a single line.
- There is a weighing matrix $W(q^2 + q + 1, q^2)$. The DG of this weighing matrix is the incidence matrix of $\mathbb{F}P$.
- For $p = n = 2$ the DG obtained is the Fano plane mentioned above. This is the reason Assaf [G] chose the name 'geometry' for $|W|$

The Fano Plane

Figure: Fano's plane



Local support and shaddow geometries

- PG was used in [CRS], to classify all weighing matrices with weight not exceeding 5 and also all weighing matrices with order not exceeding 11, and DG was defined in [G].
- The idea is that for $W(23, 16)$ it is easier to deal with arrangements of $n - w = 7$ digits, rather than with $w = 16$ digits.
- Given the incidence matrix of any geometry, one may choose any line, called base line, and consider only the columns (points) in the support of this line and restrict to them, obtaining the so called the associated local geometry.
- For PG one obtains an $w \times n$ incidence submatrix of the Local Support geometry LPG
- For DG one obtains the $(n - w) \times n$ incidence matrix of the Local Shadow Geometry LDG.

Local support and shaddow geometries

- For example, using the first line of the shadow geometry above the following incidence matrix for the above shadow geometry is obtained

$$LDG(top - line) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- We define the type of the local geometry. Suppose that we have a local geometry matrix of order $m \times n$. Then the type is a list of indices $z_i, 0 \leq i \leq m$ presenting the number of lines intersecting the baseline with i intersection points.

The type of the LG

- Claerly it must hold that $\sum_{i=1}^{m} z_i = n - 1$. For example the above local geometry has 6 lines intersecting the baseline with 1 point.
- It should be emphasized that the type is a weaker invariant than the local geometry, for example the following local geometry matrix is different than the previous one but has the same type

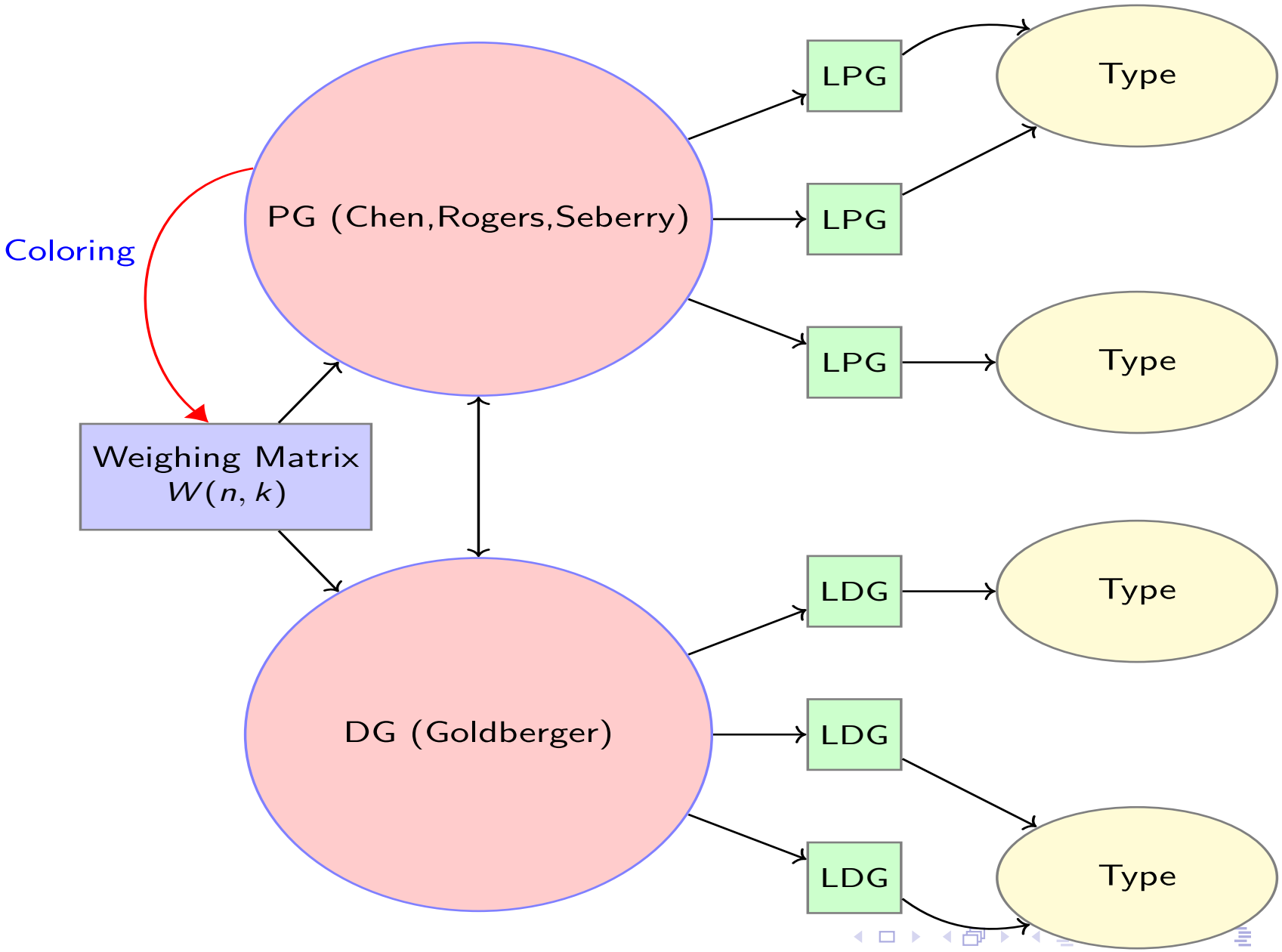
$$LDG2(top - line) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

The list of types

- The z_i are natural numbers that satisfy the equations $\sum_{i=1}^{m} z_i = n - 1$ and $\sum_{i=1}^{m} iz_i = (n - w)(n - w - 1)$.
- It follows that a finite list of all possible types can be found.
- This constitutes the stage where the necessary conditions for the existence of W may become sufficient conditions that can be used to build W.
- It may be inferred from the above equations that in the $W(23, 16)$ shadow geometry, every line has at least 10 lines intersecting it at exactly one point. This seemed at first too big to fit into a space of 23 points. Therefore we conjectured at first that $W(23, 16)$ does not exist.

.

A Schematic Diagram



Ruling out some types

- There were 14 different types for $LDG(23, 16)$ some of them could immidiatly be ruled out.
- For example the type $z_7 = 3, z_3 = 1, z_1 = 18$ satisfies the true necessary equations, but fails to satisfy another condition for $LDG(23, 16)$ that every pair of points have an odd number of lines on which they all lie.
- The three lines intersecting the base line with 7 points, together with the top line itself, give the following submatrix:

$$LDG(23, 16) = \begin{pmatrix} (base - line) & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ (z_7 = 1) & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ (z_7 = 2) & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ (z_7 = 3) & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \dots & & & & & & & \\ \dots & & & & & & & \end{pmatrix}$$

in which every pair of points lies on 4 lines.

Chosing the type

- Thus the bottom part of $LDG(23, 16)$ which is yet to be determined, must satisfy the parity condition. $z_1 = 18$ gives 18 lines that do not contribute to the pairs of points in the same line.
- Since one can not spread out a triple of points, so that any of the $\binom{7}{2}$ possible pairs of points will lie on an odd number of lines, this type can not support a local geometry.
- Eventually after a lot of trials, the type $z_7 = 2, z_3 = 4, z_1 = 16$ was chosen with a local geometry it supports. The same local geometry was set for the dual geometry. It filled the DG matrix except for a 16×16 core to give the picture:
- $$DG(23, 16) = \begin{pmatrix} 7 \times 7 - intersection & dual - lg & dual - lg \\ lg & 16 \times 16 - core & 16 \times 16 - core \\ lg & 16 \times 16 - core & 16 \times 16 - core \end{pmatrix}$$

Chosing the type

$$reish = \left(\begin{array}{cccc|cccc|cccc|cccc|cccc|cccc}
1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
\hline
1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0\\
1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0\\
1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1\\
\hline
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{array}\right)$$

filling the core

- It so happens that the 16×16 core must be a tiling design of 4×4 tiles each of which is 4×4 digits.
- Each row or column in each tile may have 3 or 1 digits, so any tile may have 4, 6, 8, 10 or 12 digits.
- The 4 and 12 tiles can be paired as disjoint matrices. There are 24 paired disjoint $T4, T12$.
- Similarly there are more than 24 pairs of $T6 - T10$. There are two different hadamard equivalence classes of T6, and of T10, so that one can not permute one type of T6 to the other.
- All $T8$ are paired with themselves. Assaf chose a canonical representative of each tile, denoted CTi for $i = 4, 6, 8, 10, 12$.
- Eventually two full non isomorphic shadow geometries based on the type $z_7 = 2, z_3 = 4, z_1 = 16$ both for the usual and dual geometries were discovered

the two cores

- The tiling of the first core

$$1core - DG(23,16) = \begin{pmatrix} CT12 & CT4 & CT4 & CT4 \\ CT4 & T12 & T4 & T4 \\ CT4 & T4 & T12 & T4 \\ CT4 & T4 & T4 & T12 \end{pmatrix}$$

- the tiling of the second core

$$2core - DG(23,16) = \begin{pmatrix} CT12 & CT4 & CT4 & CT4 \\ CT4 & T8 & T8 & T4 \\ CT4 & T8 & T4 & T8 \\ CT4 & T4 & T8 & T8 \end{pmatrix}$$

A doubly indexed family of geometries

- consequently we were able to extend the first geometry to an infinite family of geometries.
- Let k be a natural number, $m = 2^k$, $w = m^2$, $n = w + m + 1 + i(m-2), 0 \leq i \leq m$. For every k and i so that $0 \leq i \leq m = 2^k$, there is a shadow geometry for $W(n, w)$.
- The core consists of a design with $\sqrt{w} \times \sqrt{w}$ tiles, each tile with dimension $\sqrt{w} \times \sqrt{w}$, and of two kinds $T(\sqrt{w})$ and $T(w - \sqrt{w})$.
- For the particular case that k=2,m=4,w=16,i=1,n=16+4+1+1 $\cdot 2 = 23$, the core has 4×4 tiles of dimension 4×4 and each one is either $T4$ or $T(16-4)$, yielding the firsly found geometry.

coloring

- The geometry that corresponds to $i = 0$ is the honest to god geometry of a projective plane formed from the Galois field of 2^k elements. The case of $k = 2$ and $i = 1$ is the geometry (of only T(4) and T(12)) that was found for $W(23, 16)$.
- The shadow geometry determines a support geometry. We call the process of passing from the support geometry to the full W 'coloring'. The only W we were able to color (which is truely unknown) was $W(23, 16)$, using the geometry with only $T4$ and $T12$.

coloring

- The stages of the coloring were the following. The top three rows had 16 1 digit in the same location. We colored them as the top three rows of a standard H_{16} matrix.
- This means that the top row is colored to be all $+1$. The second row is colored so that the first 8 digits are $+1$ and the last 8 digits are colored with -1. The third row is colored with 4 blocks of 4 digits, the first 4-tupple is colored with $+1$, the second with -1 and then $+1$ and then -1.
- This coloring is the one used in the standard proof that if an Hadamard matrix H_n exists, and $2 < n$, then n is divisible by 4.

Our specific W in $W(23, 16)$

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - & - & - \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & - & - & - & - & 1 & 1 & 1 & 1 & - & - & - & - \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & - & 1 & 1 & - & - & 1 & - & 1 & - & 1 & 1 & - \\
0 & 0 & 0 & - & - & 1 & 1 & 1 & - & - & 1 & 0 & 0 & 0 & 0 & - & 1 & - & 1 & 1 & - & - & 1 \\
0 & 0 & 0 & 1 & - & 1 & - & 1 & - & 1 & - & - & 1 & - & 1 & 0 & 0 & 0 & 0 & - & 1 & - & 1 \\
0 & 0 & 0 & - & 1 & 1 & - & - & 1 & 1 & - & 1 & - & - & 1 & - & 1 & - & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & - & - & 1 & 0 & 0 & 0 & 0 & 1 & - & - & 0 & - & - & 1 & 0 & - & 1 & 1 \\
1 & 1 & 1 & 0 & - & 1 & 1 & 0 & 1 & 0 & 0 & - & 0 & - & 1 & 1 & 0 & - & - & 1 & 0 & 1 & - \\
1 & 1 & 1 & 0 & - & - & 1 & 0 & 0 & 1 & 0 & 1 & - & 0 & - & - & 1 & 0 & - & - & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & - & 0 & 0 & 0 & 1 & - & - & 1 & 0 & - & - & 1 & 0 & 1 & 1 & - & 0 \\
1 & 1 & - & 1 & 0 & - & 1 & 0 & - & 1 & - & 0 & 0 & 0 & 1 & - & 0 & 1 & 1 & 1 & - & 0 & - \\
1 & 1 & - & - & 0 & 1 & - & 1 & 0 & - & - & 0 & 0 & 1 & 0 & 0 & 1 & 1 & - & - & - & 1 & 0 \\
1 & 1 & - & - & 0 & - & - & - & - & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & - & 0 & 0 & 1 & - & - \\
1 & 1 & - & 1 & 0 & 1 & 1 & - & 1 & - & 0 & 1 & 0 & 0 & 0 & 1 & - & 0 & 1 & - & 0 & - & 1 \\
1 & - & - & - & 1 & 0 & 1 & 0 & 1 & 1 & - & - & 1 & 0 & - & 0 & 0 & 0 & - & 1 & 0 & - & 1 \\
1 & - & - & 1 & - & 0 & - & - & 0 & 1 & 1 & - & - & 1 & 0 & 0 & 0 & - & 0 & 0 & - & 1 & 1 \\
1 & - & - & - & 1 & 0 & 1 & 1 & - & 0 & 1 & 0 & - & - & 1 & 0 & - & 0 & 0 & - & 1 & 1 & 0 \\
1 & - & - & 1 & - & 0 & - & 1 & 1 & - & 0 & 1 & 0 & - & - & - & 0 & 0 & 0 & 1 & 1 & 0 & - \\
1 & - & 1 & - & - & 1 & 0 & 0 & - & 1 & - & 1 & 0 & 1 & - & 1 & - & 0 & 1 & 0 & 0 & 0 & - \\
1 & - & 1 & 1 & 1 & - & 0 & 1 & 0 & - & - & 0 & - & 1 & 1 & 1 & 1 & - & 0 & 0 & 0 & - & 0 \\
1 & - & 1 & 1 & 1 & 1 & 0 & - & - & 0 & 1 & 1 & 1 & - & 0 & 0 & 1 & 1 & - & 0 & - & 0 & 0 \\
1 & - & 1 & - & - & - & 0 & - & 1 & - & 0 & - & 1 & 0 & 1 & - & 0 & 1 & 1 & - & 0 & 0 & 0
\end{pmatrix}$$

http://www.emba.uvm.edu/ jdinitz/hcd/W2316.txt

coloring

- There is the submatrix of the support geometry in rows 4 throu 7 and columns 4-7 . This submatrix has no 0 digits. Then it was conjectured that this is a subHadamard H_4 matrix.
- Thus, all the rest of the one digits of rows 4-7 are in columns 8-23, and the submatrix of W which consists of rows 1-7 and columns 8-21 must stisfy that non identical rows are perpendicular. Rows 1-3 were already colored to be perendicular to one another.
- Thus we can enumerate on the 12 digits of each row 4-7. The first digit can be colored to be $+1$, and the fact that this row has to be perpendicular to rows 1-3, leaves about 10 candidates for each row 4-7. From this it is easy to determine all possible simultaneous colorings for rows 4-7.

coloring

- For any such colored 7 top rows of the geometry, one can find all possible colorings of each row 8-23.
- On the average there are 200 solutions for each such row.
- We define a graph of about 3200 vertices. Each vertex presents a colored row of rows 8-23 which is perpendicular to rows 1-7. Join two rows if they present different rows and are colored to be perpendicular to one another.
- One only needs to find a clique of 16 vertices to complete the coloring and this was found after 11 atempts.

bibliography

- I. S. Kotsireas, C. Koukouvinos, J. Seberry , New weighing matrices constructed from two circulant submatrices,
- R. M. Adin, L. Epstein and Y. Strassler, The Classification of Circulant Weighing Matrices of Weight 16 and Odd Order https://arxiv.org/abs/math/9910164
- M. H. Ang, K.T.Arasu, S. L Ma and Y. Strassler Study of proper circulant weighing matrices with weight 9 Discrete Mathematics Volume 308, Issue 13, 6 July 2008, Pages 2802-2809 http://www.sciencedirect.com/science/article/pii/S0012365X070041
- Hadamard Matrices of the Williamson Type by L. D. Baumert and M. Hall, Jr. Journal of Combinatorial Theory, Series A Volume 14, Issue 3, May 1973, Pages 334-340 http://www.ams.org/journals/mcom/1965-19-091/S0025-5718-1965-0179093-2/S0025-5718-1965-0179093-2.pdf

bibliography

- I. Bengtsson, Three ways to look at mutually unbiased bases https://arxiv.org/abs/quant-ph/0610216
- H.C. Chan, C.A. Rodger and J. Seberry, On inequivalent weighing matrices, Ars Combin. 21 (1986), 299333. https://www.uow.edu.au/ jennie/WEBPDF/107_1986.pdf http://ro.uow.edu.au/infopapers/1022/
- C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs, Second Edition*, Taylor and Francis 2006,ISBN-13: 978-1584885061
- A. Craigen Signed groups, sequences, and the asymptotic existence of Hadamard matrices Journal of Combinatorial Theory, Series A Volume 71, Issue 2, August 1995, Pages 241-254 https://www.sciencedirect.com/science/article/pii/009731659590002

bibliography


M. Kervaire and S. Eliyahu A survey on modular Hadamard matrices Morfismos, Vol. 7, No. 2, 2003, pp. 1745 http://morfismos.cinvestav.mx/Portals/morfismos/SiteDocs/Articulo and Discrete Mathematics Volume 302, Issues 13, 28 October 2005, Pages 85-106 https://ac.els-cdn.com/S0012365X05002918/1-s2.0-S0012365X05002918-main.pdf?_tid=2469d5fc-fd27-11e7-8091-00000aacb360&acdnat=1516373202_360f6341b51702df59fa1dafe8bd


Goethals and Seidel Orthogonal matrices with zero diagonals Can. Jout of Math 19 1967 1001-1010 http://mathscinet.ru/files/GoethalsSeidel.pdf


A. Goldberger, On the finite geometry of $W(23, 16)$, http://arxiv.org/abs/1507.02063.


M. Harada and A. Munemasa On the Classication of Weighing Matrices and Self-Orthogonal Code,

bibliography


C. Koukouvinos and J. Seberry, Weighing matrices and their applications, *JSPI*, 62 (1997) 91-101. http://ro.uow.edu.au/cgi/viewcontent.cgi?article=2156&context=inf


H. Ohmori and T. Miyamoto Construction of Weighing Matrices W(17, 9) Having the Intersection Number 8 Designs, Codes and Cryptography December 1998, Volume 15, Issue 3, pp 259269


Y. Strassler, The classification of circulant weighing matrices of weight 9, Ph.D. Thesis, Bar-Ilan University, Israel, 1998


The site of Jeff Dinitz -content of the second edition of the book Handbook of Combinatorial Designs edited by Chales J Colbourn and by Jefferry H. Dinitz the table of content http://www.emba.uvm.edu/ jdinitz/contents.html. New weighing matrices http://www.emba.uvm.edu/ jdinitz/part5.newresults.html

bibliography

- The site of Akihiro Munemassa http://www.math.is.tohoku.ac.jp/ munemasa/index-e.html has a link to new unpublished weighing matrices http://www.math.is.tohoku.ac.jp/ mune-masa/research/matrices/wo.htm
- J. Seberry (Wallis) On Hadamard Matrices Journa of Combinatorial Theory (A) 18, 149-164 (1975)
- Hadamard matrix wikipedia https://en.wikipedia.org/wiki/Hadamard_matrix
- Mutually unbiased bases https://en.wikipedia.org/wiki/Mutually_unbiased_bases
- Wikipedia complex Hadamard matrices https://en.wikipedia.org/wiki/Complex_Hadamard_matrix

bibliography


William Cherowitzo Hadamard matrices and designs
http://math.ucdenver.edu/ wcherowi/courses/m6406/hadamard.pdf
s


M. Xia Some Infinite Classes of Williamson Matrices and Weighing Matrices The Australasian Journal of Combinatorics
https://ajc.maths.uq.edu.au/pdf/6/ocr-ajc-v6-p107.pdf
historical bibliography
http://sites.math.rutgers.edu/ zeilberg/Opinion75.html
http://www.eoht.info/page/Greatest+mathematician+ever

Keywords: weighing matrix, geometry, local geometry

Appendix to Applications to quantum random access codes

- In quantum mechanics a Physical state is presented by a normalized L^2 function $\psi : X \to \mathbb{C}$.
- An observable on the space of states is a Hermitian operator M on $L^2(X, \mathbb{C})$. A measurment is a physical operation applied to M that assigns to M an eigenvector v_i and its eigenvalue λ_i of M.
- The probability to measure (v_i, λ_i) is given by $| < \psi | v_i > |^2$.
- The expected value of the measurment is $E(M) = \psi \to \int_X \psi M \psi^* dx =< \psi, M, \psi >$.

Applications to quantum random access codes

- M has an orthonormal eigenbasis presentation $M = \sum \lambda_i |v_i><v_i$ with real eigenvalues λ_i. The Copenhagen interpretation is that the measurement cause ψ to collapse to one eigenvector.
- If M_1 and M_2 commute then there is a common eigenbasis so that each one has a presentation with respect to this common basis. If M_1 and M_2 do not commute, one can not measure both measurements simultaneously, we get Heisenberg uncertainty principle.
- If H_1 and H_2 do not commute, there is still a favorable relationship beteen them which called Mutually unbiased bases (of the correspondive Hermitian operators).
- In this case the second measurement is independant of the first one in the sense that knowing the value of the first gives no knoledge of the second measurement.