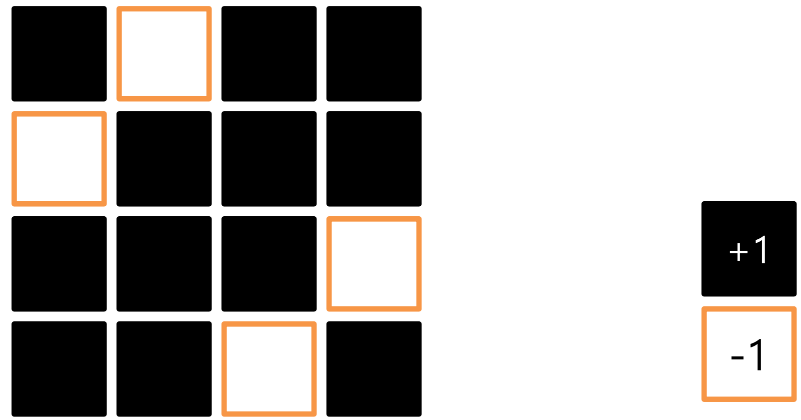
Eigenvalues and eigenvectors of Paley-type Hadamard matrices

Hong-Yeop Song

Yonsei university

KICS-NA 2017, Feb. 10-11.

Hadamard Matrix



DEFINITION.

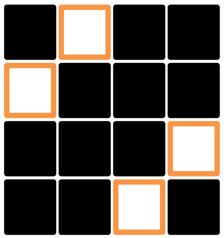
Let n be a positive integer. A Hadamard matrix H of order n (or, size $n \times n$) is an $n \times n$ matrix with all entries +1 or -1 such that

$$H\,H^T = nI,$$

where I is the $n \times n$ identity matrix.

Some Well-known Types

circulant

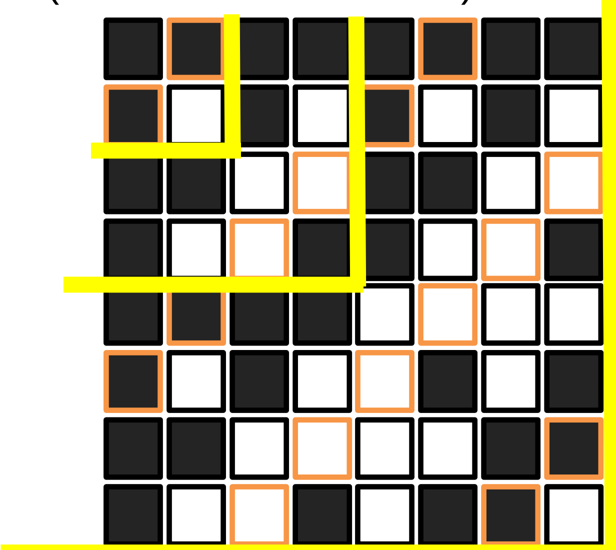


Only for n=4 ??
True for n up to 548 Million

Walsh-Hadamard

(Sylvester)
(Kronecker Product)

For all $n=2^t$



Special case of **Paley-type**

cyclic type

+	+	+	+	+	+	+	+	+	+	+	+
+	−	+	−	+	+	+	−	−	−	+	−
+	−	−	+	−	+	+	+	−	−	−	+
+	+	−	−	+	−	+	+	+	−	−	−
+	−	+	−	−	+	−	+	+	+	−	−
+	−	−	+	−	−	+	−	+	+	+	−
+	−	−	−	+	−	−	+	−	+	+	+
+	+	−	−	−	+	−	−	+	−	+	+
+	+	+	−	−	−	+	−	−	+	−	+
+	+	+	+	−	−	−	+	−	−	+	−
+	−	+	+	+	−	−	−	+	−	−	+
+	+	−	+	+	+	−	−	−	+	−	−

Cyclic Hadamard Conjecture:
For all n such that
n-1 is either
(1) p = 3 mod 4, or
(2) p(p+2), twin primes, or
(3) 2^t -1.
True for all n-1 (=3 mod 4) up to 10,000, except possibly for 7 cases, smallest of which is 3439.

Williamson type

+	+	+	−	+	+	−	+	+	−	+	+
+	+	+	+	−	+	+	−	+	+	−	+
+	+	+	+	+	−	+	+	−	+	+	−
+	−	−	+	+	+	+	−	−	−	+	+
−	+	−	+	+	+	−	+	−	+	−	+
−	−	+	+	+	+	−	−	+	+	+	−
+	−	−	−	+	+	+	+	+	+	−	−
−	+	−	+	−	+	+	+	+	−	+	−
−	−	+	+	+	−	+	+	+	−	−	+
+	−	−	+	−	−	−	+	+	+	+	+
−	+	−	−	+	−	+	−	+	+	+	+
−	−	+	−	−	+	+	+	−	+	+	+

Williamson Conjecture
turns out to be false:
n=4*35=140.

Paley-type Hadamard matrix
exists for all odd prime power q with size
(1) n=q+1 when q ≡ 3 (mod 4)
(2) n=2(q+1) when q ≡ 1 (mod 4)

Notation

- p : an odd prime
- $q = p^k$: an odd prime power
- I_n (or 0_n) : the identity matrix (or the all-zero matrix) of order n
- $\underline{1}_n$ (or $\underline{0}_n$) : the all-one vector (or the all-zero vector) of length n
- $j = \sqrt{-1}$: the imaginary unit
- ω_n : a complex primitive n-th root of unity
- $\Omega_n = \mathrm{diag}(1, \omega_n, \dots, \omega_n^{n-1})$
- F_n : the Fourier matrix of order n
- Z_q : the set of integers modulo q
- $\mathrm{GF}(q)$: the finite field of size q

- **Jacobsthal matrix** Q of order q
- **Paley matrix** C of order $q+1$
- **Paley-type Hadamard matrix** H of order $q+1$ or $2(q+1)$

Paley-type Hadamard matrices from Paley matrices

- Let C be a **Paley matrix** of order $q+1$ where $q = p^k$.

- (Type 1) If $q \equiv 3 \pmod 4$, then

$$C + I_{q+1}.$$

- (Type 2) If $q \equiv 1 \pmod 4$, then

$$H = \begin{bmatrix} C + I_{q+1} & C - I_{q+1} \\ C - I_{q+1} & -C - I_{q+1} \end{bmatrix}.$$

Paley matrices from Jacobsthal matrices

- For a given a **Jacobsthal matrix** Q of order q, a Paley matrix C of order $q+1$ is defined by

$$C = \begin{bmatrix} 0 & \underline{1}_q^T \\ \pm\underline{1}_q & Q \end{bmatrix},$$

where the sign of $\pm\underline{1}_q$ is
    - $+$, if $q \equiv 1 \pmod 4$ so that C becomes **symmetric**
    - $-$, if $q \equiv 3 \pmod 4$ so that C becomes **skew-symmetric**

Jacobsthal matrices

Let Ψ be a **bijective map** from Z_q to GF(q) such that $\Psi(0) = 0$.
Then, a **Jacobsthal matrix** $Q_\Psi = (\sigma_{s,t})$ is a $q \times q$ matrix with

$$\sigma_{s,t} = \chi\big(\Psi(s) - \Psi(t)\big)$$

where χ is the **quadratic character** of GF(q) and we use the convention that $\chi(0) = 0$.

Property of Jacobsthal matrices (I)

- (Definition of Jacobsthal matrices)
  Let Ψ be a bijective map from Z_q to GF(q) such that $\Psi(0) = 0$.
  Then, a Jacobsthal matrix $Q_\Psi = \left(\sigma_{s,t}\right)$ is a $q \times q$ matrix with
  $$\sigma_{s,t} = \chi\left(\Psi(s) - \psi(t)\right)$$
  where χ is the quadratic character of GF(q) and we use the convention that $\boldsymbol{\chi(0) = 0}$.

- **There are $\frac{q-1}{2}$ quadratic residues and $\frac{q-1}{2}$ quadratic non-residues. Therefore,**

$$Q_\Psi \underline{1}_q = \underline{0}_q$$

for any bijective map Ψ.

Property of Jacobsthal matrices (II)

- Let Ψ and Φ be two **bijective maps** from Z_q to GF(q).
  Then, there exists a **permutation** f on GF(q) such that
  $$f\big(\Psi(x)\big) = \Phi(x), \qquad \text{for all} \;\; x \in Z_q$$
  since Ψ and Φ are bijective.
- Therefore, any two **Jacobsthal matrices** Q_Ψ and Q_Φ corresponding to Ψ and Φ, respectively, are related by
  $$Q_\Phi = P_f Q_\Psi P_f^T$$
  where P_f is the permutation matrix of the permutation f on GF(q).
- If $Q_\Psi = S\Lambda S^H$ is the diagonalization of Q_Ψ by S, then,
  $$Q_\Phi = P_f Q_\Psi P_f^T = P_f S \Lambda S^H P_f^T = P_f S \Lambda \big(P_f S\big)^H$$
  is the diagonalization of Q_Φ by $P_f S$.
- **Therefore, it is enough to find eigenvalue decomposition of any one Jacobsthal matrix for the same order.**

The Jacobsthal matrix

- Let α be a primitive element of GF(q).
  We define a map Ψ from Z_q to GF(q) as

$$\Psi(i) = c_0 + c_1\alpha + \cdots c_{k-1}\alpha^{k-1} = \sum_{z=0}^{k-1} c_z\alpha^z ,$$

  where $i = \sum_{z=0}^{k-1} c_z p^z$ is the unique representation with $0 \leq c_z < p$, for $z = 0,1, \ldots, k-1$.

- In the remaining, we denote **the Jacobsthal matrix**, which constructed by using the bijective function Ψ, by Q.

- This map Ψ gives Q an interesting structure, called multi-level circulancy, which we will use.

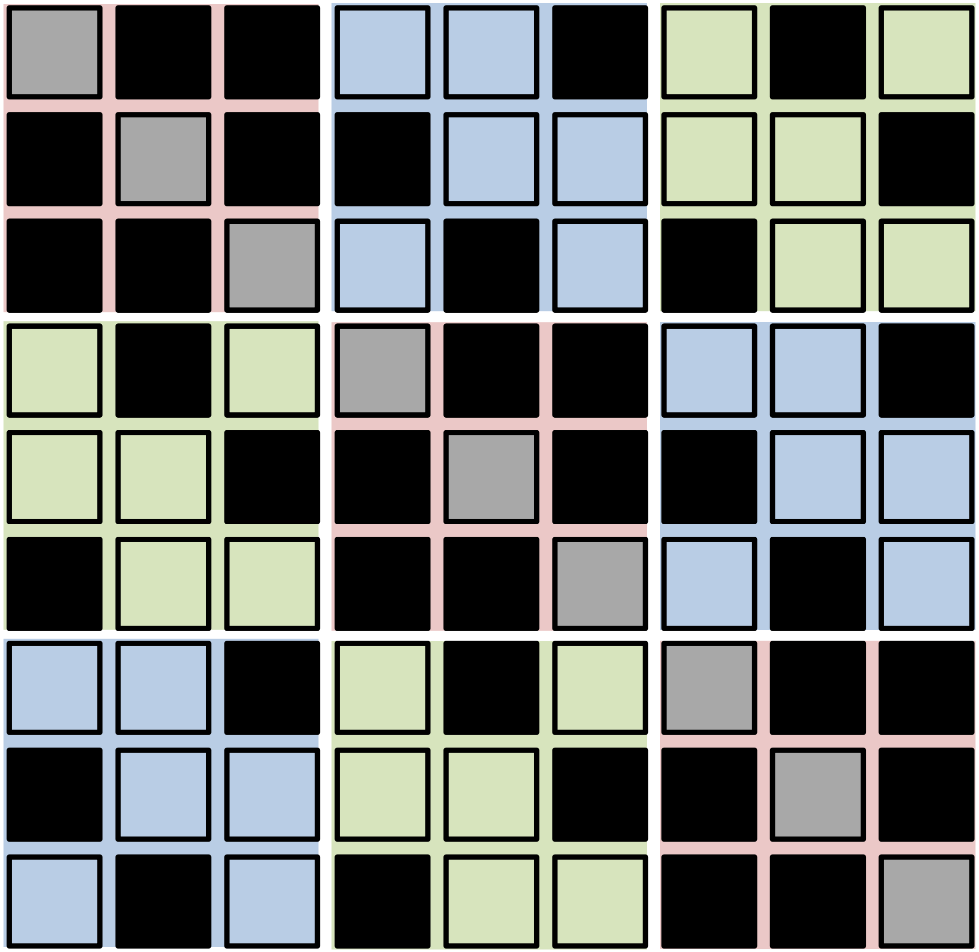
Example

$$Q = \begin{bmatrix} 0 & + & + & - & - & + & - & + & - \\ + & 0 & + & + & - & - & - & - & + \\ + & + & 0 & - & + & - & + & - & - \\ - & + & - & 0 & + & + & - & - & + \\ - & - & + & + & 0 & + & + & - & - \\ + & - & - & + & + & 0 & - & + & - \\ - & - & + & - & + & - & 0 & + & + \\ + & - & - & - & - & + & + & 0 & + \\ - & + & - & + & - & - & + & + & 0 \end{bmatrix}$$

※ Notation

- (grey square) $= 0$
- (white square) $= -$
- (black square) $= +$

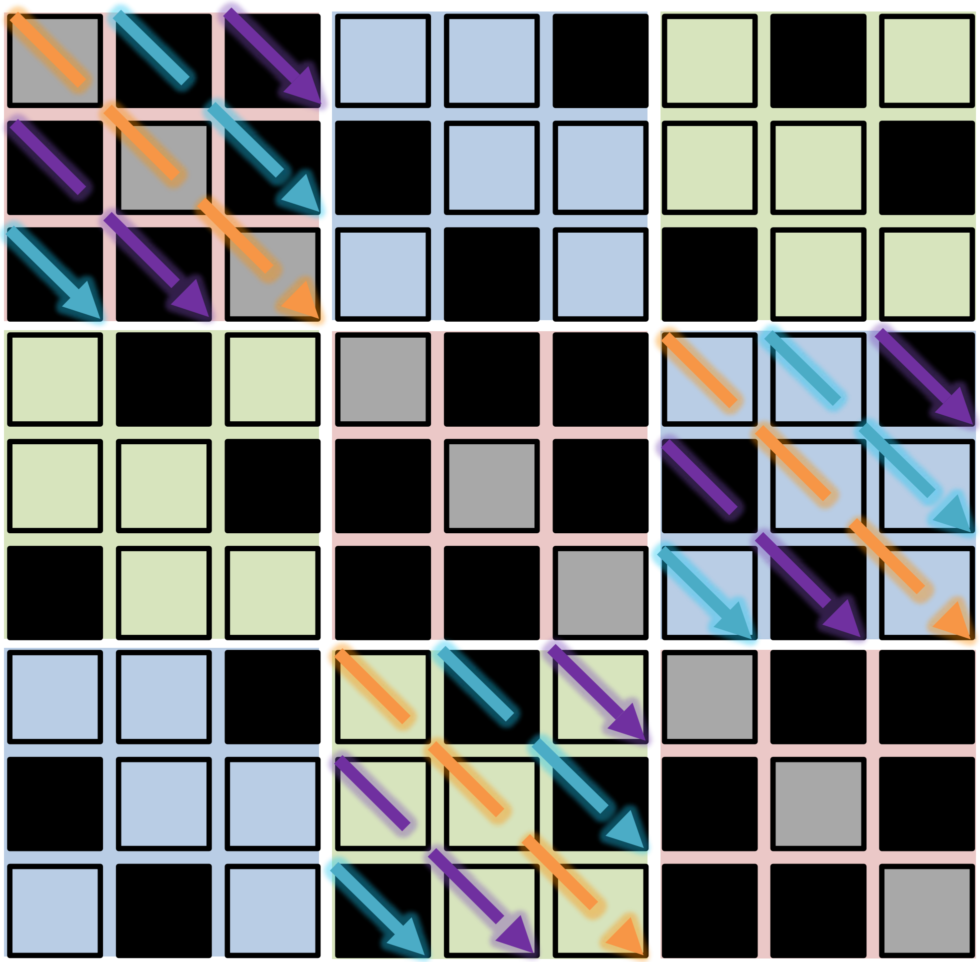
Example



Circulant when we regard the 3×3 block as elements.

$\Rightarrow$ *'Block circulant'*

Example



Each block is circulant.

⇒ *'Block circulant with circulant blocks'*

Property of Jacobsthal matrices (III)

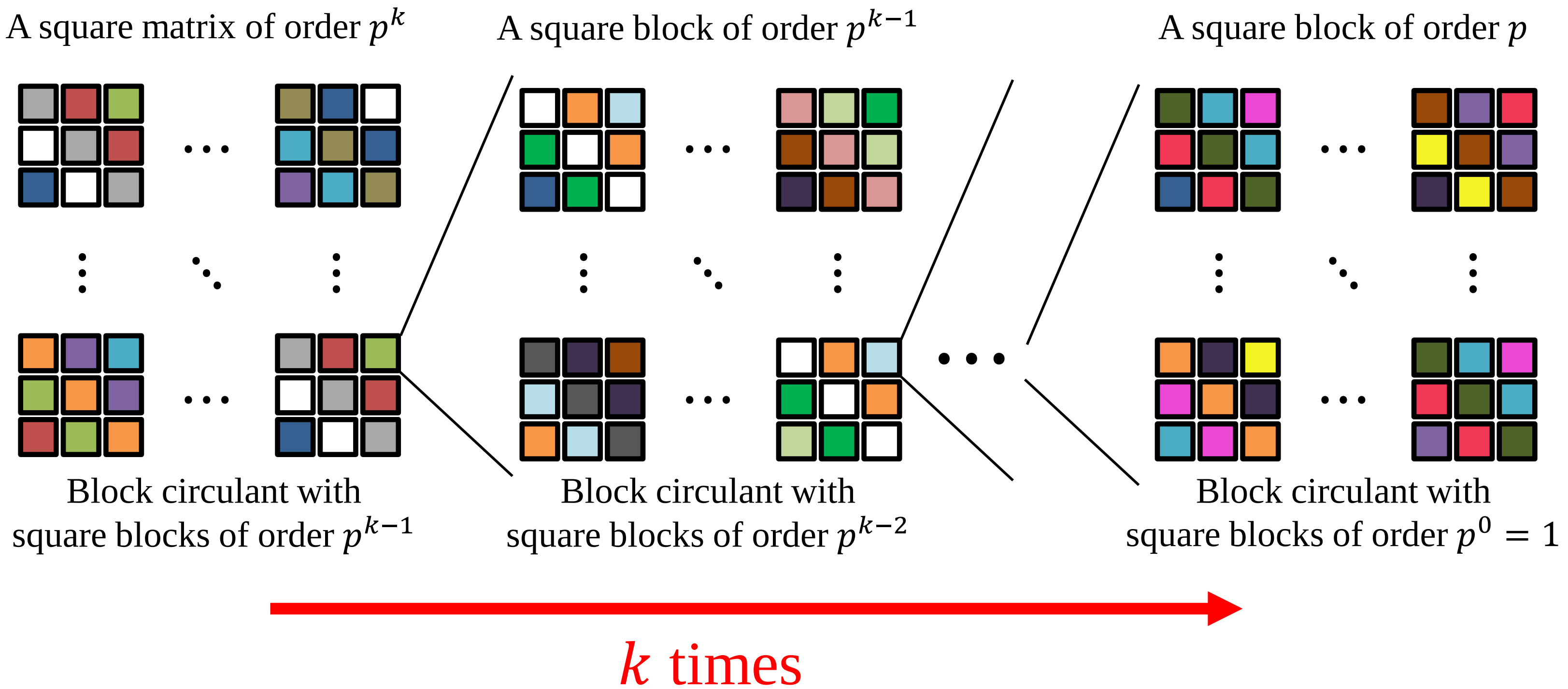
Multi-level circulancy

- (Multi-level circulant matrix of order p^k)
  A square matrix of order $q = p^k$ is a k-level circulant if, for any integers $t = 1, 2, \dots, k$, all the partitioned $p^{2(k-t)}$ **square blocks** of order p^t are **block circulant** with blocks of order p^{t-1}.

- (Fact)
  The Jacobsthal matrix Q of order $q = p^k$ is a k-level circulant matrix.

Multi-level circulant

- A visualization of k-level circulant matrix of order p^k



Eigenvalue decomposition of Q

- (Lemma – well-known: ED of ANY k-level circulant matrix)
  Let Q be the Jacobsthal matrix of order $q = p^k$ and
  $$\beta = \left(\beta_0, \beta_1, \dots, \beta_{p^k-1}\right)$$
  be the first row of Q.
- Then,
  $$\boldsymbol{Q} = \boldsymbol{S_Q \Lambda_Q S_Q^H}$$
  where
  $$\boldsymbol{S_Q} = \underbrace{F_p \otimes F_p \otimes \cdots \otimes F_p}_{k \text{ times}} := \bigotimes^{k} F_p\,,$$
  $$\boldsymbol{\Lambda_Q} = \sum_{l_0=0}^{p-1} \cdots \sum_{l_{k-1}}^{p-1} \beta_{\Psi^{-1}(\theta)} \left(\Omega_p^{l_0} \otimes \cdots \otimes \Omega_p^{l_{k-1}}\right),$$
  and
  $$\theta = \sum_{e=0}^{k-1} l_e \alpha^e \text{ and } \boldsymbol{\Omega_p} = \mathrm{diag}(1, \omega_p, \dots, \omega_p^{p-1})$$

when $k = 1, p = 7$

- $GF(q) = GF(p) = Z_p$ and $\Psi(i) = c_0 = i$ for all $i \in Z_p$
- $\sigma_{s,t} = \chi(\Psi(s) - \Psi(t)) = \chi(s-t)$ for $s,t = 0,1,\ldots,p-1$
- The top row of the Jacobsthal matrix Q of order 7 become

$$\begin{aligned}\beta &= (\beta_0, \beta_1, \ldots, \beta_6)\\ &= (\chi(0), \chi(-1), \ldots, \chi(-6))\\ &= (\chi(0), \chi(6), \chi(5), \chi(4), \chi(3), \chi(2), \chi(1))\\ &= (\mathbf{0}, -\mathbf{1}, -\mathbf{1}, +\mathbf{1}, -\mathbf{1}, +\mathbf{1}, +\mathbf{1})\end{aligned}$$

- Next row becomes

$$\begin{aligned}&(\chi(1), \chi(0), \ldots, \chi(-5))\\ &= (\chi(1), \chi(0), \chi(6), \chi(5), \chi(4), \chi(3), \chi(2))\\ &= (+\mathbf{1}, \mathbf{0}, -\mathbf{1}, -\mathbf{1}, +\mathbf{1}, -\mathbf{1}, +\mathbf{1})\end{aligned}$$

etc. Therefore,

$$Q = \begin{bmatrix} \mathbf{0},-,-,+,-,+,+ \\ +,\mathbf{0},-,-,+,-,+ \\ +,+,\mathbf{0},-,-,+,- \\ -,+,+,\mathbf{0},-,-,+ \\ +,-,+,+,\mathbf{0},-,- \\ -,+,-,+,+,\mathbf{0},- \\ -,-,+,-,+,+,\mathbf{0} \end{bmatrix}$$

$Q = S_Q \Lambda_Q S_Q^H$

- $S_Q = F_p$ is the Fourier matrix of order $p = 7$, where

$$F_p^H = \frac{1}{\sqrt{p}} \begin{bmatrix} 1, & 1, & 1, \ldots, & 1 \\ 1, & \omega^1, & \omega^2, \ldots, & \omega^6 \\ 1, & \omega^2, & \omega^4, \ldots, & \omega^{12} \\ 1, & \omega^3, & \omega^6, \ldots, & \omega^{18} \\ 1, & \omega^4, & \omega^8, \ldots, & \omega^{24} \\ 1, & \omega^5, & \omega^{10}, \ldots, & \omega^{30} \\ 1, & \omega^6, & \omega^{12}, \ldots, & \omega^{36} \end{bmatrix}$$

$$S_Q = \underbrace{F_p \otimes F_p \otimes \cdots \otimes F_p}_{} := \bigotimes^{k} F_p \,,$$

- $\Lambda_Q = \sum_{l_0=0}^{6} \beta_{\Psi^{-1}(\theta)} \Omega_7^{l_0} = \sum_{l=0}^{6} \beta_{\theta} \Omega_7^{l} = \sum_{l=0}^{6} \beta_{l} \Omega_7^{l}$,

  where

$$\Omega_7 = \mathrm{diag}(1, \omega, \omega^2, \ldots, \omega^6)$$

  and

$$\theta = \sum_{e=0}^{k-1} l_e \alpha^e = l_0 \alpha^0 = l_0 = l$$

$$\Lambda_Q = \sum_{l_0=0}^{p-1} \cdots \sum_{l_{k-1}}^{p-1} \beta_{\Psi^{-1}(\theta)} (\Omega_p^{l_0} \otimes \cdots \otimes \Omega_p^{l_{k-1}}),$$

$\theta = \sum_{e=0}^{k-1} l_e \alpha^e$ and $\Omega_p = \mathrm{diag}(1, \omega_p, \ldots, \omega_p^{p-1})$

$\boldsymbol{\Lambda_Q} = \sum_{l=0}^{6} \beta_l \Omega_7^l$

$\beta = (\beta_0, \beta_1, \dots, \beta_6) = (0, -1, -1, +1, -1, +1, +1)$

$$\boldsymbol{\Omega_7} = \begin{bmatrix} 1, & 0, & 0, & \dots & , 0 \\ 0, & \omega^1, & 0, & \dots & , 0 \\ 0, & 0, & \omega^2, & \dots & , 0 \\ 0, & 0, & 0, & \dots & , 0 \\ 0, & 0, & 0, & \dots & , 0 \\ 0, & 0, & 0, & \dots & , 0 \\ 0, & 0, & 0, & \dots & , \omega^6 \end{bmatrix}$$

Therefore, i-th eigenvalue λ_i becomes (for $i = 0,1,\dots,6$)

$$\lambda_i = \sum_{l=0}^{6} \beta_l \omega^{li} = -\omega^i - \omega^{2i} + \omega^{3i} - \omega^{4i} + \omega^{5i} + \omega^{6i}$$

and hence,

$$\begin{aligned} \lambda_0 &= 0 \\ \lambda_1 &= -2j\mathrm{Im}\{\omega^1 + \omega^2 + \omega^4\} \\ &= -2j\left\{\sin\left(\frac{2\pi}{7}\right) + \sin\left(\frac{4\pi}{7}\right) + \sin\left(\frac{8\pi}{7}\right)\right\} \cong -j\,(2.6458) \\ \lambda_2 &= \lambda_1 \\ \lambda_3 &= -\lambda_1 \\ \lambda_4 &= \lambda_1 \\ \lambda_5 &= -\lambda_1 \\ \lambda_6 &= -\lambda_1 \end{aligned}$$

$$\boldsymbol{\Lambda_Q} = \lambda_1 \begin{bmatrix} 0 & & & & & & \\ & 1 & & & & \mathbf{0} & \\ & & 1 & & & & \\ & & & -1 & & & \\ & & & & 1 & & \\ & \mathbf{0} & & & & -1 & \\ & & & & & & -1 \end{bmatrix}$$

Eigenvalue decomposition of Paley matrices

- Let $\widetilde{S}_Q$ and $\widetilde{\Lambda}_Q$ be the $(q-1)\times(q-1)$ right-bottom sub-matrices of S_Q and Λ_Q, respectively. Then

$$C = S_C \Lambda_C S_C^H$$

where

for $q \equiv 3 \pmod 4$	for $q \equiv 1 \pmod 4$
$S_C = \begin{bmatrix} j\sqrt{q} & -j\sqrt{q} & \underline{0}_{q-1}^T \\ 1 & 1 & \sqrt{2}\underline{1}_{q-1}^T \\ \underline{1}_{q-1} & \underline{1}_{q-1} & \sqrt{2q}\widetilde{S}_Q \end{bmatrix}$	$S_C = \begin{bmatrix} \sqrt{q} & -\sqrt{q} & \underline{0}_{q-1}^T \\ 1 & 1 & \sqrt{2}\underline{1}_{q-1}^T \\ \underline{1}_{q-1} & \underline{1}_{q-1} & \sqrt{2q}\widetilde{S}_Q \end{bmatrix}$
$\Lambda_C = \begin{bmatrix} -j\sqrt{q} & 0 & \underline{0}_{q-1}^T \\ 0 & j\sqrt{q} & \underline{0}_{q-1}^T \\ \underline{0}_{q-1} & \underline{0}_{q-1} & \widetilde{\Lambda}_Q \end{bmatrix}$	$\Lambda_C = \begin{bmatrix} \sqrt{q} & 0 & \underline{0}_{q-1}^T \\ 0 & -\sqrt{q} & \underline{0}_{q-1}^T \\ \underline{0}_{q-1} & \underline{0}_{q-1} & \widetilde{\Lambda}_Q \end{bmatrix}$

Some remarks for the proof

- Jacobsthal matrix Q is diagonalized by its eigenvector matrix

$$S_Q = \bigotimes^{k} F_p \, .$$

  - (Fact1) The left-most column of S_Q is a constant vector.
  - (Fact2) The others are not constant vectors.
  - (Fact3) All the columns of S_Q are orthonormal with each other.

- Paley matrix is of the form,

$$C = \begin{bmatrix} 0 & \underline{1}_q^T \\ \pm\underline{1}_q & Q \end{bmatrix}.$$

border

circulant core

  - We can guess that eigenvectors and eigenvalues of C are related to those of the circulant core Q.
  - We will show that it is true by deriving the eigenvectors of C from those of Q.

Proof: when $q \equiv 3 \pmod 4$

Let λ be an eigenvalue of Q corresponding to a not all-one eigenvector $\underline{v}$.
Since $\underline{1}_q$ and $\underline{v}$ are orthogonal, we have

$$C\begin{bmatrix} 0 \\ \underline{v} \end{bmatrix} = \begin{bmatrix} 0 & \underline{1}_q^T \\ -\underline{1}_q & Q \end{bmatrix}\begin{bmatrix} 0 \\ \underline{v} \end{bmatrix} = \lambda\begin{bmatrix} 0 \\ \underline{v} \end{bmatrix}.$$

Therefore, $\begin{bmatrix} 0 \\ \underline{v} \end{bmatrix}$ is the eigenvector of C and its corresponding eigenvalue is λ.

$\Rightarrow q-1$ eigenvalues & eigenvectors are found.

For the remaining two, consider

$$C\begin{bmatrix} x \\ \underline{1}_q \end{bmatrix} = \begin{bmatrix} 0 & \underline{1}_q^T \\ -\underline{1}_q & Q \end{bmatrix}\begin{bmatrix} x \\ \underline{1}_q \end{bmatrix} = \lambda\begin{bmatrix} x \\ \underline{1}_q \end{bmatrix},$$

for some λ.
This gives $q = x\lambda$ and $-x = \lambda$.
Solving these two equations gives

$$(x, \lambda) = (j\sqrt{q}, -j\sqrt{q}) \quad \text{or} \quad (-j\sqrt{q}, j\sqrt{q}).$$

These two solutions give two remaining eigenvectors and their corresponding eigenvalues.

Eigenvalue decomposition of Paley-type Hadamard matrices

- Recall the definition of **Paley-type Hadamard matrix** of order $q+1$, where $q = p^k$

- (Type 1) If $q \equiv 3 \pmod 4$, then

$$C + I_{q+1}.$$

- (Type 2) If $q \equiv 1 \pmod 4$, then

$$H = \begin{bmatrix} C + I_{q+1} & C - I_{q+1} \\ C - I_{q+1} & -C - I_{q+1} \end{bmatrix}.$$

Column permutation

$$H = \begin{bmatrix} C - I_{q+1} & C + I_{q+1} \\ -C - I_{q+1} & C - I_{q+1} \end{bmatrix}$$

Skew block circulant

Eigenvalue decomposition

Paley-type 1

- (Type 1) If $q \equiv 3 \pmod 4$, then
$$H = C + I_{q+1} = S_C\left(\Lambda_C + I_{q+1}\right)S_C^H.$$

All the eigenvectors are orthonormal with each other.

Proof) Obvious since $I_{q+1} = S_C S_C^H$.

Eigenvalue decomposition
Paley-type 2

- (Type 2) If $q \equiv 1 \pmod 4$, then

$$H = \begin{bmatrix} C - I_{q+1} & C + I_{q+1} \\ -C - I_{q+1} & C - I_{q+1} \end{bmatrix} = S_h \Lambda_h S_h^H$$

where

$$S_h = \frac{1}{\sqrt{2}} \begin{bmatrix} S_C & S_C \\ -jS_C & jS_C \end{bmatrix},$$

$$\Lambda_h = \begin{bmatrix} \Lambda_C - I_{q+1} + j\left(\Lambda_C + I_{q+1}\right) & 0_{q+1} \\ 0_{q+1} & \Lambda_C - I_{q+1} - j\left(\Lambda_C + I_{q+1}\right) \end{bmatrix}.$$

All the eigenvectors are orthonormal with each other.

The proof
Paley-type 2

Proof) For simplicity, denote I_{q+1} by I.

$$H = \begin{bmatrix} C-I & C+I \\ -C-I & C-I \end{bmatrix} := \begin{bmatrix} B_0 & B_1 \\ -B_1 & B_0 \end{bmatrix}$$

Skew block circulant

↓

$$AHA^H = \begin{bmatrix} I & 0 \\ 0 & jI \end{bmatrix} \begin{bmatrix} B_0 & B_1 \\ -B_1 & B_0 \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & jI \end{bmatrix}^H = \begin{bmatrix} B_0 & -jB_1 \\ -jB_1 & B_0 \end{bmatrix}$$

block circulant
(more friendly)

Since both B_0 and B_1 are diagonalizable by the orthogonal matrix S_C,

$$\begin{bmatrix} B_0 & -jB_1 \\ -jB_1 & B_0 \end{bmatrix} \begin{bmatrix} S_C \\ S_C \end{bmatrix} = \begin{bmatrix} S_C \\ S_C \end{bmatrix} \{(\Lambda_C - I) - j(\Lambda_C + I)\}$$

$$\begin{bmatrix} B_0 & -jB_1 \\ -jB_1 & B_0 \end{bmatrix} \begin{bmatrix} S_C \\ -S_C \end{bmatrix} = \begin{bmatrix} S_C \\ -S_C \end{bmatrix} \{(\Lambda_C - I) + j(\Lambda_C + I)\}$$

The proof
Paley-type 2

Therefore, we conclude that

$$AHA^H = S\Lambda S^H$$

$$\Longrightarrow H = A^H S \, \Lambda \, (A^H S)^H$$

where

$$S_h := A^H S = \frac{1}{\sqrt{2}} \begin{bmatrix} S_C & S_C \\ -jS_C & jS_C \end{bmatrix},$$

$$\Lambda_h := \Lambda = \begin{bmatrix} \Lambda_C - I_{q+1} + j\left(\Lambda_C + I_{q+1}\right) & 0_{q+1} \\ 0_{q+1} & \Lambda_C - I_{q+1} - j\left(\Lambda_C + I_{q+1}\right) \end{bmatrix}.$$

It is easy to check that all the eigenvectors of H are orthonormal with each other.

Cyclic type Hadamard matrices

- A binary sequence of length $n-1$ is called cyclic Hadamard sequence when
  - -1 occurs $(n+1)/2$ and $+1$ occurs $(n-1)/2$.
  - Out-of-phase autocorrelation is always -1.

- A cyclic type Hadamard matrix of order n, constructed by a cyclic Hadamard sequence $\gamma = (\gamma_0, \gamma_1, \ldots, \gamma_{n-2})$, is defined by

$$H = \begin{bmatrix} 1 & \underline{1}_{n-1}^T \\ \underline{1}_{n-1} & \underline{\mathrm{circ}(\gamma)} \end{bmatrix}.$$

Circulant core

- Well-known cyclic Hadamard sequences:
  - binary m-sequence
  - binary GMW sequences
  - Hall's sextic residue sequences
  - Quadratic residue sequence (or Legendre sequence)
  - Twin prime sequences

Cyclic type Hadamard matrices

- When $q = p = 3 \pmod 4$, a Paley-type Hadamard matrix is

$$H = \begin{bmatrix} 0 & \underline{1}_q^T \\ -\underline{1}_q & Q \end{bmatrix} + I_{q+1} = \begin{bmatrix} 1 & \underline{1}_q^T \\ -\underline{1}_q & Q + I_q \end{bmatrix}.$$

  Here, note that $Q + I_q$ is the circulant core of H.
- Then,

$$\begin{bmatrix} 1 & \underline{1}_q^T \\ \underline{1}_q & -Q - I_q \end{bmatrix} \text{ is of cyclic-type}$$

- Previous method for Paley matrices can be similarly used.

Eigenvalue decomposition

cyclic type

Let H be a cyclic-type Hadamard matrix of order n constructed by a cyclic Hadamard sequence γ of length $n-1$.

Then,

$$H = S_h \Lambda_h (S_h)^H$$

where

$$S_h = \begin{bmatrix} \frac{1+\sqrt{n}}{\sqrt{2n+2\sqrt{n}}} & \frac{1-\sqrt{n}}{\sqrt{2n-2\sqrt{n}}} & \underline{0}_{n-2}^T \\ \frac{1}{\sqrt{2n+2\sqrt{n}}} & \frac{1}{\sqrt{2n-2\sqrt{n}}} & \frac{1}{\sqrt{n-1}}\underline{1}_{n-2}^T \\ \frac{1}{\sqrt{2n+2\sqrt{n}}}\underline{1}_{n-2} & \frac{1}{\sqrt{2n-2\sqrt{n}}} & \widetilde{\boldsymbol{F}}_{\boldsymbol{n-1}} \end{bmatrix}$$

and

$$\Lambda_h = \mathrm{diag}(\lambda_0 = +\sqrt{n},\ \lambda_1 = -\sqrt{n},\ \lambda_2, \lambda_3, \ldots, \lambda_{n-1})$$

with

$$\lambda_{i+1} = \sum_{z=0}^{n-2} \gamma_z \omega_{n-1}^{iz} \qquad \text{for} \quad i = 1,2,3,\ldots,n-2.$$

Eigenvalues/eigenvectors of cyclic type Hadamard matrices

- **All** the cyclic-type Hadamard matrices of order n have
  - **the same eigenvector matrix** S_h
    - closely related with the **Fourier matrix of order $n-1$**.
    - (complex) unitary
  - $\pm\sqrt{n}$ as common eigenvalues, and
  - remaining $n-2$ eigenvalues

$$\boldsymbol{\lambda_{i+1}} = \sum_{z=0}^{n-2} \gamma_z \omega_{n-1}^{iz} \qquad \text{for} \quad i = 1,2,3,\dots,n-2,$$

where

$$\gamma = (\gamma_0, \gamma_1, \dots, \gamma_{n-2})$$

is the top-row of the circulant core (cyclic Hadamard sequence of length $n-1$)

Summary

- The eigenvalue decomposition of a Paley-type Hadamard matrix is obtained explicitly, by using the multi-level circulant structure of some Jacobsthal matrices.
- By using similar method, the eigenvalue decomposition of cyclic-type Hadamard matrix is also obtained.
- The eigenvalues of Paley-type and cyclic-type Hadamard matrices are closely related to their multi-level circulant cores.
- FAST Paley-Hadamard Transform algorithm??
  Or, fast cyclic-Hadamard Transform algorithm??