Konstrukcje Paley'a macierzy Hadamarda rozmiaru $q+1$ (dla $q \equiv 3 \mod 4$) oraz $2(q+1)$ (dla $q \equiv 1 \mod 4$).

Abstract

Macierze Hadamarda są kwadratowymi macierzami o elementach równych ± 1, których wiersze są ortogonalne. Konstrukcja takich macierzy stanowi jedno z kluczowych zagadnień w kombinatoryce i teorii macierzy, ze względu na ich liczne zastosowania. Jedną z klasycznych metod budowy macierzy Hadamarda jest konstrukcja Paleya, która opiera się na szczególnych własnościach ciał skończonych i kwadratów resztowych. W tej pracy analizujemy szczegóły konstrukcji Paleya oraz prezentujemy jej warianty. Omówimy również przykłady oraz dowody istnienia macierzy Hadamarda o rozmiarach opartych na ciałach skończonych, ilustrując tym samym, jak algebraiczne struktury wspomagają efektywne tworzenie tych macierzy. Praca zawiera przegląd teoretyczny, jak i praktyczne aspekty implementacji konstrukcji Paleya.

1 Wprowadzenie

Macierze Hadamarda [2] to kwadratowe macierze o wymiarach $m \times m$, których elementy wynoszą ± 1, a wiersze (lub kolumny) są wzajemnie ortogonalne, co oznacza, że ich iloczyny skalarne wynoszą zero. Formalnie, macierz Hadamarda spełnia zależność $H^T H = mI$, gdzie H^T oznacza macierz transponowaną, a I jest macierzą jednostkową.

Jedną z najprostszych metod konstrukcji macierzy Hadamarda jest rekurencyjna konstrukcja dla wymiarów będących potęgami liczby 2, na przykład:

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad H_{2m} = \begin{bmatrix} H_m & H_m \\ H_m & -H_m \end{bmatrix}.$$

W ogólności, jeśli macierz H jest macierzą Hadamarda, to macierz transponowana H^T również nią jest, co oznacza, że ortogonalność zachodzi zarówno dla wierszy, jak i kolumn.

Jednym z fundamentalnych problemów związanych z macierzami Hadamarda jest określenie, dla jakich rzędów m istnieją takie macierze. Hipoteza Hadamarda sugeruje, że macierz Hadamarda istnieje dla każdego m podzielnego przez 4, choć dla niektórych wartości m, takich jak 668, istnienie macierzy Hadamarda pozostaje niepotwierdzone.

W niniejszej pracy koncentrujemy się na jednej z klasycznych metod konstrukcji macierzy Hadamarda – konstrukcji Paleya. Metoda ta bazuje na algebraicznych własnościach ciał skończonych i kwadratów resztowych, co umożliwia budowanie macierzy Hadamarda o określonych rzędach. W kolejnych częściach pracy szczegółowo omówimy proces konstrukcji Paleya wraz z dowodem.

2 Notacja i wstępne definicje

W celu wprowadzenia konstrukcji Paleya [3] macierzy Hadamarda, niezbędne jest wprowadzenie kilku kluczowych pojęć związanych z ciałami skończonymi oraz kwadratowymi symbolami charakterystycznymi. Konstrukcja ta wykorzystuje algebraiczne własności ciał skończonych, a w szczególności charakter kwadratowy, do budowania macierzy spełniających warunki Hadamarda. Poniżej wprowadzamy podstawowe definicje i notacje, które będą używane w dalszej części pracy.

Niech q będzie potęgą nieparzystej liczby pierwszej p.

2.1 Charakter kwadratowy [5]

Charakter kwadratowy $\chi(a)$ w ciele skończonym $\mathrm{GF}(q)$ określa, czy element a jest zerem, kwadratem innego elementu ciała (reszta kwadratowa), czy niekwadratem (reszta niekwadratowa). Definiujemy go następująco:

$$\chi(a) = \begin{cases} 0 & \text{jeśli } a = 0, \\ 1 & \text{jeśli } a = b^2 \text{ dla pewnego niezerowego } b \in \mathrm{GF}(q), \\ -1 & \text{jeśli } a \text{ nie jest kwadratem żadnego elementu w } \mathrm{GF}(q). \end{cases}$$

2.2 Macierz Jacobsthala [5]

Macierz Jacobsthala Q dla ciała skończonego $\mathrm{GF}(q)$ to macierz o wymiarach $q \times q$, której wiersze i kolumny są indeksowane elementami tego ciała. Element w wierszu a i kolumnie b dany jest przez wartość $\chi(a - b)$, gdzie χ jest charakterem kwadratowym zdefiniowanym powyżej.

2.3 Konstrukcja Paleya I [5]

Jeśli $q \equiv 3 \pmod 4$, wówczas można skonstruować macierz Hadamarda H rzędu $q+1$ za pomocą następującej formuły:

$$H = I + \begin{bmatrix} 0 & j^T \\ -j & Q \end{bmatrix},$$

gdzie j to wektor kolumnowy wypełniony jedynkami o długości q, a I to macierz jednostkowa wymiaru $(q + 1) \times (q + 1)$. Taka macierz H jest macierzą Hadamarda o własności skośnosymetrycznej, czyli spełnia $H + H^T = 2I$.

2.4 Konstrukcja Paleya II [5] [4]

Jeśli $q \equiv 1 \pmod 4$, możemy skonstruować macierz Hadamarda rzędu $2(q + 1)$, zastępując wszystkie zera w macierzy:

$$C = \begin{bmatrix} 0 & j^T \\ j & Q \end{bmatrix}$$

odpowiednią macierzą:

$$\begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix},$$

a wszystkie wartości ± 1 odpowiednią macierzą:

$$\pm \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

lub (inna konstrukcja) biorąc macierz [4]

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

Taka macierz jest symetryczną macierzą Hadamarda o rozmiarze $2(q + 1)$.

3 Przygotowania

Zanim przejdziemy do dowodu konstrukcji, wprowadzimy i udowodnimy kilka lematów pomocniczych.

Lemat 1. *Jeśli* $q \equiv 3 \mod 4$ *to* -1 *nie jest kwadratem oraz macierz* Q *jest skośnosymetryczna.*

Dowód: Załóżmy przeciwnie, że istnieje $b \in GF(q)$, że $-1 = b^2$. Niech $q = 4k+3$, wtedy

$$-1 \equiv (-1)^{2k+1} \equiv (-1)^{\frac{q-1}{2}} \equiv (b^2)^{\frac{q-1}{2}} = b^{q-1} = 1$$

Wobec sprzeczności otrzymujemy tezę. Ponadto $\chi(a-b) = -\chi(b-a)$ czyli $Q^T = -Q$. □

Lemat 2. *Jeśli* $q \equiv 1 \mod 4$ *to* -1 *jest kwadratem oraz macierz* Q *jest symetryczna.*

Dowód: Mamy $q = p^n$, gdzie p jest nieparzystą liczbą pierwszą. Korzystając z twierdzenia Wilsona mamy

$$-1 \equiv (p-1)! \equiv 1 \cdot \ldots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot (p-1) \equiv \left(\frac{p-1}{2}\right)! \cdot (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! = \left[\left(\frac{p-1}{2}\right)!\right]^2$$

ponieważ $p \equiv 1 \mod 2$. Zatem -1 jest kwadratem oraz $\chi(a-b) = \chi(b-a)$, czyli $Q^T = Q$. □

Lemat 3. *Dla* $b \neq 0$ *zachodzi* $\sum_a \chi(a) \cdot \chi(a+b)$

Dowód: Oczywiście $\chi(0) \cdot \chi(0+b) = 0$. Załóżmy więc, że $a \neq 0$, wtedy istnieje $z \neq 1$, że $a + b = a \cdot z$. Takie z istnieje, bo jeśli $a = -b$, to $a \cdot z = 0$ czyli $z = 0$, zaś w przeciwnym przypadku $z = 1 + b \cdot a^{-1}$. Mamy więc

$$\sum_a \chi(a) \cdot \chi(a+b) = \sum_a \chi(a) \cdot \chi(a \cdot z) = \sum_a \chi(a)^2 \cdot \chi(z) = \sum_z \chi(z) - \chi(1) = 0 - 1 = -1$$

□

Lemat 4. $Q^T Q = qI - J$, *gdzie* I *jest macierzą jednostkową, zaś* J *jest macierzą składającą się z samych jedynek.*

Dowód: Niech $B = Q^T Q$. Wtedy dla $i \neq j$ mamy $b_{ij} = -1$, bo

$$b_{ij} = \sum_k \chi(a_i - a_k) \cdot \chi(a_j - a_k) = -1$$

bo bierzemy $a = a_i - a_k$ oraz $b = a_j - a_i$ w lemacie 3. Dla $i = j$ wyrazy w kolumnie to 0 oraz $q-1$ ± 1, zatem $b_{ij} = q - 1$. □

4 Dowód konstrukcji I

Twierdzenie 5. *Niech* $q \equiv 3 \mod 4$ *oraz niech*

$$H = I + \begin{bmatrix} 0 & j^T \\ -j & Q \end{bmatrix}$$

gdzie j *to wektor kolumnowy wypełniony jedynkami o długości* q*, a* I *to macierz jednostkowa wymiaru* $(q+1) \times (q+1)$*. Wówczas macierz* H *jest macierzą Hadamarda rzędu* $q+1$*.*

Dowód: Musimy udowodnić, że $H^T H = m \cdot I$ dla pewnego m. Mamy

$$H^T H = \left(I + \begin{bmatrix} 0 & -j^T \\ j & Q \end{bmatrix}\right) \cdot \left(I + \begin{bmatrix} 0 & j^T \\ -j & Q \end{bmatrix}\right) = I + \begin{bmatrix} 0 & 0 \\ 0 & Q^T + Q \end{bmatrix} + \begin{bmatrix} j^T \cdot j & -j^T \cdot Q \\ Q^T \cdot j & Q^T Q + J \end{bmatrix}$$

Mamy $Q^T = -Q \Leftrightarrow$, zatem druga macierz w powyższej równości jest macierzą zerową. Pokażemy, że trzecia macierz jest równa $q \cdot I$.

- $j^T \cdot j = q$
- $-j^T \cdot Q = 0$ oraz $Q^T \cdot j = 0$, ponieważ w $GF(q)$ liczba niekwadratów równa jest liczbie kwadratów.
- $Q^T Q = qI - J$ zgodnie z lematem 4

Zatem $H^T H = (q+1) \cdot I$. □

5 Dowód konstrukcji II

Twierdzenie 6. *Niech* $q \equiv 1 \pmod 4$. *Niech* H *będzie macierzą rzędu* $2(q+1)$, *która powstaje przez zastąpienie wszystkich zer w macierzy:*

$$C = \begin{bmatrix} 0 & j^T \\ j & Q \end{bmatrix}$$

odpowiednią macierzą:

$$M_0 := \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix},$$

zaś wszystkich wartości ± 1 *odpowiednią macierzą:*

$$M_{\pm 1} := \pm \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Wówczas macierz H *jest macierzą Hadamarda rzędu* $2(q+1)$.

Dowód: Aby wykazać, że H jest macierzą Hadamarda, musimy pokazać, że H spełnia równanie

$$H^T H = m \cdot I,$$

dla pewnego m. Zauważmy, że

$$M_0^2 = \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix} = 2I,$$

$$M_1^2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = 2I,$$

$$M_{-1}^2 = \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix} = 2I.$$

czyli że macierze M_0, M_1 i M_{-1} są macierzami Hadamarda. Dalej jasne jest, że $C^T C = C^2 = qI$, czyli że C również jest macierzą Hadamarda. Zauważmy, że w macierzy H na przekątnej leżą zera, zaś poza przekątną występują tylko ± 1. Zatem możemy napisać, że

$$H = C \times \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} + I \times \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix} = C \times M_1 + I \times M_0$$

gdzie $A \times B$ oznacza iloczyn Kroneckera [1] macierzy A i B. Wystarczy więc pokazać, że iloczyn Kroneckera dwóch macierzy Hadamarda jest macierzą Hadamarda (bo jasne jest że ich suma będzie). Niech H_a i H_b będą macierzami Hadamarda rzędu a oraz b. Mamy

$$(H_a \times H_b)^T \cdot (H_a \times H_b) = (H_a^T \times H_b^T) \cdot (H_a \times H_b) = H_a^T H_a \times H_b^T H_b = aI \times bI = ab \cdot I$$

Stąd H również jest macierzą Hadamarda. □

Twierdzenie 7. *Niech* $q \equiv 1 \pmod 4$. *Wówczas macierz*

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

jest macierzą Hadamarda rzędu $2(q+1)$.

Dowód: Musimy wykazać, że $H^T H = m \cdot I$, dla pewnego m. Ponieważ C jest symetryczna (wynika to z lematu 2) oraz $I_{q+1}^T = I_{q+1}$, mamy:

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

Obliczamy teraz iloczyn $H^T H$ jako:

$$H^T H = \begin{bmatrix} C + I_{q+1} & C - I_{q+1} \\ C - I_{q+1} & -(C + I_{q+1}) \end{bmatrix} \begin{bmatrix} C + I_{q+1} & C - I_{q+1} \\ C - I_{q+1} & -(C + I_{q+1}) \end{bmatrix} := \begin{bmatrix} K & L \\ M & N \end{bmatrix}$$

gdzie

$$\begin{aligned} K &= (C + I_{q+1})(C + I_{q+1}) + (C - I_{q+1})(C - I_{q+1}) = 2C^2 + 2I_{q+1}, \\ L &= (C + I_{q+1})(C - I_{q+1}) + (C - I_{q+1})(-(C + I_{q+1})) = 0, \\ M &= (C - I_{q+1})(C + I_{q+1}) + (-(C + I_{q+1}))(C - I_{q+1}) = 0, \\ N &= (C - I_{q+1})(C - I_{q+1}) + (-(C + I_{q+1}))(-(C + I_{q+1} =)) = 2C^2 + 2I_{q+1}. \end{aligned}$$

Wiemy, że macierz C spełnia:

$$C^2 = \begin{bmatrix} j^T \cdot j & j^T \cdot Q \\ Q^T \cdot j & Q^T Q + J \end{bmatrix} = \begin{bmatrix} q & 0 \\ 0 & qI \end{bmatrix} = q \cdot I_{q+1}$$

Zatem

$$\begin{aligned} K &= 2(q+1) \cdot I_{q+1}, \\ L &= 0, \\ M &= 0, \\ N &= 2(q+1) \cdot I_{q+1}. \end{aligned}$$

więc $H^T H$ jest macierzą rozmiaru $2(q+1)$ z wyrazami $2(q+1)$ na przekątnej.

□

References

[1] W. contributors. Iloczyn kroneckera, 2024. Accessed: 2024-11-10.

[2] J. Hadamard. Resolution d'une question relative aux determinants. *Bull. des sciences math.*, 2:240–246, 1893.

[3] R. E. A. C. Paley. On orthogonal matrices. *Journal of Mathematics and Physics*, 12, 1933.

[4] P. Sin. Hadamard matrices, 2022.

[5] Wikipedia contributors. Paley construction — wikipedia, the free encyclopedia, 2024.