Macierze Hadamarda

Autorzy: Krystian Urban, Filip Walkowicz

Data: 09.05.2024r.

Macierze Hadamarda to kwadratowe macierze złożone z zer i jedynek. Są ważnym elementem m.in. działań w informatyce kwantowej. Niniejszy referat zawiera przedstawienie i opis tych macierzy oraz ich zastosowania.

1. Wstęp

1.1 Życie Jacques Hadamard’a

Jacques Hadamard (1865–1963) był wybitnym matematykiem, urodzonym w Wersalu. Jego matka była pianistką, a ojciec nauczycielem. Po wojnie francusko-pruskiej przeprowadził się do Paryża. Dzięki inspirującemu nauczycielowi w szkole średniej Hadamard zainteresował się matematyką. Ukończył École Normale Supérieure jako najlepszy kandydat i rozpoczął badania nad funkcjami analitycznymi. W 1892 roku obronił doktorat oraz zdobył prestiżową nagrodę Grand Prix des Sciences Mathématiques za pracę dotyczącą liczb pierwszych i funkcji zeta. W czasie I wojny światowej stracił dwóch synów, a podczas II wojny światowej trzeci syn zginął. W 1940 roku uciekł przed nazistami do USA, później wrócił do Francji.
Hadamard był znanym i cenionym nauczycielem, którego wykłady łączyły precyzję z intuicją. Napisał również książki popularnonaukowe, m.in. The Psychology of Invention in the Mathematical Field (1945). Jego prace miały ogromny wpływ na rozwój matematyki XX wieku, szczególnie w analizie matematycznej. Zmarł w wieku 97 lat, przygnieciony śmiercią wnuka w wypadku górskim. Pozostawił po sobie około 300 publikacji naukowych oraz głęboki ślad w historii matematyki i społeczeństwa.

1.2 Odkrycie i kontekst historyczny

Pojęcie tej klasy macierzy sięga XIX wieku – podobne wzory opisał już James Sylvester w 1867 roku (nazwając je anallagmatic pavements). Jednak to Jacques Hadamard w 1893 r. przeanalizował je systematycznie przy okazji badania nierówności na wyznacznik macierzy. W swoim artykule Hadamard udowodnił, że dla dowolnej macierzy $n \times n$ o ograniczonych wartościach wpisów zachodzi $|\det A| \leq n^{\frac{n}{2}}$, i wykazał, że równość osiąga się tylko wtedy, gdy wiersze są ortogonalne. Macierze spełniające tę nierówność z równością – czyli maksymalizujące moduł wyznacznika – zaczęto nazywać od jego nazwiska. Współczesne opracowania podkreślają, że już w 1893 r. Hadamard’s theorem on determinants (nierówność Hadamarda) po raz pierwszy się pojawiła, a macierze z maksymalnym wyznacznikiem (dziś – hadamardowskie) są ważne w wielu dziedzinach matematyki stosowanej.

1.3 Wpływ na rozwój matematyki i dziedzin pokrewnych

Odkrycie i badania Hadamarda miały istotny wpływ na rozwój matematyki kombinatorycznej i stosowanej. Pobudziło to rozwój teorii blokowych układów ortogonalnych, struktur geometrycznych i optymalnego projektowania eksperymentów – wiele prac w statystyce opiera się na koncepcji macierzy ortogonalnych podobnych do hadamardowskich. Macierze Hadamarda są również fundamentem nowoczesnej teorii kodowania (w tym konstrukcji kodów o dużej odległości minimalnej) i teorii grafów (poprzez powiązane rozkłady blokowe). Od czasu pracy Hadamarda badacze postawili sobie za cel zbudowanie macierzy o kolejnych rzędach, co zaowocowało wieloma konstrukcjami (np. metodą Sylvestera, Paleya, Williamsona). Wciąż pozostaje otwartym pytaniem słynna hipoteza Hadamarda – czy dla każdego rzędu $n = 4k$ istnieje macierz Hadamarda. Ten nierozwiązany problem stymuluje prace badawcze w dziedzinie teorii kombinatorycznej i zastosowań. Ogółem, koncepcja i badania Hadamarda przyczyniły się do wielu odkryć pośrednich (w tym konstrukcji nowych rodzajów macierzy ortogonalnych) oraz do rozwoju praktycznych narzędzi matematycznych użytecznych w różnych dziedzinach nauki.

2. Definicja

Macierze Hadamarda to specjalny typ mecierzy kwadratowych $\mathbb{H} \in \mathbb{R}^{n \times n}$w których wszystkie elementy przyjmują wartości $\{+1, -1\}$, a wiersze są wzajemnie ortogonalne. Oznacza to, że iloczyn skalarny dowolnych dwóch różnych wierszy wynosi zero. Formalnie:

$$HH^T = nI_n$$

gdzie I_n to macierz jednostkowa stopnia n. Przykłady macierzy Hadamarda:

$$H_1 = (1) \quad H_4 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad H_4 = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

Własności macierzy Hadamarda

(i) $HH^T = nI_n$ - iloczyn macierzy przez jej transpozycję daje skalowaną macierz jednostkową,

(ii) $|\det A| = n^{\frac{n}{2}}$ - maksymalna możliwa wartość wyznacznika,

(iii) $HH^T = H^T H$ - macierz normalna

(iv) Macierze Hadamarda można przekształcać w inne macierze Hadamarda przez:
- permutację wierszy i/lub kolumn,
- mnożenie dowolnego wiersza lub kolumny przez −1.

(v) Każda macierz Hadamarda jest H-równoważna z macierzą, w której pierwszy wiersz i pierwsza kolumna składają się tylko z +1+1. Takie macierze nazywamy znormalizowanymi.

(vi) Dla każdej macierzy Hadamarda rzędu $4n$:
- każda kolumna/wiersz zawiera dokładnie $2n$ wartości $\{-1, +1\}$
- każda para wierszy (lub kolumn) pokrywa się w nn miejscach, gdzie występuje -1 (czyli mają wspólne minusy w dokładnie n pozycjach).

(vii) Możliwe są tylko rozmiary macierzy 1,2 lub $4n$, dla dowolnego dodatniego n

3. Właściwości

3.1 Właściwości wartości

Jedną z łatwiej zauważalnych właściwości macierzy Hadamarda jest ilość wartości dodatnich oraz ujemnych w każdym wierszu oraz kolumnie (poza pierwszym wierszem oraz niekiedy pierwszą kolumną) - **jest ona równa n, gdzie $n \in \{1, 2, ...2k\}, k \in \mathbb{N}$**. Przyjrzyjmy się przykładowi macierzy H_4:

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Wszystkie (z wyjątkiem pierwszych) wiersze i kolumny mają po dwie wartości 1 i -1. Jest jeszcze jedna właściwość, którą można dostrzec po zestawieniu dowolnych dwóch wierszy lub kolumn macierzy. Wybierzmy drugą i trzecią kolumnę:

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

W dokładnie połowie par obydwie wartości mają te same znaki, a w pozostałej połowie - przeciwne. Kolejną właściwością dotyczącą ilości elementów w tej macierzy jest fakt, że ilość wartości −1 w H_n jest równa $\frac{n(n-1)}{2}$, a wartości 1 - $\frac{n(n+1)}{2}$; w przypadku H_4 jest to odpowiednio 6 oraz 10.

3.2 Właściwości macierzy

Przydatną charakterystyką macierzy Hadamarda jest możliwość generowania macierzy większego rzędu przy pomocy macierzy mniejszego rzędu. Macierz $H_{m\times n}, m, n \in \mathbb{N}$ można uzyskać z wyniku iloczynu tensorowego macierzy $H_m \otimes H_n$:

$$H_2 = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

$$H_4 = H_{2\times 2} = \begin{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \\ -\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Metoda ta nie działa dla wszystkich macierzy Hadamarda; macierzy rzędu 12, 20, 28, 36, 44, 52, 60, 68, 76, 84, 92 oraz 100 nie można skonstruować przy pomocy macierzy niższego rzędu.

Wygenerować macierz Hadamarda można jeszcze w inny sposób - w przypadku H_n, gdzie liczba n jest podzielna przez 4 i można ją zapisać w postaci $2^e(p^m + 1), m \in \mathbb{N}, e \in \mathbb{Z}, p -$ nieparzysta liczba pierwsza możliwe jest wygenerowanie jej przy pomocy **konstrukcji Paleya**, tj. przy pomocy ciał skończonych.

Przykład: Znajdź macierz Hadamarda rzędu 4.

rząd $n = 4$ możemy przedstawić w postaci:

$$4 = p^k + 1$$

przy $p = 3, k = 1$.

Po wyznaczeniu p, następnym krokiem jest znalezienie kwadratowych reszt $\bmod n$ w przedziale $\left\{1, ... \frac{n+1}{2}\right\}$; dla $n = 4, p = 3$ jest to zbiór liczb $\{1, 2\}$. Sprawdzimy wszystkie elementy zbioru:

dla 1:

$$1^2 \bmod 4 = 1 \neq 0; \text{1 jest resztą kwadratową}$$

dla 2:

$$2^2 \bmod 4 = 0; \text{2 nie jest resztą kwadratową}$$

Zbiór interesujących nas reszt kwadratowych to $\{1\}$.

Tworzymy pustą macierz rozmiarów $n \times n$; pierwszy rząd oraz kolumnę wypełniamy jedynkami:

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

Następnie, przekątną tej macierzy wypełniamy wartościami −1, a pozostałym komórkom przypisujemy wartość $(i - j) \bmod p$, gdzie i, j to odpowiednio indeks wiersza oraz indeks kolumny:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 2 & 1 \\ 1 & 1 & -1 & 2 \\ 1 & 2 & 1 & -1 \end{pmatrix}$$

W powyższej macierzy zamieniamy wszystkie wartości nienależące do zbioru reszt kwadratowych na −1:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix} = A$$

Sprawdźmy zgodność powstałej macierzy z definicją macierzy Hadamarda:

$$A * A^T = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix} * \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix} = n * J$$

Gdzie J to macierz jednostkowa, zatem znaleziona macierz jest macierzą Hadamarda rzędu 4.

Macierz Hadamarda jest **rozwiązaniem problemu największego wyznacznika**; dotyczy on znalezienia największego wyznacznika macierzy rozmiaru $n \times n$ zawierających jedynie wartości znajdujące się w określonym zbiorze; uściślając, macierz Hadamarda rzędu n jest rozwiązaniem tego problemu dla zbioru macierzy $n \times n$, których wartości spełniają warunek $|a_{\mathrm{ij}}| \leq 1$.

Macierz Hadamarda n-tego rzędu jest też macierzą incydencji grafu Hadamarda o $4n$ wierzchołkach; ich główną właściwością jest **tranzytywność względem odległości**, co w uproszczeniu oznacza, że dowolne dwa wierzchołki można zamienić miejscami z innymi dwoma wierzchołkami o tej samej odległości między nimi.

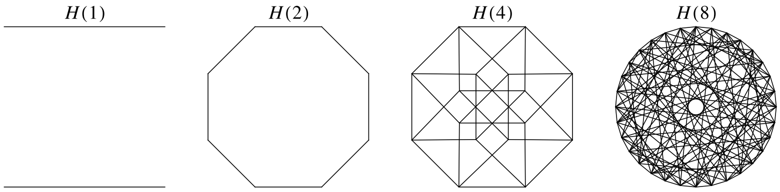

Figure 1: Przykład grafów Hadamarda.

3. Zastosowania

Macierze Hadamarda mają zastosowanie w wielu dziedzinach matematyki oraz informatyki.

3.1 Funkcje Walsha

Funkcje Walsha są dyskretną alternatywą szeregu Fouriera; zbiór funkcji Walsha może zostać użyty do przybliżenia funkcji dyskretnych. Przyjmują wartości −1 lub 1 oraz są cykliczne.

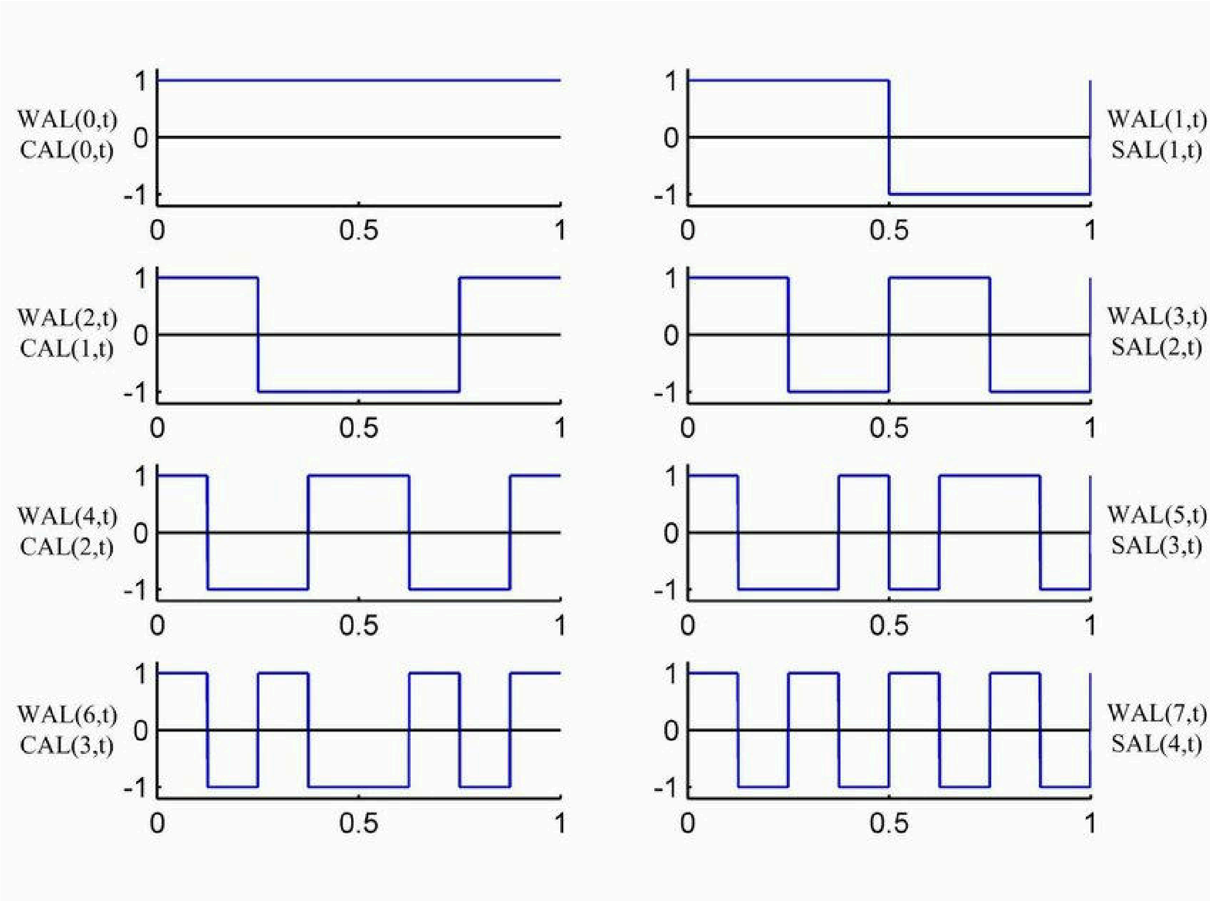

Figure 2: Przykład funkcji Walsha. Źródło: researchgate.net

Formalna definicja szeregu funkcji Walsha $W_k : [0, 1] \to \{-1, 1\}, k \in \mathbb{N}$
Niech $k \in \mathbb{N}, x \in [0, 1]$, k_j - k-ty bit binarnej postaci liczby k, x_j - j-ty bit binarnej postaci liczby x.
Wtedy:

$$W_{k(x)} = (-1)^{\sum_{j=0}^{\infty} k_j x_{j+1}}$$

Całkowity zbiór 2^n funkcji Walsha stopnia n tworzy macierz H_{2^n}.

Przykład: Wartości funkcji Walsha z rysunku 1 (oznaczone $\mathrm{WAL}(n, t)$) odpowiadają wartościom n-tego wiersza (lub kolumny) macierzy H_8:

$$H_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \end{pmatrix}$$

Dzięki temu możliwe jest wykorzystanie macierzy Hadamarda do przeprowadzenia dyskretnej transformaty Hadamarda-Walsha, która (analogicznie do transformaty Fouriera) zamienia funkcję w wartości wag przypisanych odpowiednim funkcjom Walsha w szeregu przybliżającym transformowaną funkcję.

```
x1 = ecg(512);                     % Single ecg wave
x = repmat(x1,1,8);
x = x + 0.1.*randn(1,length(x));  % Noisy ecg signal
y = fwht(x);                       % Fast Walsh-Hadamard transform

subplot(2,1,1)
plot(x)
xlabel('Sample index')
ylabel('Amplitude')
title('ECG Signal')
subplot(2,1,2)
plot(abs(y))
xlabel('Sequency index')
ylabel('Magnitude')
title('WHT Coefficients')
```

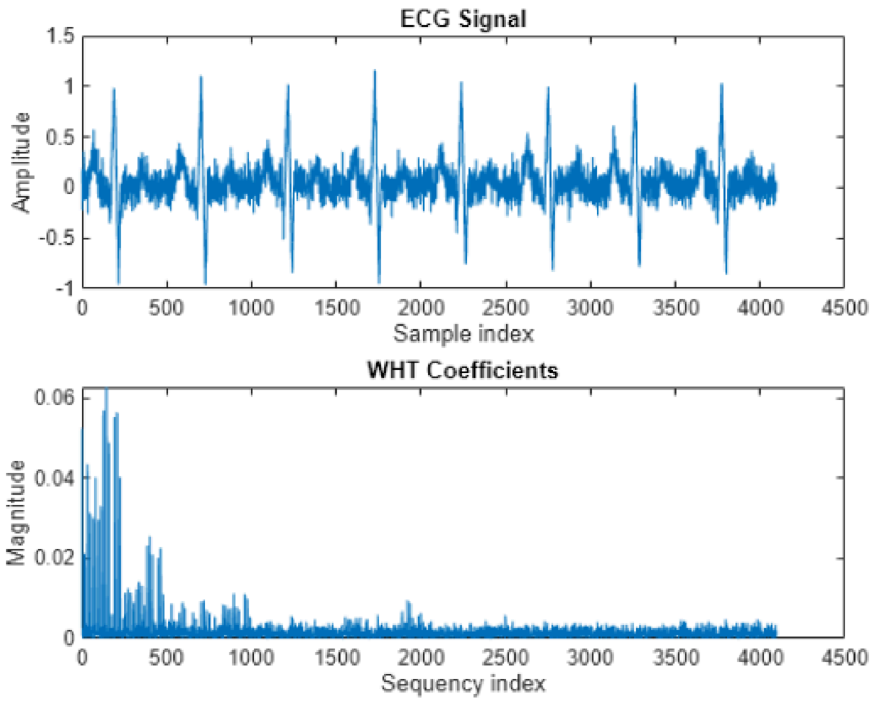

Figure 3: Zastosowanie szybkiej transformaty Walsha-Hadamarda do zdekodowania sygnału elektrokardiogramu. Źródło: Dokumentacja MATLAB

3.2 Zastosowania w uczeniu maszynowym

Współczesne badania eksplorują wykorzystanie zagadnień związanych z macierzą Hadamarda w kompresji i przyspieszaniu sieci neuronowych oraz w transformacjach losowych dla redukcji wymiarowości.

Macierz Hadamarda jest używana do osadzania obliczeń niskiej precyzji w sieciach neuronowych. W binary neural networks (BNN) transformacja Hadamarda może zastąpić kosztowne mnożenia. Park i Lee proponują wykorzystanie transformacji Hadamarda na wejściu sieci, dzięki czemu zaawansowane konwolucje w BNN-ach można realizować wyłącznie przez operacje dodawania i odejmowania.

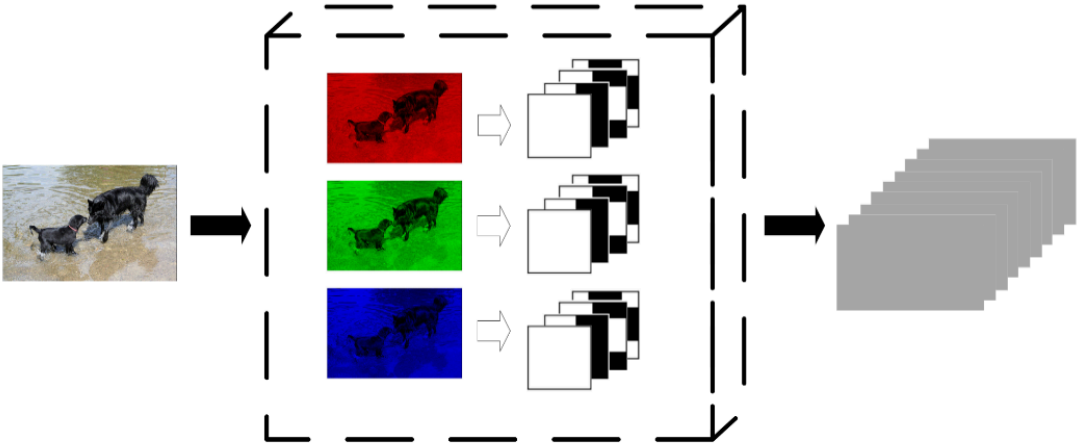

Figure 4: Zastosowanie macierzy Hadamarda jako warstwy wejściowej

W praktyce warstwa wejściowa oparta na macierzy Hadamarda dzieli obraz na bloki i dla każdego bloku przeprowadza szybką 2D-transformatę Hadamarda, uzyskując zbiór współczynników przypominający odpowiedzi filtrów konwolucyjnych.

Rozważmy przykładowy blok 4×4 w kanale R obrazu RGB (wartości od 1 do 16):

$$G = H_4 \times R_4 \times H_4$$

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix} \quad R_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{pmatrix} \quad G = \begin{pmatrix} 136 & -8 & -16 & 0 \\ -32 & 0 & 0 & 0 \\ -64 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Otrzymujemy w ten sposób 16 współczynników dla tego bloku w kanale R. Analogicznie wykonujemy tę procedurę dla bloków w kanale G i B. Każdy blok 4×4 w każdym kanale daje 16 wartości, a więc łącznie $3 \times 16 = 48$ współczynników. Te współczynniki traktujemy jako 48 kanałów wyjściowych (map cech) wygenerowanych przez warstwę Hadamarda