i oznaczamy $C^{-1}$. Na przykład dla macierzy $C = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$ mamy $C^{-1} = \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix}$, bo faktycznie $\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$. Mnożąc obie strony równości $A \cdot C = C \cdot B$ z prawej przez $C^{-1}$ i uwzględniając, że $A \cdot C \cdot C^{-1} = A \cdot I = A$, dostajemy $A = C \cdot B \cdot C^{-1}$. Wówczas dla każdego naturalnego $m$ mamy

$$\begin{aligned} A^m &= A \cdot A \cdot \ldots \cdot A = \\ &= C \cdot B \cdot C^{-1} \cdot C \cdot B \cdot C^{-1} \cdot \ldots \cdot C \cdot B \cdot C^{-1} = \\ &= C \cdot B \cdot I \cdot B \cdot I \cdot \ldots \cdot I \cdot B \cdot C^{-1} = \\ &= C \cdot B \cdot B \cdot \ldots \cdot B \cdot C^{-1} = C \cdot B^m \cdot C^{-1}. \end{aligned}$$

Na przykład dla $A = \begin{bmatrix} -1 & 2 \\ -6 & 6 \end{bmatrix}$ mamy $C = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$ oraz $B = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$. Stąd $A^{100} = C \cdot B^{100} \cdot C^{-1} =$ $= \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2^{100} & 0 \\ 0 & 3^{100} \end{bmatrix} \cdot \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} 2^{101} & 3^{100} \\ 3{\cdot}2^{100} & 2{\cdot}3^{100} \end{bmatrix} \cdot \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix} =$ $= \begin{bmatrix} 2^{102}-3^{101} & -2^{101}+2{\cdot}3^{100} \\ 3{\cdot}2^{101}-2{\cdot}3^{101} & -3{\cdot}2^{100}+4{\cdot}3^{100} \end{bmatrix}$.

**Konkluzja.** Aby obliczyć $A^m$ dla danej macierzy $A \in \mathbf{M}_{n\times n}$, wystarczy znaleźć macierz diagonalną $B \in \mathbf{M}_{n\times n}$ oraz macierz $C \in \mathbf{M}_{n\times n}$ takie, że $A = C \cdot B \cdot C^{-1}$. Wówczas obliczenie $A^m = C \cdot B^m \cdot C^{-1}$ jest proste, bo potęgowanie macierzy diagonalnej $B$ jest proste. W przypadku, gdy macierz $A \in \mathbf{M}_{n\times n}$ ma $n$ różnych wartości własnych $r_1, r_2, \ldots, r_n$, za macierz $C$ można wziąć macierz, której kolumnami są kolejno wektory własne o wartościach własnych $r_1, r_2, \ldots, r_n$. A co jeśli $A \in \mathbf{M}_{n\times n}$ nie ma $n$ różnych wartości własnych? O tym w następnym artykule o potęgowaniu macierzy i twierdzeniu Jordana.

Zauważmy na koniec, że mnożenie macierzy motywowane jest następującą podstawową interpretacją geometryczną. Oznaczmy przez $\mathbb{R}^n$ zbiór wszystkich $n$-wyrazowych ciągów $(x_1, \ldots, x_n)$ liczb rzeczywistych. Przestrzenie $\mathbb{R}^2$ i $\mathbb{R}^3$ to dobrze znane ze szkoły płaszczyzna i przestrzeń 3-wymiarowa. Funkcję $f : \mathbb{R}^n \to \mathbb{R}^m$ nazywamy przekształceniem liniowym, jeśli można ją zapisać wzorem $f(x_1, \ldots, x_n) =$ $= (a_{11}x_1 + \ldots + a_{1n}x_n,\ a_{21}x_1 + \ldots + a_{2n}x_n, \ldots$ $\ldots, a_{m1}x_1 + \ldots + a_{mn}x_n)$ dla pewnej macierzy $A = [a_{ij}] \in \mathbf{M}_{m\times n}$. Na przykład funkcja $f : \mathbb{R}^2 \to \mathbb{R}^2$ zadana wzorem $f(x_1, x_2) = (-x_1 + 2x_2, -6x_1 + 6x_2)$ jest przekształceniem liniowym o macierzy $A = \begin{bmatrix} -1 & 2 \\ -6 & 6 \end{bmatrix} \in \mathbf{M}_{2\times 2}$. Czytelnik łatwo sprawdzi, że złożenie $g \circ f : \mathbb{R}^k \to \mathbb{R}^m$ przekształcenia liniowego $f : \mathbb{R}^k \to \mathbb{R}^n$ o macierzy $B \in \mathbf{M}_{n\times k}$ z przekształceniem liniowym $g : \mathbb{R}^n \to \mathbb{R}^m$ o macierzy $A \in \mathbf{M}_{m\times n}$ jest przekształceniem liniowym o macierzy $A \cdot B$. Przekształcenia liniowe odgrywają kluczową rolę w wielu zastosowaniach matematyki.

# Macierze oczami informatyka

*Jakub RADOSZEWSKI*

## Jak informatyk potęguje macierze?

Poza wyjątkowymi sytuacjami, w których potrzebna jest zwarta postać wzoru na $n$-tą potęgę macierzy $A$ (wymiaru $d$), do obliczenia $A^n$ informatycy stosują zazwyczaj o wiele mniej skomplikowaną metodę niż wyznaczanie wartości własnych – szybkie potęgowanie binarne. Jest to algorytm rekurencyjny, wynikający wprost z poniższych wzorów:

$$A^{2k} = (A^k)^2, \qquad A^{2k+1} = (A^k)^2 \cdot A.$$

Innymi słowy, aby wyznaczyć $A^{2k}$ ($A^{2k+1}$) dla $k \in \mathbb{Z}_+$, obliczamy rekurencyjnie $A^k$, po czym wartość $A^{2k}$ ($A^{2k+1}$) otrzymujemy już za pomocą jednego mnożenia bądź dwóch. Złożoność czasowa tej metody, zakładając najprostszy możliwy algorytm mnożenia macierzy, to $O(d^3 \log n)$.

A o tym, po co informatycy potęgują macierze, opowiem pokrótce w kolejnych paragrafach.

## Ciągi zdefiniowane rekurencyjnie

Załóżmy, że dany jest ciąg $(a_i)_{i=1}^{\infty}$, zdefiniowany za pomocą następującej liniowej zależności rekurencyjnej:

$$a_1 = 1, \quad a_2 = 1, \quad a_3 = 2, \quad a_n = 2a_{n-1} + 3a_{n-2} + a_{n-3} + 4.$$

Wyznaczenie $n$-tego wyrazu tego ciągu (powiedzmy, modulo pewna nieduża liczba $M$) w złożoności czasowej $O(n)$ to dla kogoś obeznanego z programowaniem dynamicznym bułka z masłem. Ale jak obliczyć bilionowy czy trylionowy wyraz tego ciągu? Przyjrzyjmy się wektorowi, który zawiera pewne trzy kolejne wyrazy ciągu $a_i$ oraz stałą 4 (tę z zależności rekurencyjnej):

$$v_n = \begin{bmatrix} a_n \\ a_{n-1} \\ a_{n-2} \\ 4 \end{bmatrix}.$$

Spróbujemy dla $v_n$ znaleźć taką macierz $A$, żeby $A \cdot v_n$ dało analogiczny wektor, ale zawierający wyrazy ciągu o jeden indeks dalsze:

$$v_{n+1} = \begin{bmatrix} a_{n+1} \\ a_n \\ a_{n-1} \\ 4 \end{bmatrix}.$$

W tym celu zauważmy, że

$$v_{n+1} = \begin{bmatrix} 2a_n + 3a_{n-1} + a_{n-2} + 4 \\ a_n \\ a_{n-1} \\ 4 \end{bmatrix}.$$

Przy takim zapisie $v_{n+1}$ wypisanie macierzy $A$ jest już bardzo proste:

$$\begin{bmatrix} 2a_n + 3a_{n-1} + a_{n-2} + 4 \\ a_n \\ a_{n-1} \\ 4 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a_n \\ a_{n-1} \\ a_{n-2} \\ 4 \end{bmatrix}.$$

Aby obliczyć $a_n$, możemy więc zacząć od

$$v_3 = \begin{bmatrix} 2 \\ 1 \\ 1 \\ 4 \end{bmatrix},$$

a następnie wyznaczyć $v_n$ za pomocą równości:

$$v_n = Av_{n-1} = AAv_{n-2} = \ldots = A^{n-3}v_3$$

(wszystkie operacje po drodze wykonujemy modulo $M$). Wówczas wynik odczytujemy z pierwszego elementu $v_n$. Dzięki zastosowaniu szybkiego potęgowania macierzy złożoność czasowa tej metody to $O(\log n)$ – jest więc zdecydowanie bardziej satysfakcjonująca od poprzedniej.

## Ścieżki w grafie

Szybkie potęgowanie macierzy pomaga także rozwiązać problem wyznaczania liczby ścieżek długości $n$ w danym grafie $G = (V, E)$ – zakładamy, że ścieżki mogą przechodzić przez te same wierzchołki czy krawędzie wielokrotnie.

Będziemy mianowicie chcieli obliczyć taką macierz $A(n)$, że $A(n)_{ij}$ jest równe liczbie ścieżek długości $n$, startujących z wierzchołka $i$ i kończących się w $j$. Zauważmy, że $A(1)$ jest po prostu macierzą sąsiedztwa grafu $G$. Przy wyznaczaniu $A(n)$ dla $n > 1$ spróbujemy skorzystać z $A(n-1)$. Ponieważ każda ścieżka z $i$ do $j$ o długości $n$ składa się ze ścieżki z $i$ do jakiegoś wierzchołka $k$ przedłużonej o jedną krawędź $k \to j$, to

$$A(n)_{ij} = \sum_{k=1}^{|V|} A(n-1)_{ik} \cdot A(1)_{kj}.$$

A to oznacza dokładnie tyle, że $A(n) = A(n-1) \cdot A(1)$, czyli $A(n) = A(1)^n$. Korzystając z metody szybkiego potęgowania, otrzymujemy algorytm o złożoności czasowej $O(|V|^3 \log n)$ wyznaczania macierzy $A(n)$, a przez zsumowanie wszystkich jej elementów – liczby wszystkich ścieżek długości $n$.

Ze ścieżkami długości $n$ poszło całkiem gładko, to może da się efektywnie wyznaczyć liczbę ścieżek o długości *nie większej* niż $n$? To pytanie pozostawiam już Czytelnikowi. Podpowiedź – należy obliczyć sumę:

$$A(1) + A(1)^2 + \ldots + A(1)^n,$$

co można zrealizować rekurencyjnie, ale na dwa różne sposoby – jeden lepszy (złożoność czasowa $O(|V|^3 \log n)$), a drugi gorszy (o czynnik $\log n$).

O G Ł O S Z E N I E

**Wakacyjne Warsztaty Wielodyscyplinarne**

... to coroczna impreza organizowana przez studentów UW pod patronatem Koła Naukowego Informatyków UW i Studenckiego Koła Fizyki UW, przeznaczona dla licealistów zainteresowanych matematyką, informatyką, fizyką lub astronomią.

Każdy uczestnik Warsztatów będzie mógł wybrać kilka spośród kilkunastu propozycji kilkudniowych bloków zajęć. Zajęcia będą odbywać się w małych grupach i będą mieć charakter warsztatowy. Obok wykładów bardzo istotna będzie część praktyczna – na zajęciach z programowania funkcyjnego uczestnicy będą wspólnie implementować spory projekt, na zajęciach z astronomii – prowadzić obserwacje astronomiczne dobrym teleskopem... Wieczorami będzie można uczestniczyć w „luźnych” wykładach i prezentacjach, niezwiązanych z żadnym blokiem zajęć, i poruszających różne ciekawe tematy z nauk ścisłych – lub samemu wygłosić taki wykład! A pozanaukowo – integracja, gry i zabawy; dla chętnych przeprowadzimy przyspieszony kurs brydża i go, bardziej zaawansowani gracze będą mogli spróbować swoich sił w turnieju, a każdy będzie mógł zagrać w mafię, ktulu, seta, rpg, planszówki, czy zasiąść z gitarą przy ognisku.

W tym roku planowane są zajęcia m.in. z:
– rachunku kombinatorów,
– algorytmów aproksymacyjnych,
– mechaniki kwantowej,
– geometrycznej teorii grup,
– programowania funkcyjnego,
– grafów losowych...
Domyślny poziom zajęć – dla ambitnego licealisty.

Tegoroczna (już piąta) edycja WWW odbędzie się w dniach 23–30 sierpnia 2009 w Wandzinie koło Lublina. Łączna cena noclegów, pełnego wyżywienia, ubezpieczenia i dojazdu z Lublina nie przekroczy 200 zł.

Więcej informacji na stronie:

`http://warsztatywww.wikidot.com`

Zapraszamy!

## Co jeszcze?

Niniejszy artykuł nie wyczerpuje oczywiście wszystkich sytuacji, w których w informatyce potęguje się macierze. Metody tej używa się, na przykład, przy przyspieszaniu rozwiązań opartych na programowaniu dynamicznym – jak w IKO w *Delcie* 2/2009. Inny, nieco podobny problem tego typu, to zliczanie różnych pokryć prostokąta $4 \times n$ ($n$ może być bardzo duże) za pomocą klocków z Tetrisa (modulo pewna nieduża liczba $M$) – np. dla $n = 3$ istnieją 23 takie pokrycia. To (ciekawe i niełatwe według mnie) zadanie pozostawiam Czytelnikowi, zachęcając do implementacji wymyślonego algorytmu. W razie kłopotów rozwiązanie w postaci programu można znaleźć na stronie internetowej *Delty*.