Jest to tekst związany z odczytem wygłoszonym na XLVI Szkole Matematyki Poglądowej, *Podejście niestandardowe*, Warszawa–Miedzeszyn, styczeń 2011.

Grafy i macierze

Tomasz LENARCIK, Kraków

Streszczenie

Zdarza się, że na pytania dotyczące grafów prościej jest odpowiedzieć, gdy wyrazi się je w języku algebry liniowej. Wydaje się natomiast, że rzadziej (o ile w ogóle) ma miejsce sytuacja odwrotna. Okazuje się jednak, że pewne twierdzenia dotyczące macierzy mają zupełnie przekonującą interpretację w języku grafów i co więcej można je w tym języku stosunkowo łatwo dowodzić. Aby przekonać się o tym na własnej skórze, zaprezentujemy „teorio–grafowy" dowód twierdzenia Cayley'a–Hamiltona.

1. Wstęp

Zacznijmy od przykładu. Załóżmy, że ξ jest liczbą algebraiczną spełniającą równanie postaci

$$0 = f(\xi) = \xi^n + a_1\xi^{n-1} + \ldots + a_{n-1}\xi + a_n,$$

gdzie $f \in \mathbb{Q}[X]$ jest pewnym wielomianem nierozkładalnym. Wiadomo, że w takiej sytuacji najmniejsze ciało zawierające ξ, tj. $\mathbb{Q}(\xi)$, jest n-wymiarową przestrzenią wektorową nad $\mathbb{Q}$. Przykładowo, możemy wziąć bazę

$$1,\ \xi,\ \xi^2,\ \ldots,\ \xi^{n-1}. \tag{1}$$

Zauważmy teraz, że macierz odwzorowania liniowego

$$\mathbb{Q}(\xi) \ni x \longmapsto \xi x \in \mathbb{Q}(\xi).$$

wyrażona w bazie (1) ma następującą postać:

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_1 & -a_2 & -a_3 & \cdots & -a_n \end{bmatrix}.$$

Łatwo sprawdzić, że jej wielomian charakterystyczny jest równy[1]

$$p_A(X) = (-1)^n f(X).$$

Ponieważ A reprezentuje odwzorowanie (liniowe) „mnożenia przez ξ", oraz $f(\xi) = 0$, to również $0 = f(A) = p_A(A)$. Czyli A jest „pierwiastkiem" swojego wielomianu charakterystycznego. Oczywiście macierz A ma bardzo szczególną postać, ale naturalnie narzuca się pytanie czy nie jest to przypadkiem ogólna własność macierzy. Pozytywnej odpowiedzi udziela następujące twierdzenie:

Twierdzenie 1 (Cayley–Hamilton). *Niech A będzie macierzą kwadratową o współczynnikach w (dowolnym!) pierścieniu R i niech $p_A \in R[X]$ będzie jej wielomianem charakterystycznym. Wówczas $p_A(A) = 0$.*

Twierdzenie to ma wiele klasycznych dowodów, zwykle czysto algebraicznych. Odchodząc zatem od standardów, chcielibyśmy zaprezentować Czytelnikowi dowód (zob. [1]), który dla odmiany jest dość mocno osadzony w teorii grafów.

---

[1] Przypomnijmy, że w ogólnej sytuacji wielomian charakterystyczny macierzy $B = [b_{ij}]_{i,j=1\ldots n}$ jest dany wzorem:

$$p(X) := \det(B - X \cdot \mathrm{Id}) = \begin{vmatrix} b_{11} - X & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} - X & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} - X \end{vmatrix}$$

Proszę zwrócić uwagę, że zmienna X pełni tutaj rolę skalara; w szczególności jeżeli weźmiemy jakąś inną macierz C to wcale nie musi zachodzić równość $p(C) = \det(B - C)$.

2. Definicje i oznaczenia

Definicja. *Grafem (skierowanym)* [2] będziemy nazywali parę $G = (V, E)$, gdzie V jest dowolnym zbiorem skończonym natomiast E jest relacją na V, czyli $E \subset V \times V$. Powiemy, że wierzchołki v_1, v_2 są połączone krawędzią (od v_1 do v_2) jeśli $(v_1, v_2) \in E$. Jeśli dodatkowo określono odwzorowanie

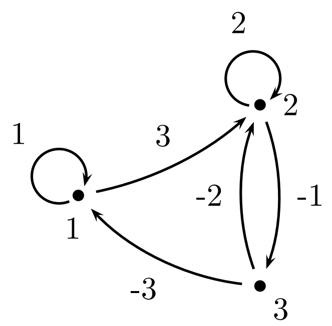
$$\omega : E \longrightarrow R \setminus \{0\}$$

to mówimy, że mamy do czynienia z *grafem ważonym.* Przyjmujemy konwencję, że jeżeli graf nie ma wag zadanych w sposób jawny, to i tak traktujemy go jako graf ważony, w którym każda krawędź ma wagę 1.

Z pewnych względów wygodnie będzie nam zakładać, że elementy zbioru V zostały w pewien sposób uporządkowane. Dla uproszczenia notacji przyjmijmy po prostu, że

$$V = \{1, 2, \ldots, n\}.$$

Dzięki temu, z dowolnym grafem ważonym rozpiętym na wierzchołkach V możemy skojarzyć tzw. *macierz sąsiedztwa* $A \in M(n \times n; R)$ określoną w taki sposób, że wartość w i-tym wierszu i w j-tej kolumnie jest równa wadze krawędzi (j, i), gdy ta należy do grafu, oraz zero w przeciwnym przypadku.



macierz sąsiedztwa

$$\begin{pmatrix} 1 & 0 & -3 \\ 3 & 3 & -2 \\ 0 & -1 & 0 \end{pmatrix}$$

Rys. 1. Graf ważony i odpowiadająca mu macierz sąsiedztwa.

Odwrotnie, każdej macierzy $A \in M(n \times n; R)$ możemy na tej samej zasadzie przypisać pewien graf ważony. Co więcej, operacje te są wzajemnie odwrotne.[3]

Definicja. *Drogą* (lub *ścieżką*) w grafie $G = (V, E)$ będziemy nazywali taki ciąg krawędzi (dopuszczamy ciąg pusty!) $e_1, \ldots, e_k \in E$, że koniec e_i pokrywa się z początkiem e_{i+1} dla $i = 1, \ldots, k$. Liczbę k nazywamy długością drogi. Każda niepusta droga ma wierzchołek początkowy i wierzchołek końcowy. Drogę (niepustą), która rozpoczyna się i kończy w tym samym wierzchołku nazywamy *pętlą.*

Jeżeli $P = (e_1, \ldots, e_k)$ jest drogą w grafie ważonym (G, E, ω), to definiujemy łączną *wagę* drogi jako

$$\omega(D) = \omega(e_1) \cdots \omega(e_k) \in R.$$

Podobnie, jeśli $H = (V_H, E_H)$ jest podgrafem G, to definiujemy *wagę* H jako

$$\omega(H) = \prod_{e \in E_H} \omega(e).$$

Przyjmujemy również konwencję, że $\omega(\emptyset) = 1$.

---

[2] Dalej będziemy pisali po prostu „graf” mając na myśli graf skierowany.
[3] Dzięki temu, że zażądaliśmy aby wagi krawędzi były niezerowe.

Niech G będzie grafem, oraz A jego macierzą sąsiedztwa.[4] Prosta indukcja pozwala sprawdzić następującą własność:

$$(2) \qquad (A^k)_{ij} = \text{ liczba dróg o długości } k \text{ od wierzchołka } j \text{ do wierzchołka } i.$$

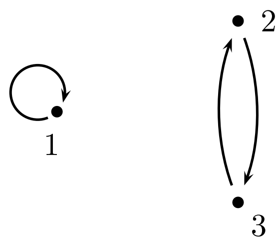
Ogólnie, tj. dla dowolnego grafu ważonego, mamy następujący fakt:

Fakt 2. *Jeżeli G jest grafem ważonym i A jego macierzą sąsiedztwa, to dla każdego $k \geqslant 1$ mamy $(A^k)_{ij} =$ suma wag wszystkich dróg długości k zaczynających się w j-tym wierzchołku a kończących się w i-tym.*

Uwaga. Ponieważ pojawiają się tutaj potęgi macierzy, to intuicja podpowiada, że przy badaniu pewnych własności grafu istotną rolę muszą odegrać wartości własne i postać Jordana macierzy sąsiedztwa.

Z dowolną permutacją σ zbioru $V = \{1, \ldots, n\}$ możemy skojarzyć odwzorowanie liniowe $\overline{\sigma}$ „mieszające" wektory bazy kanonicznej w ten sposób, że $e_i \longmapsto e_{\sigma(i)}$. Przyporządkowanie to pozwala widzieć S_n jako podgrupę $\mathrm{GL}_n(\mathbb{K})$ gdzie $\mathbb{K}$ jest dowolnym ciałem.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$



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

Z drugiej strony każdej permutacji odpowiada graf (skierowany!), z którym możemy skojarzyć macierz sąsiedztwa. Nie budzi zaskoczenia, że jest to ta sama macierz, która reprezentuje σ jako element $\mathrm{GL}_n(\mathbb{K})$. W dalszym ciągu będziemy mówili po prostu o macierzy $P = P(\sigma)$ skojarzonej z permutacją σ. Mamy następujące własności

(i) Zachodzą wzory

$$\mathrm{tr}P = \text{ liczba punktów stałych } \sigma, \quad \det P = \mathrm{sgn}\sigma.$$

(ii) Jeżeli σ rozpada się na k-cykli, tak że i-ty cykl ma n_i elementów, to wielomian charakterystyczny P wyraża się wzorem

$$p(\lambda) = (-1)^n \cdot (\lambda^{n_1} - 1) \cdots (\lambda^{n_k} - 1).$$

(iii) Rozkład na cykle odpowiada rozkładowi na podprzestrzenie niezmiennicze względem działania $\overline{\sigma}$, a wektory własne związane z n_i-elementowym cyklem są postaci

$$(1, \xi, \xi^2, \ldots, \xi^{n_i - 1})$$

gdzie ξ jest dowolnym pierwiastkiem stopnia n_i z jedynki.[5]

[4] Przypomnijmy, że wagi krawędzi są domyślnie równe 1, czyli w tym wypadku w macierzy sąsiedztwa występują zera i jedynki.

[5] W szczególności, jeżeli pracujemy nad ciałem charakterystyki zero, bądź wszystkie n_i są względnie pierwsze z charakterystyką to macierz P jest diagonalizowalna (bo wtedy, w algebraicznym domknięciu jest dokładnie n_i różnych pierwiastków stopnia n_i z jedynki). Podkreślmy jeszcze, że założenie o charakterystyce jest istotne. Przykładowo, dla $\mathbb{K} = \mathbb{Z}/2$ mamy

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

czyli postać Jordana nie jest diagonalna!

3. Obliczanie wielomianu charakterystycznego

Opiszemy teraz w języku grafów procedurę obliczania wyznacznika, dzięki czemu będziemy w stanie wyrazić w dogodny sposób współczynniki wielomianu charakterystycznego. Przypomnijmy, że ogólnie dla $A = (a_{ij}) \in M(n \times n; R)$ mamy

$$\det A = \sum_{\sigma \in S_n} (\mathrm{sgn}\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

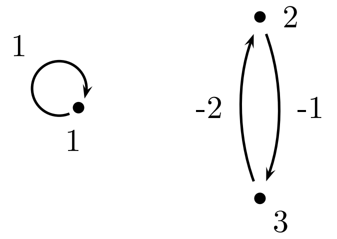
otrzymujemy stąd natychmiast następujący fakt:

Fakt 3. *Niech G będzie grafem ważonym o n wierzchołkach, a A skojarzoną z nim macierzą sąsiedztwa. Wówczas*

$$\det A = \sum_{\sigma} \mathrm{sgn}\sigma \cdot \omega(\sigma) = (-1)^n \sum_{\sigma} (-1)^{c(\sigma)} \omega(\sigma), \tag{3}$$

gdzie sumowanie przebiega po wszystkich podgrafach G, które są grafami permutacji rozpiętymi na n wierzchołkach, oraz $c(\sigma)$ oznacza liczbę cykli w σ. Druga równość wynika z faktu, że liczba nieparzystych cykli permutacji przystaje do n modulo 2.

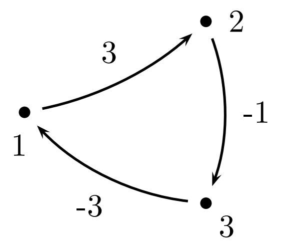
Przykład. Wykorzystując wzór (3) sprawdźmy, że wyznacznik macierzy przedstawionej na rysunku 1 jest równy 7. Mamy dokładnie dwa podgrafy, które są grafami permutacji:



macierz sąsiedztwa

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

$\mathrm{sgn}\,\sigma_1 \cdot \omega(\sigma_1) =$
$(-1) \cdot 1 \cdot (-1) \cdot (-2) = -2$



macierz sąsiedztwa

$$\begin{pmatrix} & & -3 \\ 3 & & \\ & -1 & \end{pmatrix}$$

$\mathrm{sgn}\,\sigma_2 \cdot \omega(\sigma_2) =$
$(+1) \cdot 3 \cdot (-1) \cdot (-3) = 9$

Ze wzoru (3) dostajemy:

$$\det(A + \lambda I) = (-1)^n \sum_{i=0}^{n} \left((-1)^i \sum_{\#\sigma = n-i} (-1)^{c(\sigma)} \omega(\sigma) \right) \lambda^i$$

gdzie drugie sumowanie przebiega po wszystkich podgrafach G, które są grafami permutacji rozpiętymi na $n - i$ wierzchołkach. Porządkując wyrazy w powyższej sumie otrzymujemy zatem

Fakt 4. *Niech G będzie grafem ważonym o n wierzchołkach i A skojarzoną macierzą sąsiedztwa. Wówczas*

$$\det(A - \lambda I) = (-1)^n \sum_{i=0}^{n} \left(\sum_{\#\sigma = n-i} (-1)^{c(\sigma)} \omega(\sigma) \right) \lambda^i. \tag{4}$$

4. Dowód twierdzenia Cayley'a–Hamiltona

Mamy już wszystkie niezbędne narzędzia, przejdźmy zatem do dowodu głównego twierdzenia. Weźmy dowolną macierz A i niech G będzie skojarzonym grafem ważonym. Dla uproszczenia oznaczmy $p := p_A$. Chcemy pokazać, że $p(A)$ jest macierzą zerową. Ze wzoru (4) mamy

$$p(A)_{ij} = (-1)^n \sum_{k=0}^{n} \left(\sum_{\#\sigma = n-k} (-1)^{c(\sigma)} \omega(\sigma) \right) (A^k)_{ij}.$$

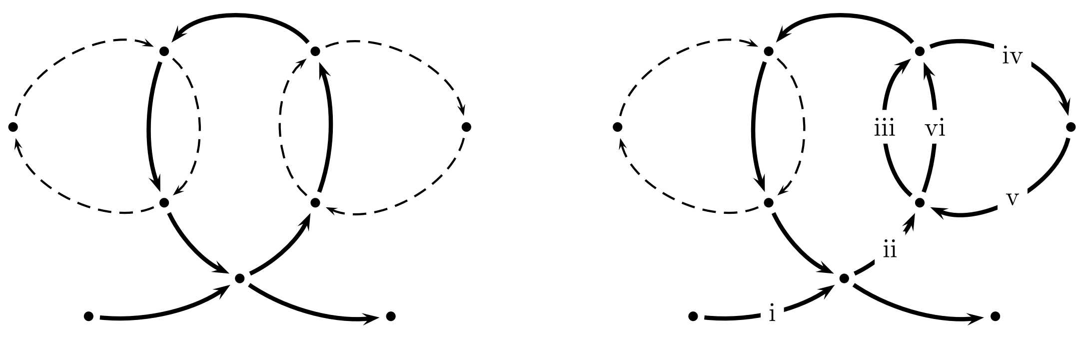
Przypomnijmy, że $(A^k)_{ij} = \sum_{\#P=k} \omega(P)$ gdzie sumowanie przebiega po wszystkich drogach w grafie G zaczynających się j i kończących w i. Wystarczy zatem sprawdzić, że zeruje się następujące wyrażenie:

$$\sum_{k=0}^{n} \left[\left(\sum_{\#\sigma=n-k} (-1)^{c(\sigma)} \omega(\sigma) \right) \cdot \left(\sum_{\#P=k} \omega(P) \right) \right] = \sum_{\#P+\#\sigma=n} (-1)^{c(\sigma)} \omega(\sigma) \omega(P), \tag{5}$$

przy czym ostatnie sumowanie przebiega po wszystkich takich parach P, σ, że P jest drogą łączącą wierzchołek j z wierzchołkiem i, σ jest podgrafem G, który jest jednocześnie grafem pewnej permutacji oraz łączna liczba krawędzi w P i σ wynosi n.[6] Pokażemy, że składniki w (5) można pogrupować w pary sumujące się do zera.

Weźmy zatem P, σ i załóżmy najpierw, że P i σ nie mają wspólnych wierzchołków. Z zasady szufladkowej Dirichleta wynika, że istnieje wierzchołek, przez który P przechodzi (co najmniej) dwukrotnie.[7] Idąc wzdłuż drogi P weźmy ostatni taki wierzchołek i oznaczmy przez P' pętlę jaką zatacza w nim droga P. Ponieważ każdy następny wierzchołek jest już „odwiedzany" jednokrotnie, to pętla P' nie ma samoprzecięć. Możemy zatem utworzyć nową permutację, którą oznaczymy przez $\sigma \cup P'$,[8] dodając do σ cykl reprezentowany przez P' oraz nową drogę, ozn. $P \setminus P'$, poprzez usunięcie z P pętli P'. Zauważmy wreszcie, że

$$(-1)^{c(\sigma)} \omega(\sigma) \omega(P) + (-1)^{c(\sigma \cup P')} \omega(\sigma \cup P') \omega(P \setminus P') = 0.$$



Rozważmy teraz sytuację odwrotną, tj. załóżmy, że droga P i permutacja σ mają wspólne wierzchołki. Weźmy zatem „ostatni" z nich (licząc wzdłuż drogi) i niech C będzie cyklem permutacji σ, do którego ten wierzchołek należy.[9] Następnie rozszerzmy drogę P o pętlę C i rozważmy nową permutację „$\sigma \setminus C$". Podobnie jak wcześniej obserwujemy, że

$$(-1)^{c(\sigma)} \omega(\sigma) \omega(P) + (-1)^{c(\sigma \setminus C)} \omega(\sigma \setminus C) \omega(P \cup C) = 0.$$

Dla zakończenia dowodu pozostaje zauważyć, że operacje opisane powyżej są wzajemnie odwrotne, dzięki czemu mamy gwarancję, że składniki sumy (5) rzeczywiście zostaną połączone w pary.

---

[6] Zwróćmy uwagę, że niektóre krawędzie w P mogą być liczone wielokrotnie.
[7] Zauważmy, że jeżeli $k = \#P$, to P „odwiedza" $k+1$ wierzchołków.
[8] Oczywiście nie jest to zapis formalnie poprawny.
[9] Może to być nawet cykl jednoelementowy!

5. Ciąg dalszy

Zainteresowanego Czytelnika zachęcamy do udowodnienia jeszcze jednego twierdzenia dotyczącego macierzy.

Twierdzenie 5 (Amistur–Levitzki)**.** *Niech* $A_1, \ldots, A_{2n}$ *będą macierzami* $n \times n$*, o współczynnikach w pierścieniu* R*. Wówczas*

$$\sum_{\sigma \in S_{2n}} A_{\sigma(1)} \cdots A_{\sigma(2n)} = 0.$$

Choć na pierwszy rzut oka może się to wydać zaskakujące, istnieje dowód w podobnym duchu jak zaprezentowany tutaj dowód twierdzenia Cayley'a-Hamiltona. Warto wykorzystać następujący fakt:

Twierdzenie 6 (Swan)**.** *Niech* $G = (V, E)$ *będzie takim grafem, że* $k := |E| \geqslant 2|V|$*. Załóżmy dodatkowo, że krawędzie grafu ponumerowano liczbami od* 1 *od* k*. Z każdą drogą Eulera* P *możemy dzięki temu skojarzyć permutację* $\sigma(P) \in S_k$*. Wówczas dla dowolnych (niekoniecznie różnych) wierzchołków* $v_1, v_2 \in V$ *liczba dróg Eulera* P *od* v_1 *do* v_2*, dla których* $sgn \sigma(P) = 1$*, jest równa liczbie dróg Eulera* P *od* v_1 *do* v_2*, dla których* $sgn \sigma(P) = -1$*.*

Dowód. Zob. [3].

Literatura

[1] R. A. Brualdi, D. Cvetković, *A combinatorial approach to matrix theory and its applications*, CRC Press (2009)

[2] I. N. Ponomarenko, *Graph Algebras and the Graph Isomorphism Problem*, Applicable Algebra in Engineering, Vol. 5 (1994), pp. 277-286

[3] R. G. Swan, *An Application of Graph Theory to Algebra*, Proc. of the AMS, Vol. 14, No. 3 (Jun., 1963), pp 367-373