O prawdopodobieństwie, wyznacznikach i pokryciach cyklowych

Wojciech NADARA[*]

Jest to skrót pracy uczniowskiej nagrodzonej złotym medalem w XXXIII Konkursie Prac Uczniowskich z Matematyki w 2011 roku (Łódź).

W tym artykule będziemy się zajmowali obliczaniem wyznaczników macierzy w dowolnym skończonym ciele F. Będziemy także badali, jakie jest prawdopodobieństwo, że taki wyznacznik dla macierzy z losowo wpisanymi elementami z ciała F jest różny od 0, oraz jakie jest prawdopodobieństwo, że w losowym grafie skierowanym jest nieparzyście wiele pokryć cyklowych.

Jeżeli mamy daną macierz kwadratową z wpisanymi w nią elementami ciała F, to ciężko na pierwszy rzut oka stwierdzić, czy jej wyznacznik jest zerowy, czy nie. Sprawa okazuje się dużo prostsza, gdy mamy do czynienia z macierzą w postaci schodkowej (tzn. z taką, która ma zera poniżej głównej przekątnej). Wyznacznik takiej macierzy jest zerowy wtedy i tylko wtedy, gdy na jej głównej przekątnej znajduje się co najmniej jedno 0. Aby sprowadzić naszą macierz do postaci schodkowej, użyjemy metody eliminacji Gaussa. Będziemy wykonywać dwa rodzaje operacji. Pierwszym będzie zamiana dwóch wierszy miejscami, a drugim będzie dodanie do ustalonego wiersza innego wiersza pomnożonego przez stałą. Jak wiadomo, operacja drugiego rodzaju nie zmienia wyznacznika macierzy, operacja pierwszego rodzaju natomiast zmienia jego znak, a więc nie zmienia tego, czy wyznacznik jest zerowy, czy nie.

```
function gauss(A, n)
  for i := 1 to n do
    for j := i + 1 to n do
      if A[j, i] ≠ 0 then
        swap(A[i], A[j]);
    if A[i, i] = 0 then return 0;
    for j := i + 1 to n do
      for k := i to n do
        A[j, k] := A[j, k]
                 − A[i, k] · (A[j, i]/A[i, i]);
  return 1;
```

Algorytm eliminacji Gaussa dla macierzy A rozmiaru $n \times n$, indeksowanej $A[wiersz, kolumna]$. Funkcja zwraca 0 lub 1 w zależności od tego, czy wyznacznik macierzy jest zerowy, czy też nie (przyp. red.).

Sprowadzając macierz do postaci schodkowej, najpierw musimy zadbać o to, aby w górnym lewym rogu naszej macierzy znalazł się jakiś niezerowy element. Jeżeli w pierwszej kolumnie są same zera, to przerywamy nasz algorytm, gdyż wyznacznik naszej macierzy na pewno jest równy 0. W przeciwnym przypadku, jeżeli w górnym lewym rogu jest już niezerowy element, to nic nie robimy, a jeśli nie, to zamieniamy pierwszy wiersz z którymś, w którym w pierwszej kolumnie znajduje się niezerowy element. Następnie musimy zadbać o to, aby w tej kolumnie nie było więcej niezerowych elementów, zatem jeżeli w górnym lewym rogu znajduje się element a, a w innym wierszu w pierwszej kolumnie znajduje się element b, to musimy do tego wiersza dodać pierwszy wiersz pomnożony przez $\frac{-b}{a}$. Zatem zrobiliśmy już wszystko, co mieliśmy zrobić z pierwszym wierszem i pierwszą kolumną, i dalej ograniczamy się do reszty naszej macierzy, dla której powtarzamy to postępowanie. Kończymy je w momencie, gdy w macierzy, która nam pozostała, w pierwszej kolumnie są same zera (wtedy wyznacznik równa się 0) lub gdy szczęśliwie dojdziemy do końca (wtedy wyznacznik jest niezerowy).

Jak ta metoda może nam pomóc w obliczeniu prawdopodobieństwa, że dla kwadratowej macierzy A rozmiaru $n \times n$, w której każde pole jest wpisany z równym prawdopodobieństwem jakiś element ciała F, jej wyznacznik jest niezerowy? Oznaczmy liczbę elementów ciała F przez q. Zastanówmy się najpierw, jakie jest prawdopodobieństwo tego, że będziemy mogli wykonać pierwszą fazę algorytmu, czyli że w pierwszej kolumnie znajdzie się jakiś niezerowy element. Abyśmy nie mogli jej wykonać, w każdym z n pól pierwszej kolumny musi znaleźć się 0, a znajduje się ono w każdym polu z prawdopodobieństwem $\frac{1}{q}$. Zatem prawdopodobieństwo tego, że będziemy mogli wykonać pierwszą fazę algorytmu, wynosi $1 - \frac{1}{q^n}$. Nietrudno przekonać się o tym, że nie tylko w pierwszej, ale w dowolnej, i-tej fazie algorytmu, rozkład prawdopodobieństwa wartości znajdujących się w polach i-tej kolumny, jest jednostajny. Stosując analogiczną argumentację wnioskujemy, iż prawdopodobieństwo tego, że będziemy mogli wykonać i-tą fazę, o ile będziemy mogli wykonać pierwsze $i-1$ faz, jest równe

$$1 - \frac{1}{q^{n-i+1}}.$$

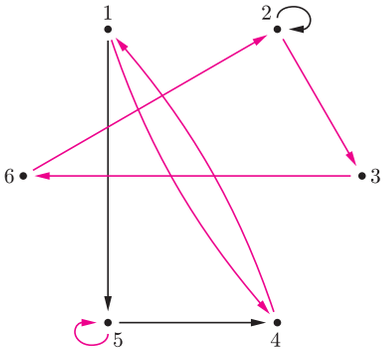
Jeżeli rozkład prawdopodobieństwa dla pewnego pola jest jednostajny, to dodanie ustalonej liczby do liczby w tym polu lub pomnożenie jej przez niezerową liczbę zachowuje jednostajność rozkładu, gdyż dodawanie i mnożenie są w ciele operacjami odwracalnymi.

[*]XIV LO im. Stanisława Staszica, Warszawa

Stąd otrzymujemy końcowy wynik, że prawdopodobieństwo wykonania całego algorytmu, czyli prawdopodobieństwo tego, że wyznacznik macierzy będzie różny od 0, jest równe

$$\left(1-\frac{1}{q^n}\right)\left(1-\frac{1}{q^{n-1}}\right)\dots\left(1-\frac{1}{q}\right).$$

Zajmijmy się teraz następującym problemem. Rozważmy graf skierowany o n wierzchołkach, w którym dla każdej uporządkowanej pary liczb (i,j), takiej że $1\leqslant i,j\leqslant n$, krawędź skierowana od wierzchołka i do wierzchołka j występuje z prawdopodobieństwem $\frac{1}{2}$ (w szczególności, w tym grafie mogą występować pętle). Jakie jest prawdopodobieństwo tego, że w tym grafie jest nieparzysta liczba pokryć cyklowych?



$$A=\begin{pmatrix}0&0&0&\mathbf{1}&1&0\\0&1&\mathbf{1}&0&0&0\\0&0&0&0&0&\mathbf{1}\\\mathbf{1}&0&0&0&0&0\\0&0&0&1&\mathbf{1}&0\\0&\mathbf{1}&0&0&0&0\end{pmatrix}$$

Przykładowy graf o sześciu wierzchołkach i jego macierz sąsiedztwa. Na rysunku zaznaczono jedno z dwóch pokryć cyklowych tego grafu, odpowiadające permutacji

$$\sigma=\begin{pmatrix}1&2&3&4&5&6\\4&3&6&1&5&2\end{pmatrix}.$$

A czym właściwie są pokrycia cyklowe? Otóż pokrycie cyklowe to taki zbiór n krawędzi grafu, że z każdego wierzchołka wychodzi dokładnie jedna krawędź i do każdego wierzchołka wchodzi dokładnie jedna krawędź z tego zbioru. Przedstawia się ono jako zbiór rozłącznych cykli o łącznej długości n. Każde pokrycie cyklowe możemy utożsamiać z n-elementową permutacją σ, w której $\sigma(i)$ jest numerem wierzchołka, do którego wchodzi krawędź wychodząca z wierzchołka o numerze i. Natomiast permutacja σ reprezentuje pokrycie cyklowe, jeżeli dla każdego $i=1,2,\dots,n$ istnieje krawędź z wierzchołka i do wierzchołka $\sigma(i)$.

Zapiszmy nasz graf w postaci macierzy sąsiedztwa A, czyli macierzy kwadratowej o wymiarach $n\times n$, w której w polu (i,j) jest 1, jeżeli istnieje krawędź od wierzchołka i do wierzchołka j, a w przeciwnym przypadku jest tam 0. A jak na tę macierz przenoszą się pokrycia cyklowe? Rozpatrzmy pewne pokrycie cyklowe i zaznaczmy w naszej macierzy pola odpowiadające krawędziom należącym do pokrycia. Będzie to n takich pól, że żadne dwa pola nie znajdują się w tym samym wierszu ani w tej samej kolumnie i, w dodatku, wszystkie te pola mają wartość 1. Zatem iloczyn liczb w tych polach będzie równy 1. A co dzieje się z permutacjami, którym nie odpowiadają pokrycia cyklowe? Jeżeli zaznaczymy w analogiczny sposób w naszej macierzy pola odpowiadające potencjalnym krawędziom z tej permutacji, to skoro nie reprezentowała ona pokrycia cyklowego, to w co najmniej jednym zaznaczonym polu znajdzie się 0. W takim razie iloczyn liczb w tych polach będzie równy 0. Możemy zatem wysunąć wniosek, że liczba pokryć cyklowych w tym grafie jest równa

$$\sum_{\sigma\in S_n} a_{1,\sigma(1)}a_{2,\sigma(2)}\dots a_{n,\sigma(n)},$$

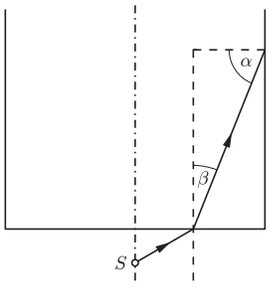
gdzie S_n to zbiór wszystkich n-elementowych permutacji, a $a_{i,j}$ to wartość pola (i,j) w macierzy sąsiedztwa. Powyższą liczbę nazywa się też permanentem macierzy A. Przypatrzmy się teraz wzorowi permutacyjnemu na wyznacznik macierzy:

$$\det A=\sum_{\sigma\in S_n}(-1)^{\mathrm{Inv}(\sigma)}a_{1,\sigma(1)}a_{2,\sigma(2)}\dots a_{n,\sigma(n)},$$

gdzie $\mathrm{Inv}(\sigma)$ jest liczbą inwersji w permutacji σ, ale dla nas istotne będzie to, że $(-1)^{\mathrm{Inv}(\sigma)}$ może przyjmować tylko wartości 1 i -1, a skoro te dwie liczby są tej samej parzystości, zatem permanent i wyznacznik macierzy całkowitoliczbowej są tej samej parzystości. Zauważmy jeszcze, że to, czy wyznacznik takiej macierzy sąsiedztwa jest parzysty, to po prostu pytanie, czy wyznacznik tej macierzy jest zerowy, jeżeli potraktujemy macierz sąsiedztwa jako macierz nad ciałem $\mathbb{Z}_2$. W dodatku, sposób, w jaki losowaliśmy krawędzie grafu, odpowiada sposobowi, w jaki losowaliśmy elementy macierzy we wcześniejszej części artykułu. Z połączenia tych faktów otrzymujemy wniosek, że prawdopodobieństwo tego, że liczba pokryć cyklowych naszego grafu jest nieparzysta, jest równe

$$\left(1-\frac{1}{2^n}\right)\left(1-\frac{1}{2^{n-1}}\right)\dots\left(1-\frac{1}{2}\right).$$

Rozwiązanie zadania F 808.
Przez boczną powierzchnię cylindra nie wydostanie się żaden promień światła, jeśli dla promienia o (skrajnym) kącie padania $\pi/2$ na dno cylindra kąt padania α na powierzchnię boczną będzie spełniał nierówność $\sin\alpha>1/n$.



W tym przypadku na powierzchni bocznej nastąpi całkowite odbicie. Z geometrii układu wynika, że

$$\sin\alpha=\sqrt{1-\sin^2\beta},\qquad \sin\beta=1/n.$$

Stąd

$$n_{\min}=\sqrt{2}.$$