Problem Skolema

*Marcin Wierzbiński**

Student, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Wiele matematycznych problemów ma bardzo proste sformułowanie, ale ich istota dotyka głębokiej matematyki. Przykładem takiego problemu jest tytułowy problem Skolema. Sformułowanie wydaje się bliskie informatyce teoretycznej, zainteresowany czytelnik znający tzw. problem stopu, może zauważyć tutaj analogię. Natomiast techniki służące do rozwiązania problemu pochodzą z algebry i, na dodatek, pełne rozwiązanie wymagałoby istotnych postępów w tej dziedzinie.

Kolejne wyrazy ciągu Fibonacciego: $0, 1, 1, 2, 3, 5, 8, 13, \ldots$

Zacznijmy od rozważenia takiego oto pytania: Czy dany liniowy ciąg rekurencyjny (np. ciąg Fibonacciego (1)) ma pewien wyraz równy zero? Każdy bez trudu odpowie na to pytanie dla ciągu Fibonacciego,. Tylko dla $n = 0$ wyraz $F_0 = 0$ jest równy zero.

$$\begin{cases} F_n = F_{n-1} + F_{n-2} \\ F_1 = 1 \\ F_0 = 0 \end{cases} \tag{1}$$

Kolejne wyrazy dla tego ciągu to: 0, 1, 2, 1, -4, -11, -10, 13, 56, 73, -22, -263 ...

Kolejne wyrazy ciągu Fibonacciego F_n zawsze będą dodatnie (suma wyrazów dodatnich jest dodatnia). Nie potrzebujemy do tego zaawansowanej matematyki. Czy odpowiedź na to pytanie dla dowolnego ciągu jest taka prosta? Rozważmy na przykład następujący ciąg:

$$\begin{cases} u_n = 2u_{n-1} - 3u_{n-2} \\ u_1 = 1 \\ u_0 = 0 \end{cases} \tag{2}$$

Na pierwszy rzut oka, problem nie jest łatwy do rozstrzygnięcia. Wypisując kolejne wyrazy, możemy wysnuć hipotezę, że owy ciąg również poza pierwszym nie ma wyrazu zerowego. Problem można sformułować w ogólności, dla większej ilości równań. W tym artykule postaramy się pokazać, że już dla prostych równań za rozwiązaniem stoi ciekawa matematyka.

Problem Skolema

Liniowa rekurencja jest fundamentem wielu pojęć w informatyce czy kombinatoryce.

Wprowadźmy potrzebne definicje. Liniowy ciąg rekurencyjny to ciąg liczb całkowitych $u_0, \ldots, u_{k-1} \in \mathbb{Z}$, taki, że dla pewnych $a_0 \neq 0$ $a_0, \ldots, a_{k-1} \in \mathbb{Z}$ oraz dla każdego $n \in \mathbb{N}$, $n \geq k$ mamy $u_n = a_0 u_{n-1} + a_1 u_{n-2} + \ldots + a_{k-1} u_{n-k}$. Rząd takiego układu to k.

Albert Thoralf Skolem (ur. 23 maja 1887 w Sandsvaer, zm. 23 marca 1963)

Problem Skolema, to pytanie, czy dla danego liniowego ciągu rekurencyjego, istnieje takie n, że $u_n = 0$?

Obecnie znane są rezultaty dla liniowych równań rzędu $2, 3$ i 4, dla których umiemy sprawdzić, czy dane liniowe równanie rekurencyjne dla pewnego n ma wyraz zerowy. W szczególności, rozstrzygalność problemu Skolema pozostaje nadal otwarta dla rzędu 5. Znamy natomiast rozstrzygalność różnych podprzypadków dla rzędu 5.

Okazuje się, że już dla równań rzędu 2 rozwiązanie jest nietrywialne. W artykule postaramy się przedstawić intuicje stojące za ową nietrywialnością. Zacznijmy od zapisu macierzowego dla liniowego równania rekurencyjnego. Każdy ciąg liniowy rekurencyjny można zapisać w postaci:

$$u_n = v^T M^n w, \tag{3}$$

Opisana redukcja jest bardzo użyteczna. Wiemy, że potęgowanie liczby x do n można wykonać w czasie $\mathcal{O}(\log(n))$. Ta sama zasada stosuje się w przypadku potęgowania macierzy. A zatem korzystając z postaci macierzowej możemy np. obliczyć n-tą liczbę Fibonacciego używając $\mathcal{O}(\log(n))$ operacji arytmetycznych.

gdzie $v, w \in \mathbb{Z}^k, M \in \mathbb{Z}^{k \times k}$, v^T oznacza transpozycje wektora v i odpowiednio:

$$M = \begin{bmatrix} a_{k-1} & 1 & \dots & 0 & 0 \\ a_{k-2} & 0 & \dots & 0 & 0 \\ \vdots & 0 & \dots & 1 & 0 \\ a_1 & 0 & \dots & 0 & 1 \\ a_0 & 0 & \dots & 0 & 0 \end{bmatrix} \quad v = \begin{bmatrix} u_{k-1} \\ u_{k-2} \\ \vdots \\ u_0 \end{bmatrix} \quad w = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

Dla zainteresowanych czytelników: do pokazania równoważności liniowego ciągu rekurencyjnego i postaci macierzowej korzysta się z takich wyników jak rozwinięcie Laplace dla macierzy M i Twierdzenie Cayleya–Hamiltona. W drugą stronę stosuje się indukcje po n.

Przypomnijmy, że wektor v jest *wektorem własnym* macierzy M jeśli $Mv = \lambda v$, czyli intuicyjnie rzecz biorąc przekształcenie M jedynie wydłuża lub skraca v, ale go nie obraca w żaden sposób. Wartość λ jest nazywana *wartością własną* M.

Reprezentacja macierzowa jest wygodną postacią do pracy z liniowymi równaniami rekurencyjnymi. Wymiar macierzy to rząd liniowego równania rekurencyjnego.

Bardzo przydatny dla nas będzie rozkład diagonalny macierzy $M = PDP^{-1}$, gdzie P jest odwracalną macierzą przejścia, jej kolumny to wektory własne M. Jeśli wszystkie wartości własne M są różne, to D jest macierzą diagonalną złożonych z wartości własnych $\lambda_1, \dots \lambda_k$. W przypadku wielokrotnych wartości własnych stosujemy rozkład Jordana, różni się on bardzo niewiele od diagonalnego. Macierz M zapisujemy jako iloczyn $M = PJP^{-1}$, gdzie J ma specjalną postać tzw. klatek Jordana. Dalsze szczególny nie są istotne dla naszego artykułu.

Równania rekurencyjne rzędu 2

W dalszej części przedstawię techniki związane z rozwiązaniem problemu Skolema dla liniowego równania rekurencyjnego rzędu 2. Rozwiązanie będzie zależało od wartości własnych macierzy ciągu. Prześledzimy je na kilku przykładach, które zilustrują techniki rozwiązywania naszego problemu w różnych przypadkach.

Różne moduły wartości własnych
Rozważmy jeszcze raz ciąg Fibonacciego. Na początek zobaczmy jak rozkład macierzy pozwala nam uzyskać wzór jawny na n-ty wyraz ciągu. Korzystając z postaci macierzowej wiemy, że $F_n = (1,0)M^n(0,1)^T$, gdzie macierz M to:

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Macierz M ma dwie wartości własne:

$$\lambda_1 = \frac{1}{2}\left(1 + \sqrt{5}\right), \lambda_2 = \frac{1}{2}\left(1 - \sqrt{5}\right).$$

A zatem

$$M = \underbrace{\begin{bmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{bmatrix}}_{P} \underbrace{\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}}_{D} \underbrace{\begin{bmatrix} 1 & -\lambda_2 \\ -1 & \lambda_1 \end{bmatrix}}_{P^{-1}},$$

z czego wynika, że

$$F_n = v^t M^n w = \frac{1}{\sqrt{5}} \underbrace{\begin{bmatrix} 1 & 0 \end{bmatrix}}_{v^t} \underbrace{\begin{bmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{bmatrix}}_{P} \underbrace{\begin{bmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{bmatrix}}_{D^n} \underbrace{\begin{bmatrix} 1 & -\lambda_2 \\ -1 & \lambda_1 \end{bmatrix}}_{P^{-1}} \underbrace{\begin{bmatrix} 0 \\ 1 \end{bmatrix}}_{w}$$

W ten sposób jawnie wyrażamy n-ty wyraz ciągu Fibonacciego:

$$F_n = \frac{\lambda_1\lambda_2^{n+1} - \lambda_2\lambda_1^{n+1}}{\sqrt{5}} = \frac{\lambda_1^{n+1}\lambda_2\left(\left(\frac{\lambda_2}{\lambda 1}\right)^n - 1\right)}{\sqrt{5}}$$

Możemy teraz ponownie (lecz inaczej) wykazać, że ciąg Fibonacciego nie ma wyrazów zerowych poza F_0. Wystarczy zaobserwować, że $F_n = 0$ wtedy i tylko wtedy, gdy $(\frac{\lambda_2}{\lambda_1})^n = 1$. Można łatwo zauważyć, że nie jest to możliwe dla $n > 0$, ponieważ $|\lambda_1| > |\lambda_2|$. Podobnymi technikami można pokazać, że dla dowolnego ciągu, którego macierz ma dwie wartości własne o różnych modułach od pewnego momentu wyrazy nie mogę być równe zero. Wówczas do sprawdzenia, czy istnieje jakikolwiek wyraz zerowy wystarczy jedynie zbadać zerowość pewnej liczby początkowych wyrazów ciągu.

Równe wartości własne
Rozważmy kolejny przykład ciągu:

$$\begin{cases} u_n = -2u_{n-1} - u_{n-2} \\ u_1 = 0 \\ u_0 = 1 \end{cases} \tag{4}$$

Kolejne wyrazy tego ciągu to $1, 0, -1, 2, -3, 4, -5, 6, -7, 8 \ldots$, więc również spodziewamy się, że tylko $u_1 = 0$. Dla tego liniowego równania rekurencyjnego macierz ma postać:

$$M = \begin{bmatrix} -2 & 1 \\ -1 & 0 \end{bmatrix}$$

Przy policzeniu wartości własnych, okazuje się, że $\lambda_1 = -1$, $\lambda_2 = -1$, czyli mamy wielokrotna wartość własną. Macierz M ma wówczas rozkład Jordana, przedstawiony jako $M = PJP^{-1}$. Potęgowanie macierzy staje się również łatwe dla postaci Jordana. Uzyskujemy:

$$M^n = \underbrace{\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}}_{P} \underbrace{\begin{bmatrix} \lambda_1 & 1 \\ 0 & \lambda_1 \end{bmatrix}^n}_{J^n} \underbrace{\begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}}_{P^{-1}} = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \lambda_1^n & \lambda_1^{n-1} n \\ 0 & \lambda_1^n \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$$

Podobnie jak poprzednio możemy jawnie wyrazić wyraz u_n jako:

$$u_n = \lambda_1^n + \lambda_1^{n-1} n$$

Wykazanie, czy istnieje n takie, że $u_n = 0$ staje się proste. A zatem $u_n = 0$ jeśli $\lambda_1 + n = 0$, czyli gdy $n = -\lambda_1 = 1$.

Nietrudno pokazać, że z kolei tą metodą można rozwiązać dowolny przypadek, gdy mamy dwukrotną wartość własną.

Ostatni przypadek
Przed nami najciekawsza cześć, przypadek gdy $|\lambda_1| = |\lambda_2|$, ale $\lambda_1 \neq \lambda_2$. Rozważmy nasz przykład (2) ze wstępu. Dla takiego równania macierz jest zdefiniowana jako:

$$M = \begin{bmatrix} 2 & 1 \\ -3 & 0 \end{bmatrix}$$

Obliczenie wartości własnych daje: $\lambda_1 = 1 - i\sqrt{2}$, $\lambda_2 = 1 + i\sqrt{2}$. Zauważmy, że co do modułów wartości własne są równe. Okazuje się, że ten przypadek jest szczególnie interesujący i wymaga trochę więcej uwagi.

Zainteresowany czytelnik może przeczytać o liczbach zespolonych: Delta, październik 2016: Liczby zespolone i kwaterniony

Nasze równanie można zapisać w postaci

$$u_n = \frac{i}{2\sqrt{2}}(\lambda_1^n - \lambda_2^n)$$

Przeniesiemy teraz nasze rozważania na grunt uogólniony.

Powiemy, że a jest liczbą algebraiczną, jeżeli jest pierwiastkiem niezerowego wielomianu o współczynnikach wymiernych. Zbiór liczb algebraicznych oznaczmy jako $\mathbb{A}$. Liczba $\sqrt{2}$ jest liczbą algebraiczną wielomianu $p(x) = x^2 - 2$

Mianowicie można nietrudno pokazać, że nasze równanie będzie przyjmowało postać $u_n = a\lambda_1^n + \overline{a}\lambda_2^n$, dla pewnej liczby algebraicznej $a \in \mathbb{A}$ i liczb zespolonych takich, że $\lambda_1 = \overline{\lambda_2}$.

Pytając się o warunek $u_n = 0$, możemy zauważyć, że $a\lambda_1^n + \overline{a\lambda_1}^n = 0$ wtedy i tylko wtedy, gdy cześć rzeczywista $a\lambda_1^n$ jest równa 0. Weźmy: $v = \frac{\lambda_1}{|\lambda_1|}$ wówczas $|v| = 1$. Wystarczy sprawdzić, czy $\frac{u_n}{|\lambda_1|^n} = 0$, czyli, czy $av^n + \overline{av}^n = 0$. To zaś jest równoważne temu, że av^n jest czysto urojone (postaci ix dla $x \in \mathbb{R}$). Ponieważ $|v| = 1$, to musi być $x = |a|$. Pytamy więc, czy istnieje takie n, że $v^n = \frac{i|a|}{a}$.

Pozostaje nam rozwiązać równanie postaci

$$v^n = \beta, \text{ gdzie } v, \beta \in \mathbb{A}, |v| = |\beta| = 1.$$

To w ogólności wymaga pochylenia się nad teorią liczb algebraicznych. Jednak dla sprawnego algebraika, takie równania nie stanowią problemu. Dla równań rzędu 3 również znamy algorytm bazujący na podobnym rozumowaniach, jednak w ogólności dla $k > 5$ nie jest znane żadne rozwiązanie problemu Skolema.