Podróże w $\mathbb{N}^d$

Wojciech CZERWIŃSKI

Autor **został właśnie** laureatem prestiżowego grantu ERC. Poniższy tekst opisuje jeden z trzech tematów badawczych, realizowanych w ramach tego grantu.

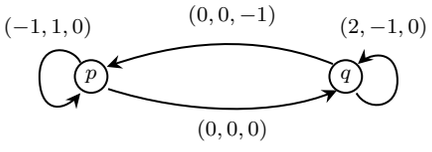
Jakiś czas temu koleżanki i koledzy z redakcji *Delty* poprosili mnie, żebym opisał, czym zajmuję się naukowo, i przedstawił pewien ciekawy wynik, który udało mi się wraz ze współpracownikami niedawno uzyskać. Pisząc ten tekst, postaram się przybliżyć tę właśnie dziedzinę, która mi osobiście wydaje się interesująca chyba dlatego, że rozważa problemy o bardzo prostym sformułowaniu geometrycznym, a mimo to jest w niej więcej znaków zapytania niż odpowiedzi. Badania często okazują się ciekawą kombinatoryką, popartą jednak zwykle geometrycznymi intuicjami. Wiele fundamentalnych pytań otwartych można sformułować bardzo szybko, jedno z nich przybliżę na końcu tego tekstu.

Niedawno w *Delcie* Δ^7_{20} pisałem o podróżach w $\mathbb{R}^d$. Można też równoważnie powiedzieć, że były to podróże w $\mathbb{Z}^d$. Jedną z konsekwencji omawianego tam lematu Steinitza był fakt mówiący, że jeśli układ n równań liniowych o d zmiennych i wartościach bezwzględnych wszystkich współczynników występujących w równaniach ograniczonych przez M ma rozwiązanie, to ma rozwiązanie niewielkie. Konkretnie rzecz biorąc, ma takie rozwiązanie $u \in \mathbb{R}^d$, że jego *norma* (tzn. maksimum z wartości bezwzględnych współrzędnych) jest ograniczona przez $(5dM+1)^d$, nie zależy w ogóle od liczby równań n. Ten fakt z kolei implikuje, że pytania o podróże w $\mathbb{Z}^d$ stają się stosunkowo łatwe. Rozważmy następujący *problem osiągalności w* $\mathbb{Z}^d$. Dany jest zbiór wektorów $U = \{u_1, \ldots, u_n\} \subseteq \mathbb{Z}^d$ oraz wektory początkowy $s \in \mathbb{Z}^d$ i końcowy $t \in \mathbb{Z}^d$ takie, że normy wszystkich s, t oraz u_i są ograniczone przez M. Pytamy, czy istnieje taka podróż składająca się z przystanków w punktach $v_0, v_1, \ldots, v_k \in \mathbb{Z}^d$, że zaczyna się ona w s (czyli $v_0 = s$), kończy w t (czyli $v_k = t$), a każdy krok jest przesunięciem o któryś wektor u_j (czyli dla każdego $i \in \{0, \ldots, k-1\}$ istnieje $u_j \in U$ taki, że $v_{i+1} - v_i = u_j$). Jak łatwo zauważyć, jest to równoważne pytaniu, czy istnieją współczynniki $a_1, \ldots, a_n \in \mathbb{N}$ (określające, ile razy użyjemy w trakcie podróży każdego z wektorów), takie że $\sum_{i=1}^n a_i u_i = t - s$. Z faktu powyżej wynika, że jeśli istnieje podróż z s do t, to istnieje taka podróż długości co najwyżej $(5dM+1)^d$. To w szczególności powoduje, że problem osiągalności w $\mathbb{Z}^d$ należy do klasy NP, możemy zgadnąć współczynniki a_i, które są reprezentowane przez liczby o wielomianowo wielu bitach, i sprawdzić, że rzeczywiście spełniają równość $\sum_{i=1}^n a_i u_i = t - s$.

Dziś rozważymy *problem osiągalności w* $\mathbb{N}^d$, bardzo podobny do problemu osiągalności w $\mathbb{Z}^d$, a jednak, jak się okaże, o zupełnie innych własnościach. Podobnie jak poprzednio w problemie osiągalności w $\mathbb{N}^d$ dany jest zbiór wektorów $U = \{u_1, \ldots, u_n\} \subseteq \mathbb{Z}^d$, wektor początkowy $s \in \mathbb{N}^d$ i końcowy $t \in \mathbb{N}^d$, każdy z nich o normie ograniczonej przez M. Również pytamy o istnienie takiej podróży $v_0, \ldots, v_k$, że $v_0 = s$, $v_k = t$ oraz każdy krok $v_{i+1} - v_i$ jest równy pewnemu wektorowi u_j. Wymagamy jednak, żeby każdy punkt podróży v_i miał wszystkie współrzędne nieujemne, czyli $v_i \in \mathbb{N}^d$. Innymi słowy, cała nasza podróż ma się zmieścić w dodatniej ćwiartce układu współrzędnych (dla $d = 2$), a ogólnie w dodatnim ortancie $\mathbb{N}^d$. Okazuje się, że problem osiągalności w $\mathbb{N}^d$ jest dużo trudniejszy od swojego odpowiednika w $\mathbb{Z}^d$ i wciąż daleki od matematycznego zrozumienia.

Bardzo często rozważa się pewne eleganckie uogólnienie problemu osiągalności w $\mathbb{N}^d$. Dodajemy do naszych rozważań *stany*, intuicyjnie rzecz biorąc, oznacza to, że w każdym punkcie naszej podróży jesteśmy w jednym ze skończenie wielu trybów, zwanych stanami. Opis problemu składa się wtedy również z podania skończonego zbioru stanów Q, a każdy krok podróży określany jest nie tylko wektorem z $\mathbb{N}^d$, a raczej trójką $(p, u, q) \in U \subseteq Q \times \mathbb{Z}^d \times Q$. Taka trójka $(p, u, q) \in U$ oznacza, że jeśli jestem w stanie p, to mogę przesunąć się o wektor u i zmienić stan na q. Wprowadzenie stanów tylko pozornie komplikuje sprawę. System z wektorami w $\mathbb{N}^d$ i $N-1$ stanami można stosunkowo łatwo zasymulować systemem o wektorach z $\mathbb{N}^{d+3}$ i bez stanów. Dodajemy do systemu trzy współrzędne i wtedy konfigurację: stan i-ty, wektor $u \in \mathbb{N}^d$, reprezentujemy jako wektor $(u, i, N(N-i), 0) \in \mathbb{N}^{d+3}$, który na pierwszych d współrzędnych ma wektor u. Przy odrobinie sprytu jesteśmy w stanie zakodować również ruchy w systemie ze stanami w tych $d+3$ współrzędnych (przy czym jednemu ruchowi w oryginalnym systemie odpowiadać będzie pewien ciąg ruchów w jego reprezentacji). Ostatnia współrzędna nie jest używana przy kodowaniu stanów, ale przydaje się przy implementacji ruchów. Dociekliwy Czytelnik może spróbować dopowiedzieć sobie szczegóły.

Żeby poczuć nieco, jak ciekawe własności mogą mieć takie systemy, rozważmy przykład pokazany na rysunku 1. System ten ma dwa stany: p i q oraz cztery możliwe ruchy oznaczone strzałkami i ich etykietami. Przyjrzyjmy się, jaką podróż możemy wykonać, startując ze stanu p i punktu $(1, 0, n)$; będziemy oznaczali taką konfigurację $p(1, 0, n)$.



Rys. 1

Na początek możemy wykonać następującą trasę:

$$p(1,0,n) \to p(0,1,n) \to q(0,1,n) \to q(2,0,n) \to p(2,0,n-1),$$

i jesteśmy z powrotem w stanie p z trzecim licznikiem o jeden mniejszym, ale za to pierwszym dwa razy większym. Możemy wykonać analogiczną trasę ponownie

$$p(2,0,n-1) \Rightarrow p(0,2,n-1) \to q(0,2,n-1) \Rightarrow$$
$$\Rightarrow q(4,0,n-1) \to p(4,0,n-2),$$

gdzie przez $\Rightarrow$ oznaczamy kilka ruchów pod rząd. Powtarzając tę procedurę, możemy dotrzeć do konfiguracji $p(2^n, 0, 0)$, a stąd bardzo prosto do dowolnej konfiguracji postaci $p(x, y, 0)$, gdzie $x + y = 2^n$. Nietrudno

zauważyć, że konfiguracji, do których można dojść z $p(1,0,n)$, jest skończenie wiele, a konkretnie rzecz biorąc, wykładniczo wiele względem n. Ciekawym pytaniem (choć nie otwartym) jest, jak duży może być zbiór konfiguracji osiągalnych z jednej ustalonej konfiguracji w przypadku, gdy jest on skończony. Zachęcam Czytelników do konstrukcji systemu, w którym taki zbiór jest podwójnie wykładniczy względem wielkości początkowej konfiguracji oraz wielkości systemu (w szczególności liczb na strzałkach). Przy pewnym wysiłku można skonstruować system, który ma ten zbiór konfiguracji wielkości rzędu wieży dwójek wysokości n, czyli $2^{\cdot^{\cdot^{\cdot^{2^n}}}}$, a nawet dużo większy (rzędu $F_d(n)$, funkcje F_d omówię poniżej).

Problem osiągalności w $\mathbb{N}^d$ jest badany w informatyce teoretycznej od lat 70. XX wieku. Znany jest w delikatnie się różniących, ale równoważnych wersjach, pod nazwą problemu osiągalności w sieciach Petriego bądź problemu osiągalności w systemach zwanych *Vector Addition Systems* (brak tu powszechnie używanej polskiej nazwy). Warto podkreślić, dlaczego ten problem jest w ogóle rozważany w informatyce teoretycznej. Mianowicie sieci Petriego są jednym z podstawowych modeli programów współbieżnych, a zostały wprowadzone w latach 30. przez Carla Petriego w kontekście modelowania reakcji chemicznych. Gdy mamy w pewnym systemie d różnych substancji chemicznych, to określając liczbę ich cząsteczek liczbami naturalnymi, możemy opisać sytuację wektorem w $\mathbb{N}^d$. W takiej sytuacji reakcja chemiczna, która rozkłada 3 cząsteczki pierwszej substancji na 2 cząsteczki drugiej substancji i 4 cząsteczki trzeciej substancji, a czwartej substancji w ogóle nie dotyczy, może być przedstawiona jako zmiana o wektor $(-3,2,4,0)$. Podobnie możemy modelować inne systemy, w których równocześnie istnieje wiele zasobów. Mogą to być towary dostępne na giełdzie lub liczby procesów odpowiedniego typu w danym programie. Problem osiągalności odpowiada więc na pytanie, czy zaczynając z danego układu, można po pewnej liczbie modyfikacji dojść do pewnego innego układu. To pytanie jest przydatne przy automatycznej weryfikacji programów komputerowych: możemy zapytać, czy zaczynając z konfiguracji początkowej, można po pewnej liczbie kroków otrzymać określoną konfigurację błędną. Ta obserwacja jest jednym w ważnych powodów zainteresowania informatyki teoretycznej sieciami Petriego i ich problemem osiągalności. Ma jednak duże znaczenie również fakt, że problem osiągalności w $\mathbb{N}^d$ jest też po prostu bardzo naturalnym zagadnieniem geometrycznym.

Co zaskakujące, przez dłuższy czas nie było wiadomo, czy w ogóle istnieje jakikolwiek algorytm rozwiązujący problem osiągalności w $\mathbb{N}^d$, innymi słowy, czy problem ten jest rozstrzygalny. Pierwszy algorytm został zaproponowany przez Ernsta Mayra w roku 1978, po około dziesięciu latach badań. Nie było jednak znane żadne ograniczenie na złożoność obliczeniową tego problemu. Inaczej mówiąc, wiadomo było, że algorytm działa bardzo wolno, ale nawet trudno powiedzieć, jak wolno. Pomimo wielu lat badań nad podobnymi problemami najlepszy aktualnie znany algorytm, opublikowany w 2019 roku przez Leroux i Schmitza, działa w czasie rzędu $F_{d+4}(n)$, gdzie n to rozmiar danych wejściowych, a d to wymiar przestrzeni $\mathbb{N}^d$. Funkcje F_k to przykład bardzo szybko rosnących funkcji, zdefiniowanych (w jednej z wersji definicji) następująco: $F_0(n) = n+1$, $F_k(n) = F_{k-1}^n(n)$, czyli $F_k(n)$ to n-krotne złożenie funkcji F_{k-1} na argumencie n. Mamy wówczas

$$F_1(n) = \underbrace{F_0(F_0(\dots(}_{n \text{ razy}} n)\dots)) = 2n,$$

$$F_2(n) = \underbrace{F_1(F_1(\dots(}_{n \text{ razy}} n)\dots)) = 2^n \cdot n \approx 2^n, \quad F_3(n) \approx 2^{\cdot^{\cdot^{\cdot^{2^n}}}},$$

gdzie w $F_3(n)$ wieża dwójek jest wysokości n, a liczba $F_4(n)$ i następne są już dość trudne do wyobrażenia. Widać więc, że faktycznie najlepszy znany dziś algorytm dla problemu osiągalności jest bardzo wolny.

To nie znaczy jednak, że każdy algorytm musi być tak wolny. Znane są pewne dolne ograniczenia na złożoność problemu, ale jest tu wiele znaków zapytania. Już w roku 1976 Richard Lipton udowodnił, że problem osiągalności w $\mathbb{N}^d$ jest ExpSpace-trudny, czyli z grubsza rzecz biorąc, że żaden algorytm nie może działać szybciej niż w pamięci wykładniczej. W szczególności nie może działać w czasie szybszym niż podwójnie wykładniczy. Jednak przez wiele lat dość powszechną hipotezą było, że taki algorytm działający w czasie podwójnie wykładniczym powinien istnieć. Wielu osobom wydawało się prawdopodobne, że jeśli istnieje podróż od konfiguracji startowej s do końcowej t, to istnieje również taka podróż o długości co najwyżej podwójnie wykładniczej. Osobiście, z tego, co pamiętam, też wierzyłem w tę hipotezę. Konkretnie rzecz biorąc, wspomniana konstrukcja Liptona pokazuje, że podróże w $\mathbb{N}^d$ nie mogą być krótsze niż rzędu M^{2^d}, co dla stałego d oraz M reprezentowanego binarnie jest ograniczeniem wykładniczym. Dopiero w 2018 roku udało się nam z kolegami udowodnić, że problem osiągalności w $\mathbb{N}^d$ nie może dać się rozwiązać szybciej niż w czasie $F_3(n) \approx 2^{\cdot^{\cdot^{\cdot^{2^n}}}}$, co w szczególności implikuje, że istnieją systemy, w których najkrótsza ścieżka jest bardzo długa, np. długości ośmiokrotnie wykładniczej. Temu dowodowi można przyjrzeć się w artykule na serwisie arXiv:`arxiv.org/abs/1809.07115`. Przedstawię tu jednak pewien przykład, który pokazuje, że oszacowanie Liptona nie jest optymalne. Ten przykład był jednym z początkowych na naszej drodze do ostatecznego rozwiązania i naprowadził nas na właściwą konstrukcję. Sam w sobie zaś stanowi ciekawe zrozumienie tego, co może stać się w wymiarze $d = 4$.

Tak jak wspomniałem powyżej, konstrukcja Liptona pokazywała, że w stałym wymiarze d najkrótsze podróże mogą być długości rzędu M^{2^d}, czyli wykładnicze, ale nieznane były przykłady, w których są one istotnie dłuższe. Przykład, który udało nam się znaleźć, pokazuje, że już w stosunkowo niewielkim wymiarze

najkrótsze podróże mogą być długości podwójnie wykładniczej. Konstrukcja opiera się na następującym lemacie, dotyczącym ułamków, co dość zaskakująco okazuje się związane z podróżami w $\mathbb{N}^d$.

Lemat. *Dla każdego $k \in \mathbb{N}$ istnieje k ułamków $\frac{a_1}{b_1}, \ldots, \frac{a_k}{b_k}$, takich że*

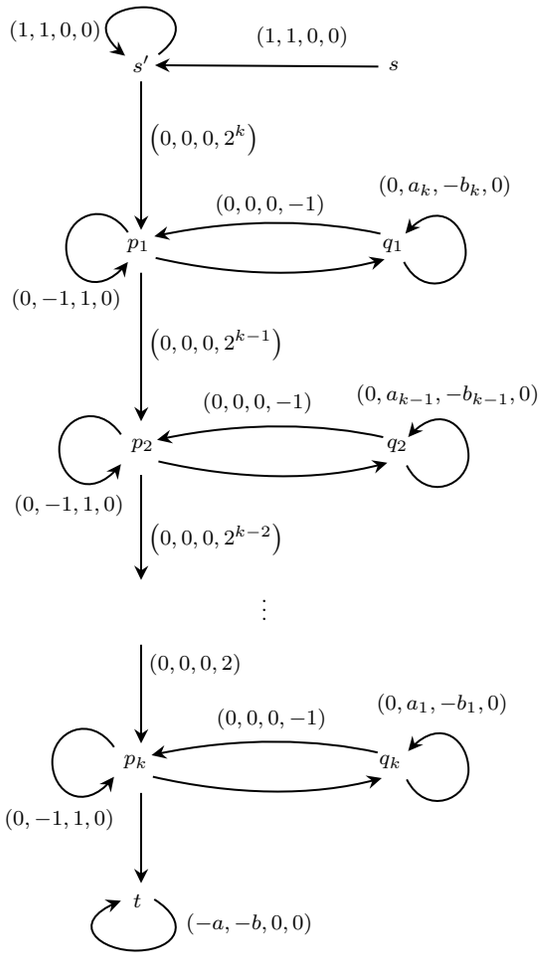
$$1 < \frac{a_1}{b_1} < \ldots < \frac{a_k}{b_k} = 1 + \frac{1}{4^k},$$

$$\left(\frac{a_1}{b_1}\right)^{2^1} \cdot \left(\frac{a_2}{b_2}\right)^{2^2} \cdot \ldots \cdot \left(\frac{a_k}{b_k}\right)^{2^k} = \frac{a}{b},$$

oraz wszystkie liczby całkowite a, b, a_i oraz b_i są ograniczone przez 16^{k^2+k}.

Zauważmy, że istnienie ułamków postulowanych w lemacie wcale nie jest oczywiste. Żeby $\frac{a_i}{b_i}$ był nie większy niż $1 + \frac{1}{4^k}$, to jego mianownik musi być równy co najmniej 4^k. Taki ułamek podniesiony do potęgi 2^i, dla i rzędu k, ma licznik oraz mianownik podwójnie wykładniczy względem k. Trudność w dowodzie powyższego lematu polega na tym, że liczniki i mianowniki wielu ułamków podwójnie wykładniczej wielkości muszą się poskracać przy mnożeniu w taki sposób, by w rezultacie otrzymany został ułamek $\frac{a}{b}$ dla a i b wielkości wykładniczej względem k. Dowodu lematu nie przedstawimy, choć dałoby się go udowodnić mniej więcej na jednej stronie.

Teraz pokażemy bardzo szkicowo, w jaki sposób lemat może posłużyć do konstrukcji zbioru ruchów dla $d = 4$, $U = \{u_1, \ldots, u_n\} \subseteq Q \times \mathbb{N}^4 \times Q$ oraz konfiguracji



Rys. 2

takich $s(0,0,0,0), t(0,0,0,0) \in Q \times \mathbb{N}^4$, że podróż z $s(0,0,0,0)$ do $t(0,0,0,0)$ przy użyciu U jest podwójnie wykładnicza względem wielkości tych wektorów. System jest zilustrowany na rysunku 2 (niepodpisane ruchy oznaczają brak przesunięcia). Tak dobraliśmy zbiór U, żeby każda podróż musiała wyglądać w bardzo konkretny sposób. Na początku generujemy wektor postaci $(N, N, 0, 0)$ przy użyciu pętli w stanie o efekcie $(1, 1, 0, 0)$ w stanie s'. Potem mnożymy drugą współrzędną przez $\left(a_k/b_k\right)^{2^k}$ w stanach p_1 i q_1. Robimy to podobnie, jak w systemie na rysunku 1, używając dwóch stanów. Tam mnożyliśmy liczbę 1 przez ułamek $\frac{2}{1}$ co najwyżej n razy, ale każde mnożenie mogło mieć pewne straty. W efekcie po n pętlach między stanami p i q z liczby 1 uzyskaliśmy najwyżej liczbę 2^n. W analogiczny sposób możemy pomnożyć liczbę N przez co najwyżej $\left(a_k/b_k\right)^{2^k}$. Następnie mamy $k-1$ podobnych faz, w których mnożymy drugą współrzędną przez co najwyżej $\left(a_{k-1}/b_{k-1}\right)^{2^{k-1}}, \ldots, \left(a_2/b_2\right)^{2^2}$ i na końcu przez co najwyżej $\left(a_1/b_1\right)^{2^1}$. Po tych wszystkich operacjach nasza druga współrzędna ma wartość co najwyżej $N \cdot \frac{a}{b}$, co wynika z równania w lemacie. A więc cała konfiguracja ma postać $t(N, N', 0, 0)$, gdzie $N' \leqslant N \cdot \frac{a}{b}$. Na koniec w stanie t w pętli odejmujemy wektor $(b, a, 0, 0)$ i chcemy dojść do konfiguracji $t(0,0,0,0)$. Okazuje się, że jedyny sposób dojścia do $t(0,0,0,0)$ jest taki, żeby N' było równe dokładnie $N \cdot (a/b)$, a to z kolei jest możliwe tylko, jeśli wszystkie mnożenia na trasie były dokładne. Pierwsze mnożenie, to w stanach p_1 i q_1, było mnożeniem przez $\left(\frac{4^k+1}{4^k}\right)^{2^k}$. Aby było zrealizowane dokładnie, to liczba N musiała być podzielna przez $(4^k)^{2^k}$, co jest liczbą podwójnie wykładniczą, a więc oznacza, że N musiało być podwójnie wykładnicze. Zatem oczywiście długość trasy też musiała być podwójnie wykładnicza, co kończy szkic konstrukcji. Szczegóły można znaleźć w artykule w serwisie arXiv:`arxiv.org/abs/2001.04327`.

Przedstawiona konstrukcja dowodzi, że istnieją systemy w wymiarze $d = 4$, które mają najkrótszą ścieżkę pomiędzy dwoma niewielkimi konfiguracjami długości podwójnie wykładniczej względem opisu systemu. Czy możemy skonstruować takie systemy z najkrótszą ścieżką potrójnie wykładniczą? Tego nie wiadomo. Najlepsze górne oszacowanie to $F_7(n)$, czyli olbrzymie. Co ciekawe, podobnie jest również dla innych wymiarów. Dla $d = 2$ wiadomo, że w każdym systemie o ile dany punkt jest osiągalny w $\mathbb{N}^2$, to jest osiągalny trasą co najwyżej wykładniczej długości. Wiadomo też, że są systemy, w których taka trasa wykładniczej długości jest faktycznie najkrótszą trasą. Jak jednak wygląda sytuacja dla wymiaru $d = 3$? Tego również nie wiadomo. Najlepsze znane górne oszacowanie to funkcja $F_6(n)$, czyli dużo większa niż wieża dwójek wysokości n. Możliwe jest też, że zawsze taka najkrótsza trasa jest wykładniczej długości. Osobiście obstawiam, że druga możliwość jest prawdziwa, ale to tylko dywagacje. Być może odpowiedzi udzieli ktoś z Czytelników, tworząc konstrukcję podobną do powyższej. Rozwiązania problemów otwartych od dziesięcioleci wcale nie muszą być bardzo trudne.