NR 5 (612) 2025
CENA 9 ZŁ VAT 8%
PL ISSN 0137-3005 | NR IND 35 550 X
MIESIĘCZNIK
www.deltami.edu.pl

$h=6{,}63\cdot10^{-34}\ \mathrm{J\cdot s}$ $\pi=3{,}141592\ldots$

delta

MATEMATYKA – FIZYKA – ASTRONOMIA – INFORMATYKA

Artystyczne piękno osobliwych zbiorów

str. 17

25 lat

Wydziału Matematyki i Nauk Informacyjnych Politechniki Warszawskiej

Wydział Matematyki i Nauk Informacyjnych
POLITECHNIKA WARSZAWSKA

UNIWERSYTET WARSZAWSKI

ISSN 0137-3005

Nakład: 2700 egz.

delta

W następnym numerze:

Co nazwy pierwiastków mówią o stosunku uczonych do nauki?

SPIS TREŚCI
NUMERU 5 (612) 2025

Miesięcznik *Delta – matematyka, fizyka, astronomia, informatyka* założony został w 1974 roku przez Marka Kordosa. Wydawany jest przez Uniwersytet Warszawski przy współpracy towarzystw naukowych: Polskiego Towarzystwa Matematycznego, Polskiego Towarzystwa Fizycznego, Polskiego Towarzystwa Astronomicznego i Polskiego Towarzystwa Informatycznego.

Adres do korespondencji:
Redakcja *Delty*, ul. Banacha 2, pokój 4020, 02-097 Warszawa
e-mail: delta@mimuw.edu.pl tel. 22-55-44-402.
Okładki i ilustracje:
Anna Ludwicka Graphic Design & Serigrafia.
Skład systemem LaTeX wykonała Redakcja.
Druk: Arkuszowa Drukarnia Offsetowa Sp. z o.o.
www.ado.com.pl

Prenumerata:
Garmond Press: www.garmondpress.pl (tylko instytucje)
Kolporter: www.kolporter.com.pl (tylko instytucje)
Na stronie Empiku *Deltę* można zamówić co miesiąc:
www.empik.com/delta,p1235643855,prasa-p

Numery archiwalne można nabyć w Redakcji osobiście lub zamówić przez e-mail.

Cena 1 egzemplarza: z ostatnich 12 miesięcy 9 zł; wcześniejsze egzemplarze 4 zł

Strona internetowa (w tym artykuły archiwalne, linki itd.): deltami.edu.pl

Można nas też znaleźć na facebook.com/Delta.czasopismo

Wydawca: Uniwersytet Warszawski

Archipelag możliwości

O powstaniu Wydziału Matematyki i Nauk Informacyjnych (MiNI) Politechniki Warszawskiej

*Tadeusz RZEŻUCHOWSKI**

Pierwszy dziekan Wydziału MiNI PW, w latach 1999–2003

Wydział Matematyki i Nauk Informacyjnych Politechniki Warszawskiej powstał w roku 1999, na bazie istniejącego wcześniej Instytutu Matematyki. Związane były z tym nadzieje na rozwój oraz nowe możliwości. Z perspektywy 25 lat można stwierdzić, że nie tylko zostały one spełnione, ale też przekroczone. Duża intensyfikacja i wzrost poziomu badań naukowych, nowe, atrakcyjne kierunki i specjalności studiów, wysoka ocena absolwentów przez pracodawców – to w największym skrócie bilans tych 25 lat.

Wydział od początku starał się wyjść z działaniem poza swoje mury, zwłaszcza do uczniów szkół średnich i starszych klas podstawowych, traktując to jako ważną część misji.

Od roku 2000 Wydział prowadzi Internetowy Konkurs Matematyczny, skierowany szczególnie do uczniów z małych miejscowości. Główna idea to motywowanie młodzieży do robienia jak największej liczby zadań. Wiadomo, że z matematyką jest trochę jak z tańcem – nie wystarczy znać kroki i figury – trzeba dużo ćwiczyć. Dobrze skonfigurowany zbiór zadań większości uczniów powinien wystarczyć. Konkurs nie był pomyślany jako konkurencja dla Olimpiady, gdzie zadania są dużo bardziej wyrafinowane. Tu wystarczy solidne przygotowanie z materiału szkoły średniej.

Również w roku 2000 Wydział zaczął realizować działania pod nazwą „Zielona Informatyka”, później „Zielona Akcja”. W czasie wakacji studenci wolontariusze jechali prowadzić zajęcia i realizować projekty edukacyjne z dziećmi w wiejskich szkołach. Chodziło nie tylko o nauczenie dzieci czegoś konkretnego, ale również o zmniejszenie dystansu, o przekonanie ich, że dalsza edukacja i związany z tym awans są w ich zasięgu. Po kilku latach akcję przejęła Polsko-Amerykańska Fundacja Wolności i pod nazwą „Projektor” prowadzi ją na ogromną skalę do tej pory.

Inny charakter miał realizowany w latach 2010–2012 projekt o nazwie „Archipelag Matematyki”. Tworzony był wirtualny świat, po którym wędrując i rozwiązując pojawiające się zagadki o charakterze matematycznym, uczestnik uzyskiwał dostęp do stworzonych w ramach projektu materiałów zawierających różne ciekawostki matematyczne, problemy i zastosowania. W Archipelagu powstało ponad 300 filmów, animacji czy gier matematycznych i innych materiałów edukacyjnych.

Takich działań na Wydziale jest dużo więcej: MiNI Akademia Matematyki, Dzień Popularyzacji Matematyki... to tylko niektóre przykłady.

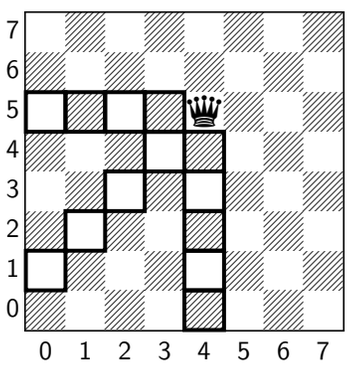
Metafora Archipelagu dobrze pasuje do samej Matematyki – to aktywny sejsmicznie obszar, gdzie powstają wciąż nowe wyspy, między którymi zachodzi intensywny przepływ informacji i współpraca, i które pełne są zasobów wykorzystywanych nawet w odległych akwenach.

Życzę Czytelnikom *Delty* fascynujących podróży po tym Archipelagu.

Wythoff Nim, czyli krótkie warsztaty z kombinatorycznej teorii gier

*Rafał GÓRAK**

* Wydział Matematyki i Nauk Informacyjnych, Politechnika Warszawska



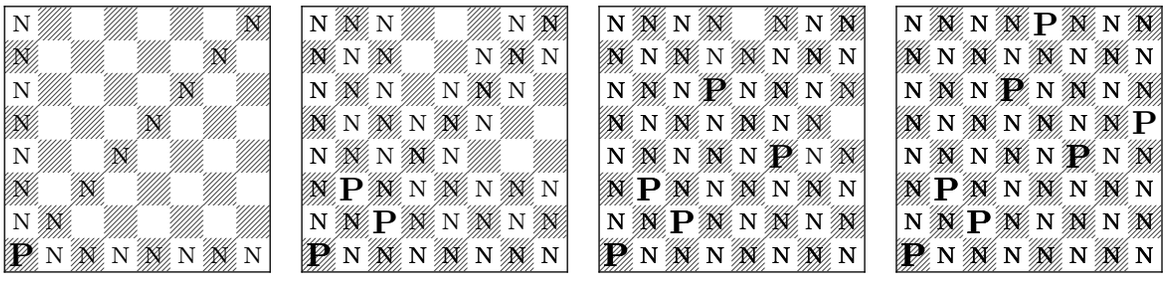
Rys. 1. Dostępne ruchy

W pewnym miejscu na skończonej szachownicy ustawiono hetmana. Dwóch graczy wykonuje nim ruchy naprzemiennie, a grę przegrywa ten z graczy, który ruchu nie może wykonać (a jest jego kolej). Jednak aby mieć pewność, że gra kiedyś się skończy, dopuszczamy jedynie ruchy w lewo, w dół oraz po jednej z przekątnych (tyle samo pól w lewo co w dół). Gra ta nosi nazwę Wythoff Nim, od nazwiska holenderskiego matematyka Willema Abrahama Wythoffa, który na początku dwudziestego wieku ją zaproponował i badał. Gra ta jest przykładem szerszej klasy gier kombinatorycznych, tzw. gier bezstronnych (*impartial*). Są to gry, w których gracze wykonują ruchy naprzemiennie, dostępne ruchy zależą jedynie od kolejności graczy, a przegrywa ten, który ruchu nie może wykonać – tak jak w Wythoff Nim. Co więcej, zakładamy, że niezależnie od przebiegu gry kończą się w pozycji terminalnej (nie ma remisów), a liczba wszystkich możliwych pozycji jest skończona (w skrócie: gra jest skończona). Zatem jeżeli będziemy w dalszej części używali terminu gra, to właśnie takie gry będziemy mieli na myśli. Naszym celem jest oczywiście ustalenie strategii wygrywającej.

Aby tego dokonać, podzielimy pozycje (czyli pola szachownicy) na dwa rodzaje. Pozycje **P**, czyli pożądane, oraz pozycje **N**, czyli niepożądane. Celem każdego gracza będzie wykonanie ruchu na pozycje pożądane, czyli zwycięskie, a unikanie pól niepożądanych. Precyzyjna definicja wygląda następująco:

Definicja. Pozycja terminalna w grze to pozycja **P** (w przypadku Wythoff Nim lewy dolny róg). Z pozycji **P** możliwe są jedynie ruchy do pozycji **N**, a z pozycji **N** istnieje ruch do pozycji **P**.

Chwila refleksji pozwala nam stwierdzić, że taki podział umożliwia jednemu z graczy rozegrać zwycięską partię. Dokładniej, gracz, który wykonuje ruch z pozycji **N**, ma zwycięską strategię, wykonując ruch do **P**. Z kolei ruszając się z **P**, nigdy do pozycji **P** nie trafimy, czyli w szczególności do lewego dolnego rogu – jedynej pozycji terminalnej. Zatem gracz wykonujący ruch z pozycji **P** nie ma strategii wygrywającej. Co więcej, przytoczona tutaj definicja w istocie pokazuje, jak rekurencyjnie (i jednoznacznie) podzielić pozycje na **N** i **P**. Zróbmy to w sytuacji gry Wythoff Nim na standardowej szachownicy 8 na 8. Podziału można dokonać w kilku prostych krokach, zaczynając od pozycji terminalnej, jak ukazane jest to na rysunku 2.



Rys. 2. Rekurencyjny podział na pozycje **P** i **N**

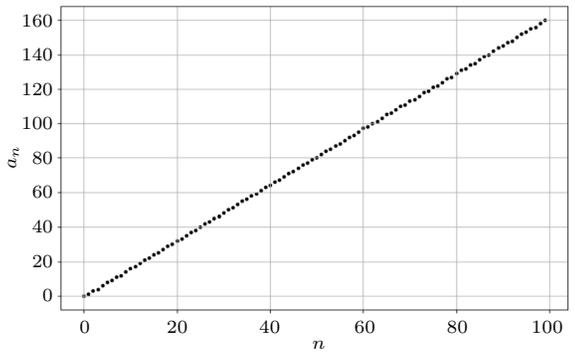
Jak widać na rysunku 2, pozycje pożądane **P** są znacznie rzadsze niż pozycje **N**. Ostatnia szachownica na powyższym rysunku daje nam pełen opis strategii w grze na szachownicy 8 na 8.

(a) Jeżeli na początku gry hetman jest ustawiony na pozycji **P**, to pierwszy z graczy przegrywa.
(b) Jeżeli zaś na początku gry hetman jest ustawiony na pozycji **N**, to pierwszy z graczy przesuwa go na pozycję **P**, i tak za każdym razem, kiedy jest jego kolej. Postępując w ten sposób, gwarantuje sobie wygraną.

Jeżeli kolumny i wiersze będziemy numerować, poczynając od 0, to przy pewnym niewielkim wysiłku (co pozostawiamy Czytelnikowi) można wykazać, że pozycje **P** są postaci $(a_n, a_n + n)$ bądź symetrycznie $(a_n + n, a_n)$, gdzie a_n to ciąg spełniający następujący wzór rekurencyjny:

$$a_0 = 0 \text{ oraz } a_n = \operatorname{mex}\{a_i, a_i + i \mid 0 \leqslant i < n\},$$

w którym $\operatorname{mex}(A) = \min(\mathbb{N} \cup \{0\} \setminus A)$. Przyjrzyjmy się wykresowi a_n dla pierwszych 100 wartości.



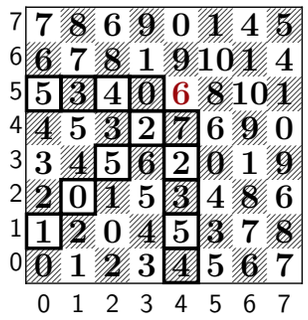
Rys. 3. Wykres a_n dla $n \leqslant 100$

Widać, że wartości a_n rosną w sposób prawie liniowy. Dokładniejszy rachunek pokazuje, że $\lim_{n\to\infty} \frac{a_n}{n} \approx 1{,}61803$. Nietrudno rozpoznać, że jest to $\varphi = \frac{1+\sqrt{5}}{2}$, czyli tzw. złoty podział. Można wykazać, że $a_n = \lfloor n\varphi \rfloor$, uzyskując rozwiązanie nierekurencyjne Wythoff Nim:

Twierdzenie 1. *W grze Wythoff Nim gracz drugi ma strategię wygrywającą, jeśli pozycja początkowa jest planszą z hetmanem na pozycji* $(\lfloor n\varphi \rfloor, \lfloor n\varphi \rfloor + n)$ *lub* $(\lfloor n\varphi \rfloor + n, \lfloor n\varphi \rfloor)$*, dla* $n \in \mathbb{N} \cup \{0\}$*. W przeciwnym wypadku gracz pierwszy ma strategię wygrywającą (zwycięski ruch prowadzi na pozycję przedstawionej wcześniej postaci).*

Zdefiniujmy następujące zbiory: $A = \{\lfloor n\varphi \rfloor : n \in \mathbb{N} \cup \{0\}\}$ oraz $B = \{\lfloor n\varphi \rfloor + n : n \in \mathbb{N} \cup \{0\}\}$. Pokaż, że $A \cap B = \{0\}$ oraz $A \cup B = \mathbb{N} \cup \{0\}$. Korzystając z tego faktu, udowodnij twierdzenie 1.

Zastanówmy się teraz, co wydarzy się, gdy na planszy rozstawionych zostanie kilka hetmanów, a gracze w swojej turze mogą poruszyć tylko jednego z nich.



Rys. 4. $g(5,6) = \text{mex}\{0,1,2,3,4,5,7\} = 6$

Dla dwóch liczb a, b całkowitych nieujemnych definiujemy sumę Nim $a \oplus b$ jako `xor` ich rozwinięć binarnych, wyrażony na powrót w systemie dziesiętnym. Przykładowo, chcąc policzyć $29 \oplus 11$, najpierw reprezentujemy liczby w systemie dwójkowym, czyli $29 = 11101_2$ oraz $11 = 1011_2$, następnie

$$\begin{array}{r} 11101_2 \\ \texttt{xor}\ \ 1011_2 \\ \hline 10110_2. \end{array}$$

Ponieważ $10110_2 = 22$, więc możemy zapisać, że $29 \oplus 11 = 22$.

Sformułowanie twierdzenia Sprague'a–Grundy'ego w pełnej ogólności wymaga wprowadzenia pojęcia sumy gier. Suma gier kombinatorycznych $G + H$ to nowa gra, gdzie gracze w każdej turze wykonują ruch tylko w jednej z nich. Grę przegrywa ten gracz, który nie może wykonać ruchu. W istocie opisana wersja gry Wythoff Nim z wieloma hetmanami jest sumą gier Wythoff Nim z jednym hetmanem. Gdy mamy do czynienia z grami bezstronnymi, skończonymi i bez remisów, gdzie ostatni wykonujący ruch wygrywa, przyjmujemy wartość S-G dla każdej pozycji x w G, y w H oraz dla (x, y), która jest pozycją w $G + H$, jako odpowiednio $g(x), g(y)$ i $g(x, y)$. Wtedy $g(x, y) = g(x) \oplus g(y)$. Oczywiście twierdzenie zachodzi również dla sumy większej liczby gier.

Dopuszczamy możliwość, że na jednym polu stoi wiele hetmanów. Gra kończy się, gdy nie można poruszyć żadnego z nich. Do tej pory pozycję w grze mogliśmy utożsamiać z polem, na którym stoi hetman. Natomiast jeśli na planszy jest ich więcej, to mówiąc „pozycja", mamy na myśli całą planszę z zadanym układem. Dla rozróżnienia polem **P** będziemy nazywać takie pole szachownicy, że po ustawieniu tam jednego hetmana odpowiadająca pozycja (w grze z jednym hetmanem) jest pozycją **P**. Analogicznie definiujemy pole **N**. Podziału na pola **P** i **N** dokonaliśmy w pierwszej części artykułu. W pewnych sytuacjach strategia wygrywająca jest łatwa do przewidzenia:

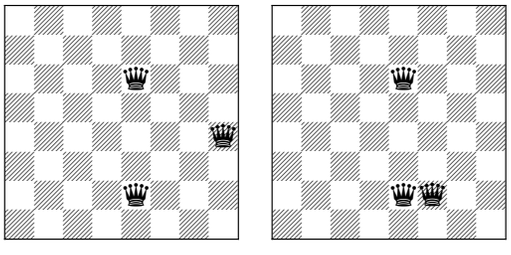
(a) Gdy wszystkie hetmany, poza jednym, ustawione są na polu **P**, to zwycięża gracz wykonujący ruch, mianowicie: przesuwając hetmana z pola **N** na pole **P**.
(b) W grze z dwoma hetmanami, jeżeli ustawione są na tym samym polu (lub polach symetrycznych), to drugi z graczy ma strategię zwycięską: wystarczy, że będzie kopiował ruchy przeciwnika.

W pełnej ogólności sam podział na pola **P** i **N** nie wystarczy. Wtedy w sukurs przychodzi pojęcie wartości Sprague'a–Grundy'ego (w skrócie S-G). Dokładniej, wartość S-G $g(x)$ dla pozycji x w grze z jednym hetmanem definiujemy rekurencyjnie: $g(t) = 0$ dla dowolnej pozycji terminalnej, $g(x) = \text{mex}\{g(y) |$ z x istnieje ruch do pozycji $y\}$. Postępując podobnie jak z wyznaczaniem pozycji **P** i **N**, otrzymujemy wartości S-G dla pozycji w grze z jednym hetmanem, co ilustruje rysunek 4.

Obserwacja. *Wartość S-G pozycji wynosi 0 wtedy i tylko wtedy, gdy jest to pozycja* ***P****.*

Obserwację tę nietrudno udowodnić, i to nie tylko dla Wythoff Nim, ale dla wszystkich gier kombinatorycznych bezstronnych, skończonych i bez remisów. Zatem wartości S-G niosą więcej informacji niż tylko podział na pozycje **P** i **N**. Zachodzi bowiem znane klasyczne twierdzenie Sprague'a–Grundy'ego, które w wersji dla gry Wythoff Nim formułuje się następująco:

Twierdzenie 2. *Jeżeli n hetmanów zostało ustawionych na polach $(a_1, b_1), (a_2, b_2), \ldots (a_n, b_n)$, to wartość S-G tej pozycji jest równa $g(a_1, b_1) \oplus g(a_2, b_2) \oplus \ldots \oplus g(a_n, b_n)$, gdzie $g(a_i, b_i)$ to wartość S-G pozycji z pojedynczym hetmanem na planszy, na polu o współrzędnych (a_i, b_i). W szczególności grę wygrywa gracz drugi wtedy i tylko wtedy, gdy wartość S-G (czyli wspomniana suma) wynosi* 0.



Rys. 5. Zwycięski ruch z pozycji **N** na pozycję **P**

Przykładowo na rysunku 5 mamy hetmany ustawione na pozycjach o wartościach S-G $6, 9$ i 5 (lewa szachownica, korzystamy z rys. 4). Ponieważ $6 \oplus 9 \oplus 5 = 10$, jest to pozycja **N**. Rzeczywiście, jeśli przesunąć hetmana z pozycji o współrzędnych $(7, 3)$ na pozycję $(5, 1)$, hetmany stałyby na polach o wartościach S-G $6, 3, 5$. Skoro $6 \oplus 3 \oplus 5 = 0$, z twierdzenia 2 otrzymujemy, że prawa szachownica to pozycja **P**.

Okazuje się, że wyznaczenie wzoru nierekurencyjnego wartości Sprague'a–Grundy'ego dla gry Wythoff Nim jest problemem otwartym. Podkreślmy, że opisaną tutaj technikę można zastosować jedynie w grach kombinatorycznych, bezstronnych i skończonych. Gdybyśmy jednak dopuścili dwa rodzaje hetmanów, czarnych i białych, a każdemu z graczy pozwolili poruszać jedynie hetmanami w swoim kolorze, to taka gra nie byłaby bezstronna i do jej analizy potrzebne byłyby inne narzędzia. Podobnie zmiana warunku zwycięstwa na odwrotny, czyli na zwycięstwo gracza pozbawionego ruchu, zazwyczaj dużo bardziej komplikuje analizę gier bezstronnych. Zachęcamy Czytelnika do dalszych dociekań.

Zadanie. Na trzech stołach rozrzucona została pewna ilość monet. Dwóch graczy może naprzemiennie zabierać 1, 2 lub 3 monety, ale tylko z jednego, wybranego przez siebie stołu. Oczywiście wyboru stołu gracze mogą dokonywać za każdym razem, gdy wykonują swój ruch. Opisz pozycje pożądane **P** oraz niepożądane **N**. Wskaż zwycięski ruch z pozycji, gdzie na stołach mamy odpowiednio 61, 101 i 15 monet.

Zadanie. Rozważ grę Wythoff Nim z jednym hetmanem z odwrotnym warunkiem zwycięstwa. Rozwiąż ją dla szachownicy 8 na 8.

Dane kierunkowe

*Przemysław GRZEGORZEWSKI**

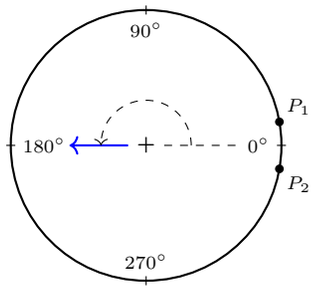
* Wydział Matematyki i Nauk Informacyjnych, Politechnika Warszawska

W wielu dziedzinach nauki można wskazać sytuacje, w których pomiary mają postać kierunków lub kątów – zarówno w dwóch, jak i w trzech wymiarach. Przykładowo, biolog może być zainteresowany badaniem kierunków sezonowego przemieszczania się ptaków wędrujących lub niektórych gatunków ryb (np. łososia) bądź kierunkami migracji zwierząt wywołanych określonymi bodźcami środowiskowymi. Geolodzy mierzą kierunki uskoków, spękań oraz szczelin w skałach w celu określenia przebiegu deformacji tektonicznych, rozkładu naprężeń czy orientacji warstw skalnych. Ortopedę oceniającego stan pacjenta powracającego do zdrowia po kontuzji interesuje kąt zgięcia kolana. Natomiast ekolodzy mierzą dominujący kierunek wiatru na danym obszarze, by wyciągnąć wnioski dotyczące rozprzestrzeniania się zanieczyszczeń.

Wnioskowanie na podstawie danych tego typu, określanych mianem **danych kierunkowych**, wymaga stosowania metod i modeli różniących się od standardowych sposobów analizy danych jednowymiarowych lub wielowymiarowych, jakie znamy z klasycznych podręczników statystyki. W niniejszym artykule zaprezentujemy kilka przykładowych problemów, które pozwolą dostrzec specyfikę danych kierunkowych.

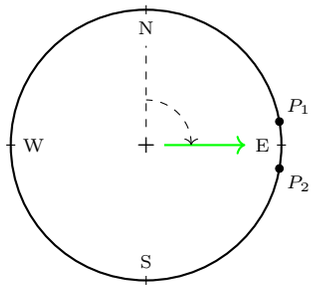
Dane kierunkowe na płaszczyźnie przyjęło się przedstawiać jako punkty leżące na okręgu jednostkowym lub, równoważnie, za pomocą kąta, w związku z czym tego typu dane określa się czasem mianem danych kołowych lub cyrkularnych (ang. *circular data*).

Pierwszym krokiem analizy danych jest zwykle próba ich zwięzłego opisu, a w szczególności wyznaczenie podstawowych charakterystyk liczbowych dostępnego zbioru obserwacji, takich jak wartość „typowa” (przeciętna, średnia) czy też miara rozrzutu. Nie inaczej jest w przypadku danych kierunkowych. Zacznijmy od wyznaczenia średniego (centralnego, preferowanego) kierunku dla danego zbioru obserwacji.



Rys. 1

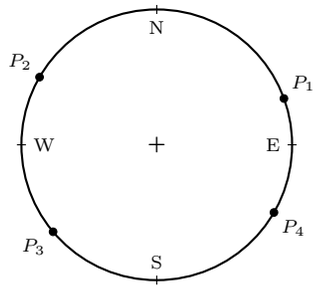
Przykład 1. Wyobraźmy sobie dwa klucze ptaków lecące w kierunkach P_1 i P_2, wskazanych na rysunku 1. Załóżmy, przyjmując standardowy sposób określania kątów w matematyce (tzn. z kierunkiem wschodnim jako kierunkiem zerowym i zwiększaniem kąta przeciwnie do ruchu wskazówek zegara), że owe dwa klucze ptaków leciały pod kątem 10° i 350°. Gdyby uśrednić zaobserwowane kierunki lotu ptaków za pomocą średniej arytmetycznej, otrzymalibyśmy w wyniku $\frac{1}{2}(10° + 350°) = 180°$, czyli kierunek zachodni (zaznaczony na rys. 1), podczas gdy nasze obserwacje ewidentnie wskazują na wschód. Nietrudno zauważyć, że gdyby kąty określał przyrodnik, przyzwyczajony do przypisywania im wartości zgodnie z ruchem wskazówek zegara, począwszy od północy, to według niego mielibyśmy do czynienia z kluczami lecącymi pod kątem 80° i 100°, i średnia arytmetyczna wskazałaby 90°, czyli spodziewany kierunek wschodni (rys. 2). Z niniejszego przykładu nie należy jednak pochopnie wysnuwać wniosku, że przyrodnicy lepiej określają średni kierunek lotu ptaków niż matematycy. Gdyby bowiem punkty P_1 i P_2 zostały obrócone o 90° przeciwnie do ruchu wskazówek zegara, to średnia arytmetyczna wyznaczona przez matematyka wyniosłaby 90°, wskazując kierunek zgodny z intuicją, w przeciwieństwie do przyrodnika, który otrzymałby wskazanie na południe.



Rys. 2

W rozważanej sytuacji łatwo jest ocenić, który wynik wydaje się poprawny, a który jest ewidentnie sprzeczny z oczekiwaniem. Ogólnie rzecz biorąc, sytuacja nie musi być aż tak oczywista, co pokażemy w kolejnym przykładzie.

Przykład 2. Na rysunku 3 zaznaczono kierunki poruszania się czterech żółwi po wykluciu się z jajek. Załóżmy, że i tym razem chcielibyśmy wyznaczyć średni kierunek poruszania się żółwi. Jeśli przyjąć „matematyczny” sposób określania kątów, to owe cztery żółwiki wędrowałyby w kierunkach: 20°, 150°, 220° i 330°, które po podstawieniu do wzoru na średnią arytmetyczną wskazałyby 180°, tj. kierunek zachodni. Gdyby ostatnie dwa kierunki określić kątami ujemnymi, tzn. −140° i −30°, to średnia przyjęłaby wartość 0°, odpowiadającą kierunkowi



Rys. 3

O zaletach i wadach różnych rodzajów średnich pisaliśmy w Δ^{12}_{2014}.

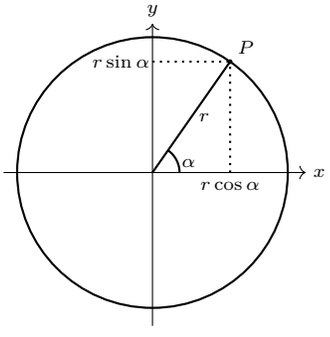
wschodniemu. Jednocześnie, gdyby kąty określał przyrodnik – zgodnie z ruchem wskazówek zegara, począwszy od północy, to według niego mielibyśmy do czynienia z następującymi obserwacjami: 70°, 120°, 230° i 300°, które po podstawieniu do wzoru na średnią arytmetyczną dałyby 180°, czyli wynik wskazujący tym razem kierunek południowy. A gdyby nasz przyrodnik wyraził dwie ostatnie obserwacje za pomocą ujemnych wartości kąta, tzn. $-130°$ i $-60°$, to średnia arytmetyczna byłaby równa 0°, wskazując północ.

Mamy nadzieję, iż przytoczone dwa przykłady przekonały Czytelników, że średnia arytmetyczna, mimo swoich wielu dobrych własności, nie nadaje się do uśredniania danych kierunkowych: nie tylko dlatego, że daje nieraz wyniki sprzeczne z intuicją, ale również z tego powodu, że jej wskazania są uwarunkowane przyjętym arbitralnie punktem odniesienia (kierunek zerowy) oraz sposobem nadawania wartości kątom. Zastanówmy się zatem, jak wyznaczać „typowy” (średni, przeciętny) kierunek?

Jak widać, dane kierunkowe (na płaszczyźnie) mogą być reprezentowane jako punkty na okręgu lub jako kąty. Pozycja każdej obserwacji może być więc jednoznacznie określona przez dwie współrzędne. I można to zrobić np. na następujące dwa sposoby. Przyjmując układ współrzędnych prostokątnych wyznaczonych przez dwie prostopadłe osie X i Y, z początkiem w punkcie O (tj. w środku okręgu), usytuowanie danego punktu P zapiszemy jako $P = P(x, y)$, gdzie x i y będą rzutami prostokątnymi tego punktu, odpowiednio, na osie X i Y. Zarazem miejsce położenia punktu P można określić w tzw. współrzędnych biegunowych, podając jego odległość r od środka okręgu (tzw. promień wodzący) oraz kąt α między odcinkiem OP a wybraną osią (z reguły osią X). Obie reprezentacje są wzajemnie równoważne, tzn. współrzędne biegunowe można przekształcić na prostokątne i na odwrót (por. rys. 4). W szczególności, znając współrzędne biegunowe punktu $P = P(r, \alpha)$, gdzie $r > 0$, $\alpha \in [0, 2\pi)$, współrzędne prostokątne tego punktu wyznaczamy ze wzorów

$$\begin{cases} x = r\cos\alpha, \\ y = r\sin\alpha. \end{cases}$$

W szczególnym przypadku, gdy rozważany punkt pokrywa się z początkiem układu, tj. $r = 0$, kierunek α nie jest zdefiniowany.



Rys. 4. Współrzędne prostokątne i biegunowe

Z kolei dla punktu P o współrzędnych prostokątnych (x, y) promień wodzący tego punktu dostajemy z twierdzenia Pitagorasa, otrzymując $r = \sqrt{x^2 + y^2}$, natomiast wartość kąta α wyznaczamy z odpowiednio dostosowanej funkcji arcus tangens.

W analizie danych kierunkowych wygodnie jest czasem postrzegać daną obserwację jako wektor o początku w punkcie O i końcu w punkcie P lub, w układzie biegunowym, jako parę uporządkowaną (r, α). A ponieważ w analizie danych kierunkowych interesuje nas kierunek, a nie długość wektora, więc przyjmujemy, że rozważane wektory mają długość jednostkową (czyli $r = 1$). Tym samym przekształcenie współrzędnych biegunowych na prostokątne wyraża się następująco: $(1, \alpha) \iff (x = \cos\alpha, y = \sin\alpha)$.

Powróćmy teraz do zagadnienia uśredniania danych kierunkowych. Załóżmy, że mamy do czynienia z n-elementową próbką danych kierunkowych $P_1, \ldots, P_n$. W świetle tego, co powiedziano powyżej, możemy myśleć o tych obserwacjach jak o zbiorze odpowiadających im kątów $\alpha_1, \ldots, \alpha_n$. Po przekształceniu współrzędnych z biegunowych na prostokątne naszą próbkę będziemy mogli zapisać w postaci $(\cos\alpha_1, \sin\alpha_1), \ldots, (\cos\alpha_n, \sin\alpha_n)$.

Utwórzmy teraz nowy wektor o współrzędnych otrzymanych przez uśrednienie, odpowiednio, pierwszych i drugich współrzędnych wektorów tworzących naszą próbkę. Tym sposobem otrzymamy tzw. **wektor średni** o współrzędnych

$$(\star) \qquad (\overline{x}, \overline{y}) = \left(\frac{1}{n}\sum_{i=1}^{n} \cos\alpha_i, \frac{1}{n}\sum_{i=1}^{n} \sin\alpha_i \right).$$

Jest to oczywiście środek ciężkości wielokąta o wierzchołkach w punktach $(\cos\alpha_1, \sin\alpha_1), \ldots, (\cos\alpha_n, \sin\alpha_n)$. **Średnią kołową** $\overline{\alpha}$ definiujemy teraz jako kątową współrzędną biegunową wektora $(\overline{x}, \overline{y})$. Oznacza to również, że jeśli

$(\overline{x},\overline{y}) = (0,0)$, to średnia kołowa nie jest dobrze zdefiniowana (i jest tak tylko w tym przypadku).

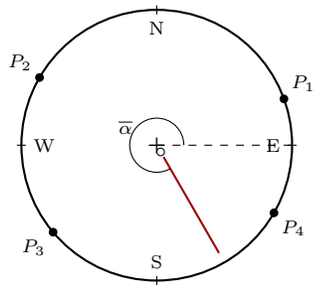
Przykład 2 (c.d.). Przekonajmy się, jaki wynik otrzymalibyśmy, podstawiając dane z przykładu 2. Przypomnijmy, że nasza próbka składa się z czterech punktów opisanych kątami: 20°, 150°, 220° i 330°. W pierwszym kroku przekształcamy współrzędne obserwacji z biegunowych na prostokątne i dostajemy

$$\begin{aligned}\big(\cos(20^\circ),\sin(20^\circ)\big) &\approx (0.94, 0.34),\\ \big(\cos(150^\circ),\sin(150^\circ)\big) &\approx (-0.87, 0.5),\\ \big(\cos(220^\circ),\sin(220^\circ)\big) &\approx (-0.76, -0.64),\\ \big(\cos(330^\circ),\sin(330^\circ)\big) &\approx (0.87, -0.5).\end{aligned}$$

Otrzymane w poprzednim kroku wartości podstawiamy do wzoru $(\star)$ na współrzędne wektora średniego: $(\overline{x},\overline{y}) \approx (0{,}043, -0{,}075)$. Ponieważ $\overline{x} > 0$ oraz $\overline{y} < 0$, więc kierunek tego wektora możemy wyznaczyć następująco:

$$\overline{\alpha} = 2\pi - \operatorname{arc\,tg}\left(\frac{|\overline{y}|}{\overline{x}}\right) = 300^\circ$$

Naszą próbkę wraz z wyznaczonym kierunkiem średnim (zaznaczonym kolorem czerwonym) pokazuje rysunek 5.



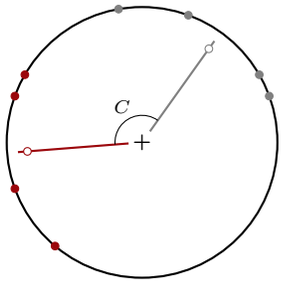
Rys. 5. Kierunki poruszania się żółwi i wyznaczona średnia kołowa $\overline{\alpha}$. Biały punkt odpowiada punktowi $(\overline{x},\overline{y})$, czyli środkowi ciężkości wielokąta $P_1P_2P_3P_4$

Polecamy Czytelnikowi zastanowienie się, dlaczego w tym wypadku średnia kołowa wynosi *dokładnie* 300°.

W kontekście kłopotów omawianych w przykładach 1 i 2 warto byłoby przekonać się, czy średnia kołowa dla danego zestawu danych zależy od wyboru kąta zerowego lub od przyjętego kierunku obrotu.

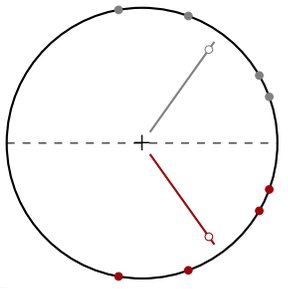
Twierdzenie 1. *Średnia kołowa $\overline{\alpha}$ wyznaczona na podstawie obserwacji kierunkowych danych kątami $(\alpha_1,\ldots,\alpha_n)$ ma następujące własności:*

(a) *jeśli $\alpha_i = \alpha_0$ dla $i = 1,\ldots,n$, to $\overline{\alpha} = \alpha_0$,*
(b) *dla dowolnego C średnia kątowa $\overline{\alpha}'$ zbioru obserwacji $(\alpha_1 + C,\ldots,\alpha_n + C)$ jest równa $\overline{\alpha} + C$,*
(c) *średnia kątowa $\overline{\alpha}'$ zbioru obserwacji $(\alpha'_1,\ldots,\alpha'_n)$, gdzie $\alpha'_i = 2\pi - \alpha_i$, jest równa $2\pi - \overline{\alpha}$.*



Rys. 6. Oryginalne dane kierunkowe oznaczone są na szaro, a dane po obróceniu o kąt C – kolorem. Wektor średni również ulega obróceniu o kąt C, więc o tyle zmienia się średnia kołowa

Zanim przejdziemy do uzasadnienia powyższego twierdzenia, zastanówmy się nad interpretacją poszczególnych własności (a)–(c). Pierwsza z nich to *idempotencja* typowa dla funkcji uśredniających, w myśl której średnia wyznaczona dla zbioru identycznych wartości jest równa tejże wartości. Własność (b) mówi, że średnia kołowa jest *ekwiwariantna* względem przesunięcia, tzn. że jeśli wszystkie kąty w zbiorze danych zostaną przesunięte o pewną stałą wartość C, to średnia kątowa $\overline{\alpha}$ również zostanie przesunięta o tę samą wartość C, a tym samym średnia kołowa nie zależy od wyboru kąta zerowego. Wreszcie wartość (c) oznacza, że średnia kołowa jest ekwiwariantna względem zmiany kierunku obrotu przyjętego do określania wartości kąta.



Rys. 7

Przejdźmy do uzasadnienia. Własność (a) jest oczywista i wynika wprost z idempotencji średniej arytmetycznej. Pozostałe własności są naturalną konsekwencją zachowania się środka ciężkości przy zastosowaniu podstawowych przekształceń geometrycznych. Punkt (b) wynika z tego, że po obróceniu wszystkich wektorów jednostkowych tworzących próbkę o dany kąt C wokół początku układu współrzędnych, wektor średni (czyli środek ciężkości wyznaczonego przez te wektory wielokąta) ulegnie temu samemu obrotowi (rys. 6). Punkt (c) ma dokładnie tę samą interpretację, przy czym tutaj zamiast obrotu rozpatrujemy odbicie symetryczne względem osi OX (rys. 7).

Należy zaznaczyć, że własności opisane w twierdzeniu 1 posiada również średnia arytmetyczna liczb rzeczywistych. Jednak średnia kołowa nie posiada pewnych własności średniej arytmetycznej. Przykładowo, w przypadku n obserwacji rozłożonych równomiernie na prostej ich średnia arytmetyczna jest równa wartości środkowej obserwacji, gdy n jest nieparzyste, lub średniej arytmetycznej z dwóch środkowych obserwacji, gdy n jest parzyste. Tymczasem dla zbioru obserwacji rozłożonych równomiernie na okręgu średnia kołowa nie istnieje, gdyż ze względu na symetrię konfiguracji wektor średni jest wektorem zerowym.

Porównując niektóre własności średniej arytmetycznej i średniej kołowej, warto przywołać pewną cechę, dzięki której średnia arytmetyczna jest postrzegana jako wielkość dobrze reprezentująca dany zbiór obserwacji na prostej. Otóż, jak wiadomo, średnia arytmetyczna minimalizuje sumę kwadratów różnic od poszczególnych obserwacji. W prosty sposób wynika to z następującej tożsamości:

$$\sum_{i=1}^{n}(x_i-a)^2=\sum_{i=1}^{n}(x_i-\overline{x})^2+n(\overline{x}-a)^2,\ \text{gdzie}\ \overline{x}=\frac{1}{n}\sum_{i=1}^{n}x_i,$$

której weryfikację pozostawiamy Czytelnikom. Czy tego typu związek istnieje dla danych kierunkowych i średniej kołowej? Okazuje się, że tak, tyle że kwadrat odległości euklidesowej trzeba zastąpić przez tzw. **odległość kosinusową**, daną wzorem $d(\alpha,\beta)=1-\cos(\alpha-\beta)$.

Odległość kosinusowa $d(\alpha,\beta)$ przyjmuje najmniejszą wartość równą 0 tylko, jeśli $\alpha=\beta$. Należy jednak zaznaczyć, że odległość kosinusowa nie spełnia nierówności trójkąta, nie jest zatem odległością w ogólnym, matematycznym rozumieniu.

Prawdziwe jest bowiem następujące twierdzenie:

Twierdzenie 2. *Niech $\overline{\alpha}$ będzie średnią kołową wyznaczoną na podstawie obserwacji kierunkowych danych kątami $(\alpha_1,\ldots,\alpha_n)$. Wówczas*

$$\overline{\alpha}=\arg\min_{\beta\in[0,2\pi)}\sum_{i=1}^{n}\big[1-\cos(\alpha_i-\beta)\big].$$

Uzasadnienie, wykorzystujące równość $\cos(\alpha-\beta)=\cos\alpha\cos\beta+\sin\alpha\sin\beta$ oraz podstawowy rachunek różniczkowy, ponownie pozostawiamy Czytelnikom.

Do tej pory koncentrowaliśmy się na średniej kołowej, czyli kierunku wektora średniego $(\overline{x},\overline{y})$. Rozważmy teraz jego długość $R=\sqrt{\overline{x}^2+\overline{y}^2}$. Okazuje się, że ma ona ciekawą interpretację, stanowiąc przydatny miernik skoncentrowania danych wokół średniej kątowej. Jak już zauważyliśmy, w przypadku danych rozłożonych równomiernie na okręgu mamy $R=0$, co nie dziwi, gdyż w tym przypadku nie istnieje średnia kołowa, a więc trudno byłoby oczekiwać skoncentrowania obserwacji wokół tej średniej. Z kolei dla zbioru identycznych wartości otrzymujemy $R=1$, czyli maksymalną możliwą wartość tego parametru, co również nie dziwi, bowiem wszystkie obserwacje są równe średniej kołowej. Dla przypadków pośrednich między całkowitą koncentracją wokół średniej kołowej a brakiem owej koncentracji wielkość R przyjmuje wartości z przedziału $(0,1)$. Przykładowo, dla danych z przykładu 1 mamy $R=0{,}9848$, co potwierdza ich duże skoncentrowanie wokół kierunku średniego, zaś dla obserwacji z przykładu 2 otrzymujemy $R=0{,}0875$, co oznacza bardzo małą koncentrację wokół średniej kołowej.

W analizie danych kierunkowych wykorzystuje się również wielkość

$$V=1-R,$$

będącą miarą rozrzutu, która jest traktowana jako odpowiednik wariancji próbkowej i bywa nazywana **wariancją kołową**. W przeciwieństwie do klasycznej wariancji próbkowej V jest miarą *unormowaną*, tzn. taką, której największa możliwa wartość to 1, przy czym wartości V bliskie zeru oznaczają małe rozproszenie, podczas gdy wartości bliskie 1 świadczą o dużym rozrzucie obserwacji.

Na zakończenie dodajmy, że poruszone w niniejszym artykule zagadnienia dotyczą jedynie wstępnego opisu danych kierunkowych, których dalsza i bardziej zaawansowana analiza pozwala wyciągać ogólne wnioski na podstawie dostępnych obserwacji. Ale to jest już materiał na odrębną opowieść.

Zadania

Przygotował Dominik BUREK

M 1816. Czy istnieje taki wielomian P stopnia 2025, że dla dowolnej liczby rzeczywistej x spełniona jest równość

$$P(x)+P(1-x)=1?$$

M 1817. Wyznaczyć liczbę 2025-cyfrowych liczb podzielnych przez 2^{2025}, których cyfry należą do zbioru $\{2,3,4,5,6,7\}$.

M 1818. Kwadratową planszę o wymiarach 10×10 podzielono na 25 kwadratów 2×2. Następnie planszę wypełniono kostkami domina (prostokątami 1×2 ułożonymi pionowo lub poziomo). Jaka jest najmniejsza liczba kostek domina, które mogą znajdować się wewnątrz kwadratów 2×2 z podziału?

Przygotował Andrzej MAJHOFER

F 1119. W szczelnym kontenerze o stałej pojemności (sztywne metalowe ściany) $V=10\ \mathrm{m}^3$ znajduje się powietrze pod ciśnieniem 1 atmosfery, $p_0=101\cdot10^3$ Pa, w temperaturze $T_0=273$ K (0°C). Ile ciepła potrzeba do ogrzania powietrza w kontenerze do temperatury $T=293$ K? Stała gazowa $R=8{,}31$ J/(mol·K).

F 1120. Naczynie w kształcie pionowego walca o wewnętrznym promieniu R ma u podstawy kołowy otworek o promieniu r. Jak prędkość wypływu wody z naczynia zależy od wysokości h jej powierzchni nad odpływem (dolnym otworkiem)? Przyspieszenie ziemskie wynosi g.

Rozwiązania na str. 24

Magia rytmu

*Jarosław GRYTCZUK**

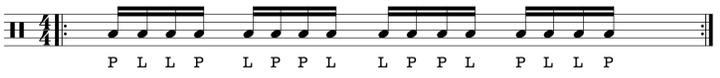
Rytm ma w sobie coś magicznego, sprawia nawet, że wierzymy, iż wzniosłość jest w naszym posiadaniu.

– Johan Wolfgang von Goethe

* Wydział Matematyki i Nauk Informacyjnych, Politechnika Warszawska

Paradiddle Nørgårda

Podręczniki do nauki gry na perkusji zawierają serie ćwiczeń z nutami podpisanymi literami P i L. Oznaczają one uderzenia odpowiednio prawą i lewą ręką. Są to tak zwane *paradiddle* – rutynowe ćwiczenia perkusisty stanowiące element codziennego treningu niezbędnego do osiągnięcia odpowiedniej sprawności technicznej.



Paradiddle

Jedno z najbardziej wyrafinowanych paradiddle wynalazł duński kompozytor Per Nørgård w latach siedemdziesiątych ubiegłego wieku. Jest to właściwie cała kolekcja coraz dłuższych ciągów prowadzących do jednego nieskończonego paradiddle. Kolejny wyraz kolekcji powstaje przez sklejenie wyrazu poprzedniego z jego „lustrzaną” kopią, w której litery P i L zamieniły się wzajemnie miejscami, niczym ręce perkusistki ćwiczącej przed lustrem:

$$\mathtt{P}, \mathtt{PL}, \mathtt{PLLP}, \mathtt{PLLPLPPL}, \mathtt{PLLPLPPLLPPLPLLP}, \ldots$$

Na przykład czwarty wyraz kolekcji PLLPLPPL składa się z wyrazu poprzedniego, PLLP, i jego lustrzanej kopii, LPPL. Można go także otrzymać poprzez naprzemienne przetasowanie tych kopii: PLLPLPPL. Nieskończone paradidle Nørgårda stanowi zatem rodzaj rytmicznego *fraktala* będącego naprzemiennym splotem dwóch kopii samego siebie – wiernej i lustrzanej:

$$N = \mathtt{PLLPLPPLLPPLPLLPLPPLPLLPPLLPLPPL}\ldots$$

Swój wynalazek Per Nørgård stosował w wielu kompozycjach, z których najsławniejszą jest chyba suita *I Ching* na perkusję solo, dedykowana duńskiemu wirtuozowi tego instrumentu Gertowi Mortensenowi. Nie jest to zatem tylko wprawka dla perkusistów, lecz złożona struktura rytmiczna, której muzyczna realizacja wymaga nie lada kunsztu. Jej psychodeliczny urok fascynuje zresztą nie tylko muzyków.

W rzeczywistości Per Nørgård wymyślił najpierw ciąg liczbowy: $0, 1, -1, 2, 1, 0, -2, 3, -1, 2, 0, 1, 2, -1, \ldots$, będący splotem dwóch ciągów, które są prostymi przekształceniami wyjściowego ciągu. Pierwszy powstaje przez *inwersję*, czyli zastąpienie wyrazów wyjściowego ciągu elementami do nich przeciwnymi: $0, -1, 1, -2, -1, 0, 2, -3, \ldots$, drugi zaś powstaje w wyniku działania *translacji*, czyli przez dodanie 1 do każdej z pierwotnych liczb: $1, 2, 0, 3, 2, 1, -1, 4, \ldots$ Kopie te przeplatają się naprzemiennie, tworząc oryginalny ciąg. Nie był on znany wcześniej w matematyce. Kompozytor stosuje go często w swoich utworach jako linię melodyczną, ale także jako hierarchiczną strukturę harmoniczną. Paradiddle N powstaje przez zastąpienie liczb parzystych literą P, a nieparzystych literą L.

Twierdzenia Thuego

W istocie ciąg N pojawił się w matematyce już w połowie dziewiętnastego stulecia w pracy francuskiego matematyka Eugène'a Prouheta, która traktowała o pewnym problemie rozkładania liczb naturalnych na sumy potęg. Jako osobny obiekt studiów matematycznych został na nowo odkryty na początku dwudziestego wieku przez norweskiego matematyka Axela Thuego. Ten wybitny specjalista teorii liczb dostrzegł czysto kombinatoryczne piękno ciągu N przejawiające się w takiej oto niesamowitej własności: *żadne dwa nakładające się segmenty ciągu N nie są identyczne.* Na przykład zaznaczone poniżej segmenty, PPLLPP i PPLPLL, różnią się na trzech ostatnich pozycjach:

$$N = \mathtt{PLLPL}\underline{\mathtt{PPLLPP}}\overline{\mathtt{LPPLPLL}}\mathtt{PLPPLPLLPPLLPLPPL}\ldots$$

Konsekwencją tej własności jest to, że żadne trzy sąsiadujące segmenty w ciągu N nie mogą być identyczne:

$$N = \mathtt{PLLPLPPLLPPLPLLPLPPLPLLPPLLPLPPL}\ldots$$

Ciąg N jest zatem wielce „niepowtarzalny” – po wystąpieniu obok siebie dwóch identycznych segmentów następny jest zawsze inny. Prawdziwy koszmar perkusistów...

Nasuwa się naturalne pytanie: czy istnieje nieskończone paradiddle, w którym dwa sąsiadujące segmenty są zawsze różne? Zauważmy, że każdy ciąg długości cztery zbudowany z dwóch liter albo zawiera bezpośrednie powtórzenie pojedynczej litery, PP lub LL, albo ma postać PLPL lub LPLP. A zatem jeżeli chcemy uniknąć powtarzających się obok siebie segmentów, to musimy

Dla zilustrowania twierdzenia Prouheta spójrzmy na czwarty ciąg kolekcji, PLLPLPPL. Wyznacza on dwa zbiory liczb odpowiadające pozycjom dwóch liter, $P = \{1, 4, 6, 7\}$ i $L = \{2, 3, 5, 8\}$. Zbiory te mają nie tylko równe sumy: $1 + 4 + 6 + 7 = 2 + 3 + 5 + 8$, ale także równe sumy kwadratów: $1^2 + 4^2 + 6^2 + 7^2 = 2^2 + 3^2 + 5^2 + 8^2$. Dla następnego ciągu analogiczne zbiory mają nie tylko równe sumy i równe sumy kwadratów, ale także równe sumy sześcianów! I tak dalej...

Dowód twierdzenia Thuego nie jest trudny. Można go przeprowadzić, wykorzystując fraktalne samopodobieństwo ciągu N. Zauważmy, że hipotetyczna nakładająca się para identycznych segmentów musiałaby zawierać na początku segment postaci $S = xAxAx$, gdzie A jest segmentem, a x pojedynczą literą. Zakładając, że S jest najkrótszym takim segmentem występującym w N, wystarczy rozważyć dwa przypadki odpowiadające różnym parzystościom długości segmentu A. Oba prowadzą szybko do sprzeczności.

powiększyć zasób liter stanowiących budulec ciągu. Na szczęście w grze na perkusji używa się nie tylko rąk, ale i nóg. W bardziej zaawansowanych paradiddle występuje wraz z literami P i L także litera S, oznaczająca uderzenie w wielki bęben wykonane za pomocą stopy.

Już w roku 1906 Thue skonstruował z trzech liter nieskończony ciąg, w którym *żadne dwa sąsiadujące segmenty nie są identyczne*. Można go otrzymać z ciągu N, odczytując liczbę wystąpień litery L pomiędzy kolejnymi literami P:

$$N = \mathtt{P}\underbrace{\mathtt{LL}}_{2}\mathtt{P}\underbrace{\mathtt{L}}_{1}\mathtt{P}\underbrace{\phantom{\mathtt{L}}}_{0}\mathtt{P}\underbrace{\mathtt{LL}}_{2}\mathtt{P}\underbrace{\phantom{\mathtt{L}}}_{0}\mathtt{P}\underbrace{\mathtt{L}}_{1}\mathtt{P}\underbrace{\mathtt{LL}}_{2}\mathtt{P}\underbrace{\mathtt{L}}_{1}\mathtt{P}\underbrace{\phantom{\mathtt{L}}}_{0}\mathtt{P}\underbrace{\mathtt{L}}_{1}\mathtt{P}\underbrace{\mathtt{LL}}_{2}\mathtt{P}\ldots$$

Podstawiając $2 = \mathtt{P}$, $1 = \mathtt{L}$ i $0 = \mathtt{S}$, dostajemy paradiddle na dwie ręce i stopę, w którym żaden segment nie powtarza się dwa razy z rzędu:

$$T = \mathtt{PLSPSLPLSLPSPLSPSLPSPLSLPLSPSLPLSLPSPLSLPLSPS}\ldots$$

Ta własność ciągu T wynika wprost z tego, że w ciągu N nie ma nakładających się identycznych segmentów. Na przykład zaznaczone powyżej segmenty w ciągu T nie są identyczne, choć różnią się jedynie na ostatniej pozycji.

Ciąg składający się z sąsiadujących powtórzeń tego samego segmentu nazywamy *repetycją*. Liczba tych segmentów to *krotność* repetycji. Na przykład ciągi PP, PLPL, LPPLPP, PLPSPLPS to repetycje dwukrotne, PPP, PSPSPS, LLSLLSLLS to repetycje trzykrotne, natomiast PPLSPPLSPPLSPPLS to repetycja czterokrotna. Nieskończony ciąg okresowy to oczywiście repetycja o krotności nieskończonej. Twierdzenia Thuego orzekają zatem, że istnieje nieskończony ciąg binarny bez repetycji trzykrotnych (ciąg N) oraz nieskończony ciąg ternarny bez repetycji dwukrotnych, a tym samym bez żadnych repetycji (ciąg T).

Twierdzenia Thuego zostały opublikowane w dwóch pracach, w roku 1906 i 1912, w mało znanym czasopiśmie. Przez wiele lat pozostawały niezauważone. Były zresztą odkrywane niezależnie przez wielu badaczy w rozmaitych kontekstach (układy dynamiczne, teoria grup, turnieje szachowe, zagadnienia sprawiedliwego podziału etc.). Obecnie uznaje się je za początek *kombinatoryki na słowach* – obszernej dziedziny o licznych zastosowaniach i powiązaniach z różnymi działami matematyki i informatyki, a także biologii obliczeniowej.

Odkrycia Thuego, wzmocnione doznaniami muzycznymi, wciąż ekscytują badaczy. Pojawiają się rozmaite warianty, uogólnienia, nowe problemy otwarte. Oto próbka zawartości tego „rogu obfitości”.

Ciągi z list

Problem 1. Niech dany będzie nieskończony ciąg zbiorów trójelementowych $A_1, A_2, A_3, \ldots$ Czy z każdego z nich można wybrać element $a_i \in A_i$ tak, aby nieskończony ciąg $a_1a_2a_3\ldots$ nie zawierał żadnych repetycji?

Twierdzenie Thuego odpowiada przypadkowi, kiedy wszystkie zbiory są identyczne. Jeżeli choć dwa zbiory A_i są różne, to mamy w sumie więcej różnych liter do dyspozycji i wydaje się, że utworzenie ciągu bez repetycji powinno być nawet łatwiejsze. Jednakże nikt jak dotąd nie podał rozwiązania problemu 1 w pełnej ogólności. Znaleziono natomiast rozwiązania pewnych szczególnych przypadków. Wiadomo, że odpowiedź jest pozytywna, jeżeli wszystkie zbiory A_i są czteroelementowe, a także jeżeli są trójelementowymi podzbiorami tego samego zbioru czteroelementowego. Ostatnio podjęta próba sprowadza problem do komputerowego sprawdzenia skończonej liczby przypadków, która wszakże jest na tyle duża, że na ostateczny efekt przyjdzie jeszcze poczekać.

W listowym kolorowaniu grafu dzieją się rzeczy dziwne. Przypuśćmy, że graf G da się poprawnie pokolorować dwoma kolorami. Ktoś przydzielił wierzchołkom palety kolorów, po sto w każdej. Czy możemy mieć pewność, że uda nam się poprawnie pokolorować graf G, wybierając każdemu wierzchołkowi kolor z jego palety? Okazuje się, że w wielu przypadkach odpowiedź jest negatywna – istnieją rozmieszczenia palet (z dowolnie dużą liczbą kolorów) tak złośliwe, że jest to niewykonalne!

Powyższy problem jest analogiem *listowego* kolorowania grafu. W zwykłym kolorowaniu grafu każdy wierzchołek dostaje kolor z jednej wspólnej palety kolorów. W kolorowaniu listowym każdy wierzchołek ma z góry określoną własną paletę kolorów (*listę*) i tylko z niej można wybierać kolor, którym zostanie pomalowany. Zachodzi pozorny paradoks – przy różnych paletach mamy w sumie więcej kolorów do dyspozycji, wydaje się zatem, że kolorowanie grafu tym łatwiej powinno się udać. Jednak rozmieszczenie palet narzuca pewne ograniczenia, które mogą skutkować zaskakującymi trudnościami. Znane są przykłady grafów planarnych z tak podstępnym rozmieszczeniem palet – z czterema kolorami każda, że poprawne kolorowanie nie istnieje, choć, jak wiadomo, w tradycyjnej wersji cztery kolory wystarczają.

Wybierzmy zbiór punktów na płaszczyźnie, a następnie połączmy niektóre pary punktów odcinkami tak, aby żadne dwa odcinki nie krzyżowały się, czyli aby ich wnętrza były rozłączne. Klasa tak uzyskanych grafów to grafy *planarne* znane ze słynnego problemu czterech barw. Inną elegancką interpretację geometryczną grafów planarnych dostaniemy, rysując na płaszczyźnie koła o dowolnych promieniach i parami rozłącznych wnętrzach, ale mogące stykać się na brzegach. Wierzchołki grafu umieszczamy w środkach tych kół, łącząc krawędziami te pary środków, które odpowiadają kołom stycznym. Każdy taki graf jest oczywiście planarny, ale zaskakujące jest to, że każdy graf planarny można w ten sposób uzyskać.

Repetycje anagramowe

Anagramem słowa (ciągu) jest słowo powstałe z niego w wyniku dowolnego przestawienia liter. Na przykład BAROK i KORBA są nawzajem swoimi anagramami. Ciąg będący sklejeniem dwóch anagramów tego samego słowa nazywamy

repetycją anagramową. Innymi słowy jest to taki ciąg, który można rozciąć jednym cięciem na dwie części, z których każda ma tyle samo wystąpień każdej litery, na przykład PLLSSSPLSSLS. Repetycje anagramowe wielokrotne definiujemy analogicznie do zwykłych repetycji, jako sklejenie wielu anagramów tego samego słowa. Na przykład KTOTOKKOT jest trzykrotną repetycją anagramową.

Słynny matematyk Paul Erdős zainspirowany twierdzeniami Thuego zadał takie oto pytanie: *Czy istnieje nieskończony ciąg bez repetycji anagramowych zbudowany z czterech liter?*

Można sprawdzić, że najdłuższy ciąg bez repetycji anagramowych utworzony z trzech liter ma długość dwanaście. Udowodniono natomiast, że trzy litery wystarczą do konstrukcji nieskończonego ciągu bez trzykrotnych repetycji anagramowych, a także że istnieją nieskończone ciągi bez czterokrotnych repetycji anagramowych zbudowane tylko z dwóch liter.

Pytanie Erdősa pozostawało bez odpowiedzi przez wiele lat, aż w końcu i ono znalazło pozytywne rozstrzygnięcie. Konstrukcję odpowiedniego ciągu podał Veikko Kearänen w roku 1992. Jest ona podobna w duchu do konstrukcji Thuego, lecz bardziej skomplikowana technicznie (nie obyło się raczej bez użycia komputera). Właściwie ciąg Keränena również można zinterpretować jako paradiddle, tym razem angażujące obie ręce i obie nogi perkusistki:

$K =$ SPSHSLSHSPHSHLHPLPSPLPHLPLSLHLSLPSLSHSPSLPLH...

Litera H oznacza hi-hat – instrument perkusyjny składający się z dwóch talerzy zamocowanych poziomo na statywie, które uderzają o siebie niczym klaszczące dłonie na skutek przyciskania lewą stopą pedału w statywie. Jeżeli poprzednie paradiddle T i N były wielce „niepowtarzalne", to co powiedzieć o tym? W ciągu K każde dwa sąsiadujące segmenty są nie tylko różne, ale pozostają różne nawet po dowolnym przestawieniu wyrazów w jednym z nich...

Gdyby w roli liter obsadzić liczby pierwsze, to w ciągu mającym własność Erdősa iloczyny wyrazów dwóch sąsiednich segmentów nigdy nie będą równe. Nie oznacza to jednak, że iloczyn liczb w żadnym segmencie nie będzie kwadratem. Można wykazać, że każdy dostatecznie długi ciąg zbudowany ze skończonej liczby liter-liczb zawiera segment o kwadratowym iloczynie wyrazów. Natomiast w ciągu liczb naturalnych, $1, 2, 3, 4, 5, 6, 7, 8, \ldots$, nie ma żadnego segmentu (długości co najmniej dwa), którego iloczyn wyrazów jest kwadratem, sześcianem czy też jakąkolwiek wyższą potęgą.

Natomiast ciągle bez odpowiedzi pozostaje poniższe pytanie.

Problem 2. Niech dany będzie nieskończony ciąg zbiorów czteroelementowych $A_1, A_2, A_3, \ldots$ Czy z każdego z nich można wybrać element $a_i \in A_i$ tak, aby nieskończony ciąg $a_1a_2a_3\ldots$ nie zawierał żadnych repetycji anagramowych?

Tym razem nie wiadomo, czy odpowiedź jest pozytywna, nawet jeżeli powiększymy rozmiar zbiorów A_i do dowolnej skończonej stałej k.

Repetycje sumacyjne

Ciąg liczbowy nazywamy *repetycją sumacyjną,* jeżeli jest sklejeniem dwóch ciągów o równej liczbie wyrazów i równych sumach. Na przykład ciąg 124232 nie jest repetycją zwykłą ani repetycją anagramową, ale jest repetycją sumacyjną. Repetycje sumacyjne wielokrotne definiujemy podobnie jak poprzednio.

Problem 3. Czy dla jakiejś liczby naturalnej k istnieje nieskończony ciąg bez repetycji sumacyjnych o wyrazach ze zbioru $\{0, 1, 2, \ldots, k\}$?

Zauważmy, że ciąg o wyrazach $\{0, 1\}$ jest repetycją sumacyjną wtedy i tylko wtedy, gdy jest repetycją anagramową. Wiemy zatem, że istnieje nieskończony ciąg binarny bez repetycji sumacyjnych czterokrotnych. Udowodniono także, że istnieje nieskończony ciąg bez trzykrotnych repetycji sumacyjnych o wyrazach $\{0, 1, 5\}$.

Repetycje na grafach

Ciąg wierzchołków $v_1v_2\ldots v_k$ grafu G nazywamy *ścieżką,* jeżeli żadne dwa jego wyrazy nie są identyczne, a każde dwa kolejne wyrazy są połączone krawędzią. Kolorowanie wierzchołków grafu G nazywamy *niepowtarzalnym*, jeżeli ciąg kolorów na żadnej ścieżce nie zawiera repetycji. Najmniejszą liczbę kolorów potrzebnych do niepowtarzalnego pokolorowania grafu G oznaczamy przez $\pi(G)$. Twierdzenie Thuego orzeka na przykład, że $\pi(P) = 3$, gdzie P oznacza dowolną ścieżkę o co najmniej czterech wierzchołkach. Ile kolorów potrzeba do niepowtarzalnego pokolorowania grafów planarnych?

Problem 4. Ile wynosi minimalne k takie, że nierówność $\pi(G) \leqslant k$ zachodzi dla każdego grafu planarnego G?

Problem ten został postawiony dwadzieścia pięć lat temu. Przez dwadzieścia lat nie było nawet wiadomo, czy odpowiedź jest liczbą skończoną. Przełom nastąpił pięć lat temu, kiedy to udowodniono, że każdy graf planarny spełnia nierówność $\pi(G) \leqslant 768$. Z pewnością nie jest to optymalne oszacowanie.

Dowód tego, że liczba $\pi(G)$ ma skończone ograniczenie w klasie grafów planarnych, jest dość prostą konsekwencją zaskakującej strukturalnej własności, pozwalającej zanurzać je w produkty znacznie prostszych grafów, podobnych do drzew. Te prostsze grafy dają się już względnie łatwo kolorować w stylu Thuego. Ostateczne kolorowanie dostajemy zatem jako „produkt" niepowtarzalnych kolorowań prostszych składników. Stąd ograniczenie na liczbę kolorów $768 = 3 \cdot 4 \cdot 64$. Więcej szczegółów można znaleźć w artykule: doi.org/10.19086/aic.12100.

Łamanie rytmu na grafie

Niech k będzie liczbą naturalną i niech $\pi_k(G)$ oznacza najmniejszą liczbę kolorów w kolorowaniu wierzchołków grafu G bez k-krotnych repetycji na ścieżkach. Oczywiście $\pi_2(G)$ to ten sam parametr co $\pi(G)$. Twierdzenie Thuego orzeka zaś, że $\pi_3(P) = 2$ dla dowolnej ścieżki P o co najmniej trzech wierzchołkach.

Hipoteza. Każdy graf planarny G spełnia nierówność $\pi_{2025}(G) \leqslant 4$.

Jeżeli to prawda, to każdy graf planarny można tak pokolorować czterema kolorami, że wędrując wzdłuż dowolnej ścieżki, być może natrafimy na 2024 identyczne segmenty z rzędu, ale na pewno nie na 2025. Jest to nieco łagodniejsza wersja hipotezy z roku 2000, która postulowała silniejszą nierówność $\pi_{2000}(G) \leqslant 4$. W przyszłym roku, a także prawdopodobnie w wielu kolejnych latach, ulegnie ona kolejnym osłabieniom. Obecnie nie wiadomo nawet, czy ma szansę być kiedykolwiek prawdziwa, to znaczy, czy nierówność $\pi_k(G) \leqslant 4$ może zachodzić, przy pewnym skończonym k, dla wszystkich grafów planarnych G. Być może liczba 4 w tej nierówności jest zbyt mała, wiadomo jednak, że nie można jej już obniżyć, istnieją bowiem grafy planarne, w których pojawiają się dowolnie długie jednobarwne ścieżki przy dowolnych kolorowaniach trzema kolorami. Jeżeli cztery kolory nie wystarczą do uniknięcia repetycji o dowolnie dużej krotności na grafach planarnych, to może trzeba użyć w tym celu pięciu, sześciu, trzynastu albo sześciuset sześćdziesięciu sześciu kolorów… ? Dla pewnej liczby $r \leqslant 768$ hipoteza musi być prawdziwa przy być może gigantycznym, ale skończonym k. Chciałoby się poznać najmniejsze takie r, a zaraz potem najmniejsze takie k, chociaż właściwie nie wiadomo po co…

Kąt Otwarty 3°: Nonszalanckie słowotwórstwo

Bartłomiej PAWLIK

Politechnika Śląska

Skończony ciąg elementów danego zbioru Σ nazywamy *słowem nad alfabetem* Σ. O ile nie prowadzi to do niejednoznaczności, słowo zapisujemy jako konkatenację elementów zbioru Σ. Na przykład słowo $(\mathtt{s}, \mathtt{ł}, \mathtt{o}, \mathtt{w}, \mathtt{o})$ nad alfabetem $\Sigma = \{\mathtt{ł}, \mathtt{o}, \mathtt{s}, \mathtt{w}\}$ można zapisać jako `słowo`.

Rozszerzeniem słowa PS jest słowo $P\mathtt{x}S$, gdzie `x` jest literą (każde ze słów P, S może być słowem pustym). Przykładowym rozszerzeniem słowa `bak` jest `bark`, a rozszerzeniem słowa `bark` jest `barek`.

Niech X będzie słowem niepustym. Słowo postaci XX (np. `kuskus`) nazywamy *kwadratem*. Mówimy, że słowo $PXXS$ *zawiera* kwadrat XX, natomiast *słowem bezkwadratowym* jest takie, które nie zawiera żadnego kwadratu. Zatem `matematyka` jest słowem bezkwadratowym, a `filologia` nim nie jest (zawiera kwadrat `lolo`).

Dany jest alfabet Σ (zakładamy, że jest *uporządkowany*, czyli litery mają – jak to w alfabecie – pewną kolejność). Rozważmy następującą *procedurę nonszalancką*: Zaczynamy od słowa pustego $W_0 = \varepsilon$. W n-tym kroku procedury tworzymy rozszerzenie W_n poprzedniego słowa W_{n-1} w następujący sposób: na końcu słowa W_{n-1} wstawiamy możliwie najmniejszą literę `x` taką, że otrzymane słowo $W_n = W_{n-1}\mathtt{x}$ jest bezkwadratowe. Jeżeli nie jest to możliwe, to próbujemy wstawić jak najmniejszą literę tuż przed ostatnią literą naszego słowa. Jeżeli to też jest niemożliwe, to próbujemy wstawić jak najmniejszą literę przed ostatnimi dwiema literami itd. Reasumując, w każdym kroku staramy się najdalej, jak tylko można, wstawić jak najmniejszą literę, by uzyskać słowo bezkwadratowe.

Zauważmy, że nad alfabetem $\{\mathtt{a}, \mathtt{b}\}$ procedura kończy się szybko:

$$\varepsilon \;\to\; \underline{\mathtt{a}} \;\to\; \mathtt{a}\underline{\mathtt{b}} \;\to\; \mathtt{ab}\underline{\mathtt{a}}.$$

Każde rozszerzenie słowa `aba` zawiera kwadrat, więc nie sposób otrzymać kolejnego rozszerzenia.

Co się stanie, gdy zwiększymy alfabet? Dla alfabetu ternarnego $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$ początkowych kilka słów to

$$\varepsilon \;\to\; \underline{\mathtt{a}} \;\to\; \mathtt{a}\underline{\mathtt{b}} \;\to\; \mathtt{ab}\underline{\mathtt{a}} \;\to\; \mathtt{aba}\underline{\mathtt{c}} \;\to\; \mathtt{abac}\underline{\mathtt{a}} \to\; \mathtt{abaca}\underline{\mathtt{b}} \;\to\; \mathtt{abacab}\underline{\mathtt{a}} \;\to$$
$$\to\; \mathtt{abacabca} \;\to\; \mathtt{abacabcac} \;\to\; \mathtt{abacabcacb} \;\to\; \cdots.$$

Czy i w tym przypadku procedura dobiega końca po skończonej liczbie kroków? **Nie wiadomo**. Teoretycznie nie można tego wykluczyć, ponieważ wiemy, że nad alfabetem ternarnym istnieje nieskończenie wiele słów, których każde rozszerzenie zawiera kwadrat. Obecnie wiemy również, że nie ma ani jednego słowa o tej własności nad alfabetem 17-elementowym (więc nad takim alfabetem procedura nonszalancka nigdy się nie zakończy).

A czy istnieją słowa, których każde rozszerzenie zawiera kwadrat w przypadku alfabetów mocy od 4 do 16? Jak powyżej – **nie wiadomo**.

O weryfikacji protokołów kryptograficznych

Tomasz BRENGOS, Anna CICHOCKA, Hubert GROCHOWSKI, Konstanty JUNOSZA-SZANIAWSKI, Adam KOMOROWSKI, Agata PILITOWSKA

Wydział Matematyki i Nauk Informacyjnych, Politechnika Warszawska

Wyobraźmy sobie, że na ważnej kolacji spotykają się dyplomaci. Rzecz jasna, podczas takiego spotkania obowiązują pewne reguły – każdy wie, gdzie ma usiąść, każdy wie, co i kiedy może powiedzieć, każdy wie, jak zareagować na działanie innych dyplomatów, tak aby było to „zgodne z protokołem". Podobnie możemy wyobrażać sobie *protokół komunikacyjny* jako zbiór zasad i instrukcji dla każdej ze stron, które chcą się ze sobą porozumieć – taki protokół dyplomatyczny dla interlokutorów. W protokole komunikacyjnym występują różne strony komunikacji, nazywane *agentami* (może to być na przykład klient banku, serwer albo brygada wojskowa), które przesyłają między sobą różne *wiadomości* według ustalonego porządku. Kiedy komunikacja przebiega zgodnie z protokołem, strony dokładnie wiedzą, co się dzieje, o co chodzi i co należy zrobić. Często od protokołu komunikacyjnego będziemy oczekiwać zapewnienia odpowiedniego poziomu bezpieczeństwa – na przykład oprócz skutecznej komunikacji będzie on musiał zagwarantować, że część wiadomości będzie dostępna wyłącznie dla uprawnionych stron (dla pozostałych pozostanie ukryta). Taki protokół nazywamy *protokołem kryptograficznym*.

Naturalnym sposobem przekształcenia zwykłego protokołu komunikacyjnego w protokół kryptograficzny wydaje się *zaszyfrowanie wiadomości*, czyli przekształcenie jej w taki sposób, aby adresat mógł ją *odszyfrować* (tzn. odwrócić przekształcenie wykonane przez nadawcę) za pomocą odpowiedniej, innej wiadomości (nazywanej *kluczem*). Chcielibyśmy to zrobić tak, aby osoba postronna, która nie posiada klucza, nie potrafiła odczytać wiadomości. Przy tym podejściu pojawiają się co najmniej dwa problemy. Pierwszy z nich został przedstawiony na rysunku.

Zaszyfrowana wiadomość, która jest łatwa do odczytu. Rysunek pochodzi z [4]

Powyższy obrazek został zaszyfrowany za pomocą algorytmu szyfrującego uważanego powszechnie za bardzo silny, który dodatkowo wykorzystuje długi klucz. Mimo to bez trudu możemy odczytać, co znajdowało się na obrazku przed szyfrowaniem. Ten przykład pokazuje, że sam dobry szyfr lub długi klucz nie wystarczą – równie istotne jest ich właściwe użycie. Konkretniej, zastosowany w tym przypadku algorytm jest deterministyczny, co oznacza, że dla tych samych danych zawsze daje ten sam wynik. (Przeciwieństwem algorytmów deterministycznych są algorytmy losowe). Co więcej, powyższy obrazek przed szyfrowaniem składał się głównie z białego tła. Algorytm szyfrujący podzielił go na mniejsze fragmenty i zaszyfrował każdy z nich osobno. Ponieważ wiele fragmentów zawierało wyłącznie białe tło, a algorytm jest deterministyczny, to każdy taki fragment został zaszyfrowany w ten sam sposób. Z drugiej strony fragmenty zawierające choćby niewielką część liter były szyfrowane inaczej. W rezultacie po zaszyfrowaniu można zauważyć różnice między obszarami tła a literami, co pozwala na częściowe odtworzenie pierwotnego obrazu.

Drugim problemem z szyfrowaniem jest konieczność zapewnienia, by adresat posiadał klucz odpowiedni do odszyfrowania wiadomości – musi on odpowiadać kluczowi użytemu do jej zaszyfrowania. To wyzwanie nazywane jest problemem wymiany klucza i przez wiele lat stanowiło poważne wyzwanie dla kryptologów. Dawniej wystarczającym rozwiązaniem było fizyczne dostarczenie wspólnego (symetrycznego) klucza obu stronom komunikacji. Nietrudno jednak zauważyć, że metoda ta jest mało wygodna i czasochłonna. Z tego powodu podjęto wiele wysiłków w celu opracowania bardziej efektywnego podejścia. Jednym z najważniejszych rozwiązań tego problemu jest protokół Diffiego–Helmana [3], opracowany w 1976 roku przez Whitfielda Diffiego i Martina Hellmana. W tym protokole uczestniczą dwie strony – zwykle nazywane Alicją i Bobem. W podstawowej wersji protokołu, na samym początku wszystkim są znane dwa parametry – dostatecznie duża liczba pierwsza p oraz liczba naturalna g od 2 do $p-1$, która ma następującą własność:

$$\{g^k \bmod p : k \in \mathbb{N}\} = \{1, 2, \ldots, p-1\}.$$

Innymi słowy, kolejne potęgi liczby naturalnej g dają wszystkie możliwe, niezerowe reszty z dzielenia przez p. W języku teorii grup oznacza to, że liczba g jest *generatorem* grupy $\mathbb{Z}_p^*$.

Liczby p oraz g są parametrami *publicznymi*, czyli mogą je znać nawet strony nieuczestniczące w tej komunikacji. Następnie protokół przebiega zgodnie z następującym schematem:

1. Alicja losuje liczbę naturalną a i wysyła do Boba liczbę $g^a \bmod p$ (resztę z dzielenia g^a przez p);
2. Bob losuje liczbę naturalną b i wysyła do Alicji liczbę $g^b \bmod p$ (resztę z dzielenia g^b przez p).

Zauważmy, że w ten sposób zarówno Alicja, jak i Bob są w stanie ustalić wspólną liczbę, którą mogą wykorzystać jako klucz. Popatrzmy na ten problem z perspektywy Alicji. Otrzymała ona od Boba liczbę $g^b \bmod p$, ale nie zna liczby b. Jednakże Alicja może podnieść otrzymaną liczbę do wylosowanej przez siebie potęgi a. W ten sposób, korzystając z własności potęgowania i arytmetyki modularnej, otrzymujemy:

$$(g^b \bmod p)^a = g^{ba} \bmod p.$$

Analogicznie Bob może podnieść otrzymaną od Alicji liczbę $g^a \bmod p$ (nie zna on a) do swojej potęgi b, otrzymując:

$$(g^a \bmod p)^b = g^{ab} \bmod p = g^{ba} \bmod p.$$

W ten sposób zarówno Alicja, jak i Bob znają razem pewną wspólną liczbę. Okazuje się, że jeśli odpowiednio dobierzemy parametry publiczne g i p, to problem znalezienia właściwego wykładnika dla osoby postronnej, mającej tylko wiedzę publiczną, wydaje się obecnie trudny do rozwiązania. Problem ten znany jest jako *problem logarytmu dyskretnego*. Warto podkreślić, że gdy jako ludzkość będziemy dysponować odpowiednio złożonym komputerem kwantowym, problem ten na pewno będziemy mogli rozwiązać „szybko". To jednak temat na zupełnie inną opowieść...

Zadanie 1. Ile wynosi $13^7 \bmod 19$? Znajdź wszystkie liczby naturalne $a \in \mathbb{N}_+$ takie, że $13^a \bmod 19 = 7$.

Zadanie 2. Ile istnieje różnych generatorów grupy $\mathbb{Z}_{13}^*$?

Innym podejściem do szyfrowania jest wykorzystanie szyfrów *asymetrycznych*. W przeciwieństwie do szyfrów symetrycznych, wykorzystują one parę kluczy – klucz *publiczny* i klucz *prywatny*. Jeden z kluczy służy do szyfrowania wiadomości, a drugi do odszyfrowania. Jeśli upublicznimy klucz używany do szyfrowania, to każdy będzie mógł zaszyfrować wiadomość (dlatego nazywany jest kluczem publicznym) i wysłać ją do właściciela drugiego klucza z pary. Tylko właściciel klucza prywatnego będzie w stanie odszyfrować taką wiadomość (stąd nazwa klucz prywatny).

Aby lepiej zobrazować działanie tej techniki, można wyobrazić sobie bank, który udostępnia jeden klucz publiczny wszystkim swoim klientom. Każdy klient może użyć tego klucza do zaszyfrowania wiadomości do banku, a ponieważ tylko bank posiada odpowiadający klucz prywatny, tylko on jest w stanie odszyfrować te wiadomości. Dzięki temu bank nie musi przechowywać osobnych kluczy dla każdego klienta, co upraszcza proces komunikacji. Ten przykład ilustruje, w jaki sposób asymetryczne szyfrowanie pozwala na bezpieczne przesyłanie danych do jednego, centralnego odbiorcy.

Pojawia się jednak kolejny problem – skąd możemy mieć pewność, że klucz publiczny rzeczywiście pochodzi od adresata naszej wiadomości, a nie od osoby podszywającej się pod niego? Podobnie, skąd wiadomo, że wiadomość zaszyfrowana przy użyciu klucza publicznego faktycznie pochodzi od zamierzonego nadawcy? Rozwiązanie tej kwestii jest dobrze znane i powszechnie stosowane we współczesnym świecie – mowa o podpisie elektronicznym. Podpis weryfikuje się jednak za pomocą klucza publicznego, i znowu wracamy do poprzedniego problemu. Oczywiście istnieją skuteczne sposoby radzenia sobie z takimi trudnościami. Na przykład w systemach komputerowych klucze publiczne producentów są wbudowane na stałe, co umożliwia weryfikację autentyczności kolejnych kluczy publicznych. Sposoby przekazywania i weryfikowania autentyczności kluczy, wiadomości oraz tożsamości uczestników komunikacji stanowią *kluczową* istotę protokołów kryptograficznych.

Kiedy zatem możemy uznać, że protokół kryptograficzny jest bezpieczny? A właściwie, co to w ogóle znaczy, że jest bezpieczny? Bezpieczeństwa protokołu nie da się ocenić w oderwaniu od modelu zagrożeń, w którym funkcjonuje. Na przykład, jeśli założymy, że atakujący nie ma możliwości podsłuchiwania wiadomości ani dostępu do żadnych dodatkowych źródeł informacji, to każdy protokół można by uznać za bezpieczny. Jednak w bardziej realistycznym scenariuszu, gdy atakujący może podsłuchiwać komunikację lub obserwować działania użytkowników, ukrycie czegokolwiek przed nim staje się znacznie trudniejsze. Właśnie dlatego określenie modelu zagrożeń jest kluczowe dla oceny bezpieczeństwa protokołu kryptograficznego.

Jednym z najprostszych, a zarazem szeroko wykorzystywanych modeli tego typu jest model symboliczny, znany jako model Doleva–Yao. Zakłada on, że atakujący ma pełną kontrolę nad kanałem komunikacyjnym. Może on podsłuchiwać, przechwytywać, zatrzymywać oraz podmieniać dowolne przesyłane wiadomości. Atakujący posiada pełną wiedzę publiczną, ale nie ma dostępu do informacji znanych wyłącznie poszczególnym agentom, takich jak klucze prywatne.

Kluczowym założeniem modelu Doleva–Yao jest również to, że wykorzystywane prymitywy kryptograficzne (czyli szyfry, podpisy i inne podstawowe funkcje kryptograficzne, o których tutaj nie mówimy) są idealne. Oznacza to, że atakujący nie jest w stanie odszyfrować wiadomości bez posiadania odpowiedniego klucza – nie potrafi nic wywnioskować o kluczach prywatnych, nawet jeśli ma dostęp do niezaszyfrowanej i zaszyfrowanej wersji kilku wiadomości (rodzaj ataku znany jako „atak ze znanym tekstem jawnym").

Niektórzy mogą twierdzić, że takie założenia są nierealistyczne, ponieważ trudno wyobrazić sobie atakującego, który ma tak szerokie możliwości kontroli nad kanałem komunikacyjnym. Dlatego analiza bezpieczeństwa w modelu Doleva–Yao jest uznawana za dość rygorystyczną – jeśli protokół okaże się bezpieczny w tak wymagającym środowisku, istnieje szansa, że będzie bezpieczny również w bardziej realistycznych warunkach. Z drugiej strony w rzeczywistości prymitywy kryptograficzne mogą być słabe lub źle zaimplementowane, a klucze zbyt krótkie.

W takich sytuacjach, dysponując wystarczającą mocą obliczeniową, atakujący może złamać szyfr i odczytać zaszyfrowaną wiadomość. Zatem protokół, którego bezpieczeństwo udowodniono w modelu Doleva–Yao, jest bezpieczny tylko wtedy, gdy prymitywy kryptograficzne są rzeczywiście bezpieczne, a hasła odpowiednio długie i trudne do odgadnięcia.

W innym modelu komunikacji, nazywanym *modelem obliczeniowym*, zakłada się, że atakujący, dysponując odpowiednio dużą mocą obliczeniową, może złamać szyfr, zwłaszcza jeśli hasło lub klucz szyfrujący są relatywnie krótkie. W przeciwieństwie do modelu symbolicznego, model obliczeniowy jest bardziej realistyczny, ponieważ uwzględnia ograniczenia obliczeniowe atakujących oraz złożoność kryptograficznych prymitywów. Istotnym wnioskiem z tej różnicy jest to, że jeśli protokół jest bezpieczny w modelu obliczeniowym, to tym bardziej będzie bezpieczny w modelu symbolicznym. Implikacja w drugą stronę nie zawsze jest prawdziwa. Jednakże zaletą modelu symbolicznego w porównaniu z obliczeniowym jest łatwość sprawdzenia i formalnego dowodzenia własności protokołu. Dlatego, mimo mniejszego realizmu, wciąż jest on wykorzystywany. Skuteczny atak w modelu symbolicznym pozwala natychmiast odrzucić badany protokół, natomiast dowód bezpieczeństwa gwarantuje bezpieczeństwo strukturalne i pozwala skupić się na ocenie elementów składowych (algorytmach szyfrujących, hasłach, prymitywach kryptograficznych). Dzięki temu można oceniać protokół w sposób bardziej przejrzysty i uporządkowany.

Skupmy się teraz na modelu symbolicznym. Rozważmy przykład, w którym występują dwaj agenci – ponownie nazwijmy ich Alicją i Bobem. W tym przykładzie zakładamy, że wiedzą publiczną jest klucz publiczny `pk(skB)`, który jest powiązany z kluczem prywatnym Boba `skB` (klucz `skB` jest znany wyłącznie Bobowi).

Alicja chce przesłać do Boba wiadomość `m` i szyfruje ją przy użyciu klucza publicznego `pk(skB)`. Alicja może to zrobić, ponieważ zakładamy, że ten klucz jest dostępny publicznie, co umożliwia każdemu (w tym Alicji) zaszyfrowanie wiadomości przeznaczonej wyłącznie dla Boba. Zaszyfrowana wiadomość jest następnie przesyłana do Boba, który może ją odszyfrować dzięki swojemu kluczowi prywatnemu `skB`.

Omówiony protokół kryptograficzny można zapisać w ustrukturyzowany sposób, który przedstawiamy poniżej.

```
Wiedza:
    Publiczna: Alicja, Bob, pk(skB);
    Alicja: Alicja, Bob, m, pk(skB);
    Bob: Alicja, Bob, skB;
Akcje:
    Alicja -> Bob : { m } pk(skB).
```

Notacja ta jest znana w literaturze jako *notacja AnB* (skrót od *Alice and Bob*). Wyróżniamy w niej informację *początkową* każdego z agentów oraz to, jakie parametry są znane publicznie. Następnie wymieniamy kolejno wykonywane akcje w opisywanym protokole, zgodnie ze strukturą:

$$nadawca \to adresat : wiadomość.$$

Użyta w powyższym opisie składnia `{ m } pk(skB)` oznacza, że korzystając z szyfru asymetrycznego, wysyłamy wynik szyfrowania wiadomości `m` za pomocą klucza publicznego `pk(skB)`. Okazuje się, że taki protokół jest bezpieczny w modelu symbolicznym. Kłopot z nim polega jednak na tym, że zakłada on publiczną znajomość klucza `pk(skB)`. Co, jeśli to założenie nie byłoby spełnione? Prostym rozwiązaniem wydaje się przesłanie klucza `pk(skB)` przez Boba do Alicji. Ale Alicja najpierw musi w jakiś sposób zasygnalizować potrzebę komunikacji z Bobem. Może to na przykład zrobić, przesyłając do Boba swój identyfikator. Tak zmodyfikowany protokół, zapisany w notacji AnB, wygląda następująco.

```
Wiedza:
    Publiczna: Alicja, Bob;
    Alicja: Alicja, Bob, m;
    Bob: Alicja, Bob, skB;
Akcje:
    Alicja -> Bob : Alicja;
    Bob -> Alicja : pk(skB);
    Alicja -> Bob : { m } pk(skB).
```

Okazuje się, że ta prosta zmiana doprowadziła do fatalnych skutków. Zmodyfikowany protokół przestał być bezpieczny! Atakujący (nazwijmy go Oskarem, w skrócie `O`, zaś Alicję i Boba oznaczmy skrótowo jako `A` i `B`) może przechwycić wiadomość `A -> B : A`. W konsekwencji nie dotrze ona do Boba, za to Oskar będzie w stanie podszywać się pod Boba i wysłać Alicji swój własny klucz publiczny `pk(skO)` (dla którego będzie znał swój własny klucz prywatny). Alicja wyśle do Boba wiadomość `m` zaszyfrowaną kluczem publicznym `pk(skO)` (gdyż taki otrzymała), ale do Boba ta wiadomość nigdy nie dojdzie. Będzie tak dlatego, że Oskar ją przechwyci i odszyfruje kluczem prywatnym `skO`. Zwróćmy uwagę, że oba protokoły są bardzo podobne, a główna różnica między nimi polega na zmianie założenia, że `pk(skB)` nie jest znany na początku komunikacji jako parametr publiczny. Jak już zauważyliśmy, ta zmiana doprowadziła do utraty poufności wiadomości `m`. Zatem słabość tego protokołu nie ma nic wspólnego z siłą szyfrowania, a jedynie ze sposobem, w jaki się posługujemy szyfrowaniem.

Wróćmy jednak do pierwszego protokołu, przed modyfikacją. Okazuje się, że jeśli bezpieczeństwo naszego protokołu zdefiniujemy w inny sposób, to nie będzie on już wcale bezpieczny. Powiedzmy, że atakujący Oskar jest w stanie podejrzewać, jaka wiadomość może być zaszyfrowana. Dla przykładu może on myśleć, że Alicja donosi na niego do Boba, że jest

złośliwy. W tym celu Oskar może we własnym zakresie zaszyfrować wiadomość `Oskar Złośliwy` za pomocą klucza publicznego `pk(skB)` (zna on ten klucz, gdyż jest dostępny publicznie). Następnie bez trudu porówna swoją wiadomość z wiadomością przesyłaną przez Alicję do Boba. Jeśli będą one takie same, to znaczy, że zaszyfrowana wiadomość `m` to właśnie `Oskar Złośliwy`. O takim protokole powiemy wtedy, że nie posiada własności *słabej poufności* względem wiadomości `m`. Formalnie mówimy, że protokół ma taką własność względem pewnej wiadomości `abc`, jeśli jej wartość jest znana tylko osobom uprawnionym, zaś atakujący nie może nawet sprawdzić, czy wiadomość przyjmuje taką wartość, jaką podejrzewa. Nazwa ta może być dla niektórych myląca – i słusznie! Słaba poufność jest własnością silniejszą od zwykłej poufności (tajności) – protokół mający własność słabej poufności ma na pewno także własność poufności.

Oczywiście takich własności bezpieczeństwa, które możemy sprawdzać, jest o wiele więcej. Możemy też definiować je sami – w zależności od tego, do jakich celów chcemy taki protokół wykorzystać i co właściwie chcemy osiągnąć. Dla przykładu, jedną z takich własności jest *nierozróżnialność*. Upraszczając – jeżeli protokół posiada własność nierozróżnialności i wiemy, że tajna wiadomość może przyjąć jedną z dwóch wartości, to atakujący nie ma lepszej możliwości stwierdzenia, która wiadomość została wybrana, niż rzut monetą, czyli wybór losowy.

Sprawdzanie własności bezpieczeństwa protokołów kryptograficznych wydaje się zadaniem skomplikowanym. W związku z tym pojawia się naturalne pytanie – czy istnieją narzędzia komputerowe, których moglibyśmy użyć do sprawdzenia bezpieczeństwa protokołów kryptograficznych? Okazuje się, że tak! Jednym z takich narzędzi jest **Proverif** [2]. Program Bruno Blancheta jest przeznaczony właśnie do weryfikacji protokołów kryptograficznych w modelu symbolicznym. Jego działanie bazuje na zaprezentowaniu wejściowego protokołu za pomocą specjalnych formuł logicznych nazywanych *formułami Horna*. Formułą Horna o zmiennych logicznych nazwiemy każdą formułę logiczną, którą możemy zapisać w postaci alternatywy zmiennych logicznych z co najwyżej jedną niezanegowaną zmienną. Przykładami formuł Horna opartych na 3 zmiennych logicznych: x, y, z, są:

$$(\neg x) \vee y \vee (\neg z), \tag{1}$$

$$(\neg x) \vee (\neg z), \tag{2}$$

$$y. \tag{3}$$

Zauważmy, że każda z tych formuł może być zapisana równoważnie za pomocą następujących implikacji:

- formuła (1) jako $(x \wedge z) \Rightarrow y$,
- formuła (2) jako $(x \wedge z) \Rightarrow 0$,
- formuła (3) jako $1 \Rightarrow y$.

Innymi słowy, poprzednikiem implikacji jest zawsze koniunkcja niezanegowanych zmiennych logicznych (lub logiczna prawda, oznaczana jako 1), zaś następnikiem implikacji jest pojedyncza niezanegowana zmienna (lub logiczny fałsz, oznaczany jako 0). Dzięki tej interpretacji łatwiej jest zrozumieć wykorzystywanie tego konkretnego rodzaju formuł logicznych do modelowania protokołów kryptograficznych i własności bezpieczeństwa. Dla przykładu załóżmy, że atakujący chce poznać pewną wiadomość m. Niech $att(x)$ oznacza zmienną logiczną wyrażającą, że atakujący może poznać wiadomość x. Rozpatrzmy następującą formułę logiczną jako koniunkcję odpowiednich formuł Horna:

- $att(e)$ dla każdej wiadomości publicznej e oraz każdej wiadomości przesyłanej e,
- $att(f) \wedge att(x) \Rightarrow att(f(x))$ dla każdej funkcji f (co oznacza, że jeśli atakujący zna wartość x oraz funkcję f, to może poznać także wartość $f(x)$),
- $att(x) \Rightarrow att(\mathrm{resp}(x))$, gdzie $\mathrm{resp}(x)$ jest odpowiedzią dowolnego uczestnika protokołu na otrzymaną wiadomość x,
- $\neg att(m)$.

Jeśli atakujący może poznać wartość m, to z powyższej formuły będzie wynikać zależność $att(m) \wedge (\neg att(m))$, co prowadzi do sprzeczności.

Oprogramowanie Proverif może być trudne w obsłudze dla początkujących użytkowników, głównie ze względu na skomplikowany format wymaganych plików wejściowych. W rezultacie użytkownik musi opanować pełną składnię języka obsługiwanego przez to narzędzie. Aby złagodzić tę niedogodność, podjęliśmy badania w ramach projektu *Eksperymentalna platforma do automatycznej weryfikacji i walidacji algorytmów i protokołów kryptograficznych* (**EPW**), realizowanego przez Instytut Łączności (lider projektu), NASK oraz Politechnikę Warszawską [1]. Celem projektu było ułatwienie korzystania z narzędzi do formalnej analizy protokołów kryptograficznych, w tym Proverif.

Głównym wynikiem projektu EPW po stronie Wydziału Matematyki i Nauk Informacyjnych Politechniki Warszawskiej jest automatyczny program tłumaczący protokół zapisany w prostej, wspomnianej wcześniej, strukturze AnB do języka używanego przez Proverif. Dzięki temu program Proverif może stać się dużo bardziej dostępny i użyteczny nawet dla mniej zaawansowanych użytkowników.

Wszyscy autorzy tego artykułu prowadzą zajęcia na specjalności Matematyka w Cyberbezpieczeństwie na Wydziale Matematyki i Nauk Informacyjnych Politechniki Warszawskiej.

Literatura

[1] www.gov.pl/web/instytut-lacznosci/epw.

[2] Bruno Blanchet, "Modeling and verifying security protocols with the applied pi calculus and proverif", *Foundations and Trends® in Privacy and Security*, 1(1-2):1–135, 2016.

[3] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[4] Christof Paar and Jan Pelzl. *Understanding Cryptography – A Textbook for Students and Practitioners*. Springer, 2010.

takie jest życie

Dajmy wytchnąć dzikości

W czerwcu 2013 roku siedzę w podskakującym na wybojach minibusie, realizując marzenie z dzieciństwa: safari w Parku Narodowym Serengeti w Kenii. Nie wiem jeszcze, że kilka godzin później euforię zastąpi palące uczucie wstydu i chęć ucieczki.

Współtowarzysze podróży ustawiają i testują aparaty fotograficzne z wielkimi teleobiektywami. Dyskutują z kierowcą, który raz po raz porozumiewa się z kimś przez krótkofalówkę. Pędzimy, by osiągnąć daleki cel.

Co roku o tej porze do Serengeti ściągają tłumy: antylopy gnu z powodu suszy ruszają na południe w poszukiwaniu pożywienia. Po drodze muszą przepłynąć pełną krokodyli rzekę Mara. Gnu stosują strategię minimalizującą ryzyko utraty życia – wszystkie razem rzucają się w wodę na sygnał przewodnika stada, „zalewając" bród wielką liczbą osobników.

Widzę wzdłuż piaszczystych, stromych brzegów Mary dziesiątki minibusów, z których wystają obiektywy aparatów. Trwa wyścig, który z kierowców zajmie lepsze miejsce. Stado gnu stoi niedaleko krawędzi skarpy i szykuje się do skoku. Zwierzęta są zdenerwowane, podchodzą bliżej, cofają się i tłoczą, wzbudzając tumany kurzu. Próbują znaleźć najlepsze zejście do wody, jednak większość miejsc jest zablokowanych przez samochody. Obserwuję trzy próby ruszenia do przodu. W ostatniej chwili zatrzymują się spłoszone przez podjeżdżające jeszcze bliżej samochody. Wreszcie stado cofa się. Kolejną próbę zwierzęta podejmą następnego dnia. Zostają w miejscu, gdzie brak jest świeżego pokarmu.

Po opuszczeniu granic parku do wstydu, że biorę udział w takim spektaklu, dochodzi głębokie przygnębienie. Mijamy wyschnięte tereny, po których wiatr toczy plastikowe worki, torebki, butelki – niezbite dowody obecności człowieka...

Dzikie rejony Ziemi są stale zagrożone. Systematycznie znikają kolejne naturalne siedliska. Niestety dokłada się do tego masowa turystyka. Parki Narodowe nie są właściwie chronione przed dewastacją. Budowane bez kontroli bazy turystyczne wokół Serengeti zmniejszyły zasoby wody w Parku. Zwierzęta hodowlane konkurują o żywność i wodę z dzikimi, stawiane płoty uniemożliwiają swobodne migracje w trudnym klimacie. Katalogi turystyczne mówią o milionie gnu, tymczasem pogłowie tych antylop spadło z miliona w latach 70. XX wieku do mniej niż 250 000, a migracje przez Marę spadły z 26 800 osobników w 1978 roku do mniej niż 3000 w 2014. Populacja żyraf Serengeti zmniejszyła się o 95%, guźców o 80%. Coraz mniejsze są mioty wielkich kotów, gepardy będą niedługo zagrożone wyginięciem.

Według danych opublikowanych w PNAS w 2018 roku, jeśli wziąć pod uwagę biomasę wszystkich ssaków na Ziemi, 62% stanowią ssaki hodowlane, 34% ludzie, a jedynie pozostałe 4% to żyjące dziko zwierzęta. Człowiek opanował i przekształcił nadające się do życia rejony naszej planety, zastępując różnorodność gatunków i ekosystemów hodowanymi na własny użytek organizmami. „Obecnie ponad połowa nadających się do zamieszkania terenów zajęta jest przez uprawę i hodowlę, (...) prawie 80% terenów uprawnych służy hodowli i wykarmieniu zwierząt. Od lat 70. XX wieku straciliśmy 60% dzikich zwierząt, XX wiek pochłonął 90% dużych ryb oceanicznych, a 70% ptaków to drób (głównie kurczaki)" – pisze w swojej znakomitej książce „Natura natury. Dlaczego potrzebujemy dziczy" Enric Sala, hiszpański profesor oceanologii i ekologii, badacz różnorodności biologicznej i ekosystemów. Opisuje analizę wielu badań naukowych, która wykazuje, że aby Ziemia przetrwała w tej formie, jaką znamy, trzeba część jej obszarów chronić przed ingerencją człowieka. Byłyby one rezerwuarem zasobów, które są niezbędne dla przetrwania także nas, dwunożnych ssaków. Szacunki mówią, że w przypadku oceanów wystarczyłoby 35%, a na lądach chronić musielibyśmy około połowę powierzchni. Niestety jesteśmy daleko od tego: dane sprzed kilku lat mówią o 15% obszarów chronionych lądów i 7% powierzchni oceanów. Polska wypada tu nieźle: obszary chronione to blisko 40% lądu (z czego jedynie 0,5% to rezerwaty) i 22% wód morskich. Problemem jest także fakt, że największy odsetek naszych terenów chronionych (45%) ma powierzchnię mniejszą niż 1 km^2, a fragmentacja siedlisk ma zgubny wpływ na naturalne procesy.

Ogrom niekorzystnych zmian widzę, wracając po wielu latach w Tatry.

Chroniony obszar wysokich gór z ich unikatową fauną i florą stanowi 2,2% powierzchni Polski. Żyje w nim 27 gatunków endemicznych i kilkanaście zagrożonych wyginięciem. W 1993 roku granicę Tatrzańskiego Parku Narodowego przekroczyło blisko 1,6 mln turystów, w 2024 roku było to rekordowe 4,9 mln. Gdyby zjawili się w tym samym momencie, na 1 metr kwadratowy parku przypadłyby 23 osoby.

W surowym klimacie gór wszystkie formy życia rozwijają się znacznie dłużej niż na nizinach. Zniszczenie odbudowywane jest przez wiele lat. Każdy patyk pokryty porostami, kamień i martwy pień porośnięte mchami, krokus wystający spomiędzy brązowych po zimie traw, śpiewający drozd, przelatujący kruk, wyczekujący ofiary krogulec w porannej mgle, stado łani na hali, świerki, modrzewie, buki. Kamienie, strumyki, skały. To wszystko jest skarbem. Stawiając stopę na szlaku, dostępujemy zaszczytu bycia gościem w enklawie dziczy.

Wraca poczucie wstydu sprzed lat. W pierwszym odruchu zbieram na szlaku puszki, butelki, kapsle, opakowania po batonach, kolce z raczków. Z żalem słucham w górskim schronisku nocnych śpiewów rozweselonych jednym (czy więcej?) napojem tych, którzy zaopatrzeni w raki, kaski i czekany wyruszą rankiem na trasę. I płakać mi się chce, kiedy grupka roześmianych kobiet na szczycie Kasprowego uruchamia głośnik z „przyjemną muzyką do tak pięknych widoków".

Sala pisze: „Mamy (...) całkowitą pewność, że wszystko, co jest nam niezbędne do przeżycia – każdy kęs jedzenia, każdy haust powietrza, każdą kroplę czystej wody – zawdzięczamy innym gatunkom. Dostajemy od nich tak wiele, a czym się odpłacamy? Ignorancją, zniszczeniem i całkowitą eliminacją".

Wiosna wybuchła. Ruszamy szukać wytchnienia w naturze. A może zostawić ją w spokoju? Przywróćmy część tego, co utraciliśmy tu, w miejscu naszego bytowania, zostańmy w swoich wygodach i dajmy odpocząć wycieńczonej dzikości. Bo jeśli nie, to co będzie z nami?

Marta FIKUS-KRYŃSKA

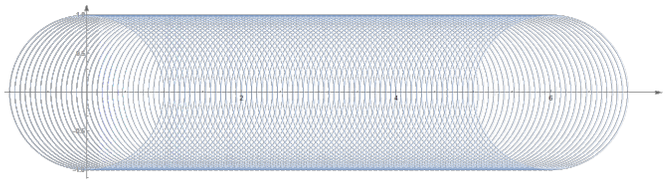
Artystyczne piękno osobliwych zbiorów

Iza DANIELEWSKA, Dawid POŁAWSKI, Michał ZWIERZYŃSKI

Wydział Matematyki i Nauk Informacyjnych, Politechnika Warszawska

Ilustracje zdobiące niniejszy artykuł to tzw. *kaustyki Wignera* oraz *zbiory środka symetrii* zamkniętej, gładkiej krzywej płaskiej. Od lat 70. XX wieku aż po dziś dzień obiekty te znajdują zastosowanie w rozmaitych dziedzinach, takich jak semiklasyczna fizyka kwantowa, teoria osobliwości czy geometria różniczkowa. Można je interpretować jako obwiednie (za moment wytłumaczymy, czym są) specjalnych rodzin prostych, co nadaje im nie tylko głębokie znaczenie geometryczne, lecz także wybitną wartość artystyczną, odzwierciedlającą piękno i harmonię matematyki.

Opiszmy najpierw pokrótce, czym jest wspomniana już obwiednia. *Obwiednią* rodziny krzywych nazywamy zbiór styczny do każdej z tych krzywych, którego każdy punkt stanowi punkt styczności do jednej z krzywych. Intuicyjnie można ją sobie wyobrazić tak, że każdy punkt obwiedni to punkt przecięcia dwóch „nieskończenie bliskich" krzywych z badanej rodziny. Na przykład, jeśli wyobrazimy sobie rodzinę okręgów o promieniu 1 i o środkach leżących na osi OX, obwiednią będą dwie proste: $y = 1$ oraz $y = -1$ (rys. 1).



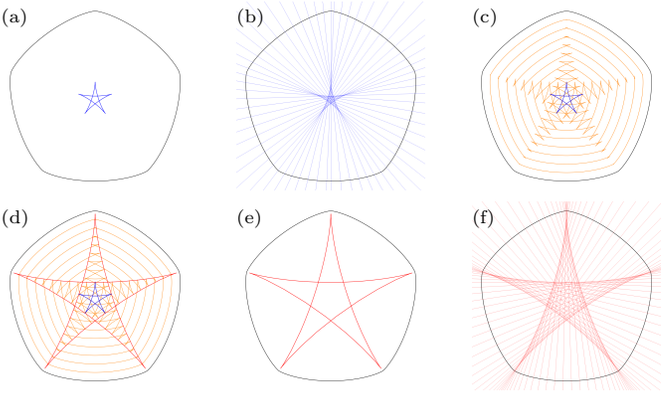
Rys. 1. Rodzina okręgów i ich obwiednia

Mając krzywą płaską γ, parę różnych punktów a, b leżących na tej krzywej nazywamy *parą równoległą*, jeśli styczne do tej krzywej w tych dwóch punktach są prostymi równoległymi (piszemy wtedy $a \| b$). Przykładowo, gdy γ jest okręgiem, to każda para punktów antypodycznych (czyli takich, które są końcami pewnej średnicy tego okręgu) jest parą równoległą.

Przystąpmy do definicji osobliwych zbiorów przytoczonych we wstępie artykułu. Ustalmy na początku krzywą płaską γ oraz liczbę rzeczywistą λ. *Zbiorem afinicznie λ-równoodległym* nazywamy zbiór

$$\mathrm{E}_\lambda(\gamma) := \{\lambda a + (1-\lambda)b \colon a, b \in \gamma, a \| b\}.$$

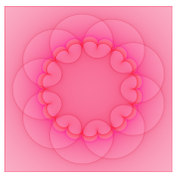
Innymi słowy (w przypadku $\lambda \in (0,1)$), gdy mamy odcinek o końcach w parze równoległej, to punkt dzielący ten odcinek w stosunku λ należy do $\mathrm{E}_\lambda(\gamma)$. *Kaustyką Wignera* krzywej γ nazywamy zbiór $\mathrm{E}_{0,5}(\gamma)$. Początek rozważań nad kaustyką Wignera zawdzięczamy sir Michaelowi Berremu oraz Nándorowi Balázsowi [1], którzy badali fazowo-przestrzenną reprezentację Wignera stanów kwantowych. Zbiór $\mathrm{E}_\lambda(\gamma)$ można również reprezentować jako obwiednię rodziny swoich stycznych (rys. 2(b)). Już za chwilkę zdefiniujemy ostatni zbiór, nazywany *zbiorem środka symetrii*, który po raz pierwszy, w trochę innych terminach geometrycznych, zdefiniował Stanisław Janeczko [3]. *Afiniczną cięciwą* krzywej γ nazywamy prostą przechodzącą przez parę równoległą krzywej γ. *Zbiór środka symetrii* jest obwiednią rodziny wszystkich cięciw afinicznych naszej początkowej krzywej (rys. 2(f)); będziemy go oznaczać $\mathrm{CSS}(\gamma)$. Okazuje się, że zbiór środka symetrii krzywej γ jest również zbiorem wszystkich punktów osobliwych (najczęściej ostrzy) rodziny wszystkich zbiorów afinicznie λ-równoodległych krzywej γ (rys. 2(c,d)).



Rys. 2. Osobliwe zbiory krzywej γ:
(a) Zbiór $\mathrm{E}_{0,5}(\gamma)$; (b) Zbiór $\mathrm{E}_{0,5}(\gamma)$ jako obwiednia prostych;
(c) Zbiory afinicznie λ-równoodległe krzywej γ; (d) Zbiory afinicznie λ-równoodległe krzywej γ oraz $\mathrm{CSS}(\gamma)$; (e) Zbiór $\mathrm{CSS}(\gamma)$; (f) $\mathrm{CSS}(\gamma)$ jako obwiednia cięciw afinicznych;

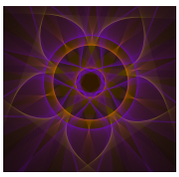
Zbiory omówione w niniejszym artykule charakteryzują się wieloma interesującymi własnościami geometrycznymi, których pełny opis wykracza poza ramy tego tekstu. Dziedziny nauki zajmujące się tymi strukturami dynamicznie się rozwijają, a na ich temat regularnie publikowane są nowe prace naukowe. Znaczna część wiedzy dotyczy lokalnych własności tych zbiorów w przestrzeniach n-wymiarowych. Natomiast w przypadku ich własności globalnych, takich jak liczba punktów osobliwych, obecny stan wiedzy pozwala na formułowanie precyzyjnych twierdzeń jedynie w odniesieniu do krzywych. Więcej na temat geometrycznych własności oraz literatury tego przedmiotu można przeczytać w [2].

Dzięki możliwości opisania rozważanych zbiorów za pomocą obwiedni rodziny prostych otwiera się przed nami przestrzeń do ich graficznej prezentacji. Autorzy niniejszego artykułu, wspólnie z Dominiką Sterczewską, wykorzystali oprogramowanie *Mathematica*, aby stworzyć artystyczne wizualizacje – różnorodne, niebanalne, otwarte na rozmaite interpretacje. Te niepowtarzalne i osobliwe obrazy stanowią wyjątkowe połączenie matematycznej precyzji i kreatywnego piękna. Refleksje o ich unikatowym charakterze można było usłyszeć wśród uczestników miniwystawy zorganizowanej z okazji obchodów XXV-lecia Wydziału Matematyki i Nauk Informacyjnych Politechniki Warszawskiej (28.11.2024 r.), za co autorzy są bardzo wdzięczni Organizatorom tego wydarzenia. Szczegółowy

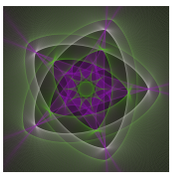


Hearts

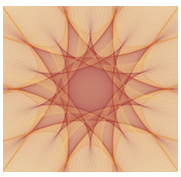
Pink Star



Lóth

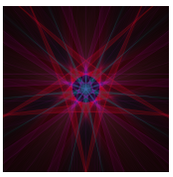


Big Purple Pentagramobile



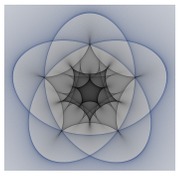
Charmander's Tail

The Beginning

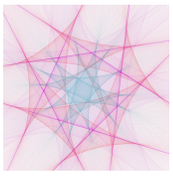


Pentaception

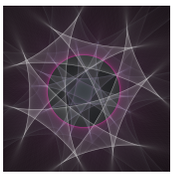
Pestilence



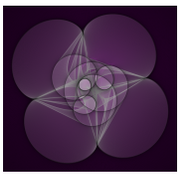
Singular MiNI



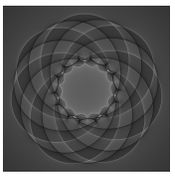
Chaos



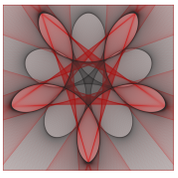
Shuriken



Singular Four-Leaf Clover



Black and White



Beast's Rosette

Literatura

[1] M.V. Berry, N.L. Balazs, *Evolution of Semiclassical Quantum States in Phase Space*, J. Phys. A Math. Gen. 12 (1979), 625–642

[2] I. Danielewska, D. Poławski, D. Sterczewska, M. Zwierzyński, *Artistic Aspects of the Wigner Caustic and the Centre Symmetry Set*, arXiv:2409.04443

[3] S. Janeczko, *Bifurcations of the Center of Symmetry*, Geom. Dedicata 60 (1996), 9–16

opis tworzenia wizualizacji, wraz z przykładowym kodem w programie *Mathematica*, znajduje się w [2]. Na rysunkach powyżej prezentujemy wybrane wizualizacje. Mamy szczerą i serdeczną nadzieję, że te obrazy przypadną do gustu Czytelnikom *Delty* i zainspirują ich do zgłębiania piękna osobliwej geometrii różniczkowej. Być może niektórzy z Państwa skorzystają z przykładowego kodu napisanego w programie *Mathematica*, zamieszczonego w [2], i sami podejmą próbę stworzenia własnych, niezwykłych wizualizacji tych tajemniczych geometrycznych zbiorów, odkrywając jednocześnie magię, jaką jest matematyka.

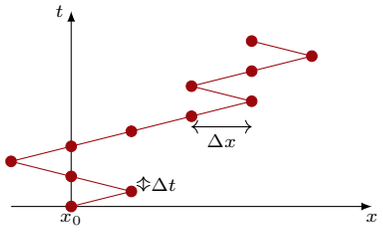
Zrozumieć dyfuzję

*Karolina PAWLAK**

* Wydział Matematyki i Nauk Informacyjnych, Politechnika Warszawska

Rys. 1

Ostatnio bardzo popularne stały się dyfuzory zapachowe, które potrafią otulić naszą domową przestrzeń przyjemnymi wonnościami i wprawić nas w dobry nastrój. Ale czy zastanawialiście się kiedyś, w jaki sposób dochodzi do rozprzestrzeniania się zapachów w pomieszczeniu? W przypadku dyfuzorów zapachowych nośnikiem zapachu są patyczki ratanowe, zanurzone w szklanym pojemniku wypełnionym olejkiem eterycznym (rys. 1). Dzięki porowatej strukturze patyczków ciecz jest wchłaniana i przenoszona aż do ich wierzchołków, gdzie olejek zaczyna odparowywać z powierzchni. Następnie cząsteczki substancji zapachowej ulegają niezliczonym zderzeniom z cząsteczkami powietrza. To je napędza i sprawia, że rozpraszają się po pomieszczeniu, a my cieszymy się pięknym aromatem. Opisane zjawisko przemieszczania się substancji z obszaru o wyższym jej stężeniu do obszaru o niższej koncentracji nazywamy **dyfuzją**.



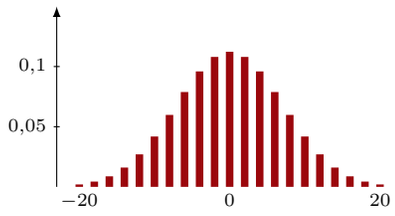
Rys. 2. Wykres prezentuje położenie cząsteczki (x) w zależności od czasu (t)

Sprawdźmy, jak rachunek prawdopodobieństwa może nam pomóc dokładniej opisać proces dyfuzji. Wyobraźmy sobie, że mamy cząsteczkę perfum w punkcie x_0, która porusza się wzdłuż osi OX i w czasie $\Delta t > 0$ przemieszcza się o $\Delta x > 0$ w prawo lub w lewo (rys. 2). Przyjmujemy, że prawdopodobieństwo pójścia w prawo/lewo w każdym kroku wynosi $\frac{1}{2}$. Jeśli n jest liczbą skoków, jakie wykonała cząsteczka, to $n = n_+ + n_-$, gdzie n_+ to liczba skoków w prawo, a n_- to liczba skoków w lewo. Ponadto $t = n\Delta t$ jest całkowitym czasem jej ruchu. Natomiast jeśli przez x oznaczymy przemieszczenie cząsteczki względem punktu x_0, to liczba $m = \frac{x}{\Delta x}$ wyraża wielkość przemieszczenia w punktach kratowych i oczywiście $m = n_+ - n_-$. Zatem liczby skoków w prawo/lewo możemy wyrazić wzorami:

$$n_- = \frac{n-m}{2}, \quad n_+ = \frac{n+m}{2}.$$

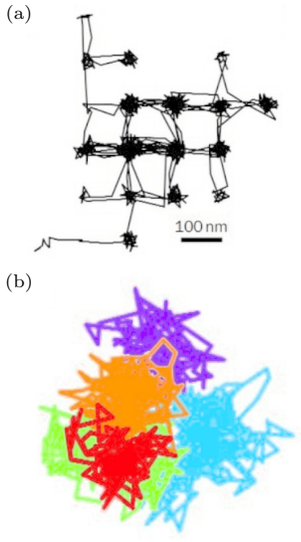
Chcemy obliczyć $P(m,n)$, czyli prawdopodobieństwo, że po n krokach cząsteczka przemieści się o m punktów kratowych względem położenia początkowego x_0. Przy każdym skoku mamy dwie równoprawdopodobne możliwości ruchu. Zatem wszystkich możliwych realizacji n kroków jest 2^n i każda ma takie samo prawdopodobieństwo zaistnienia. Aby po n krokach znaleźć się w pozycji m,

O błądzeniu losowym można przeczytać również w tekście Michała Miśkiewicza *Dyskretny wzór Itô* z Δ^{10}_{23}.

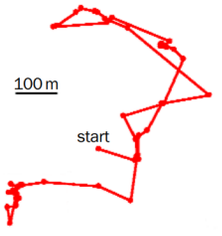


Rys. 3

Przedstawiona zależność może zostać wyprowadzona ze wzoru Stirlinga: $n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$.



Rys. 4. Na rysunku (b) kolorami wyróżniono fragmenty trajektorii przebyte w wybranych odcinkach czasu. Źródło: [1]



Rys. 5. Źródło: [1]

Literatura
[1] J. Klatfer, I.M Sokolov, *Anomalous diffusion spreads its wings*; physicsweb.org, 2005.
[2] A. Tokmakoff, Notatki do kursu *Concepts in Biophysical Chemistry*, prowadzonego na University of Chicago (*Brownian Motion*).

mamy $\binom{n}{n_+}$ możliwości. Zatem

$$P(m,n) = \left(\frac{1}{2}\right)^n \frac{n!}{n_+!n_-!} = \left(\frac{1}{2}\right)^n \frac{n!}{\left(\frac{n+m}{2}\right)!\left(\frac{n-m}{2}\right)!}.$$

Na rysunku 3 możemy zobaczyć, jakie jest prawdopodobieństwo, że przemieścimy się o m punktów kratowych po 50 krokach dla parzystych m spełniających $|m| \leqslant 20$. Widzimy, że najbardziej prawdopodobne jest przemieszczenie się o zero punktów kratowych. Analizując analogiczne wykresy dla większych wartości n, odnieślibyśmy wrażenie, że podlegają one pewnej stabilizacji. Istotnie, matematycznie ta obserwacja wyraża się w następującym stwierdzeniu:

$$P(m,n) \approx \sqrt{\frac{2}{\pi n}} e^{-\frac{m^2}{2n}} \quad \text{dla dużych } n \text{ i parzystych } m.$$

Wykorzystując informację, że $n = \frac{t}{\Delta t}$ i $m = \frac{x}{\Delta x}$, otrzymujemy dyskretną funkcję rozkładu prawdopodobieństwa:

$$P\left(\frac{x}{\Delta x}, \frac{t}{\Delta t}\right) \approx \tilde{P}(x,t) := \sqrt{\frac{(\Delta x)^2}{4\pi D t}} \exp\left\{-\frac{x^2}{4Dt}\right\}, \quad \text{gdzie } D = \frac{(\Delta x)^2}{2\Delta t}.$$

Wprowadzona wyżej funkcja $\tilde{P}(x,t)$ jest rozwiązaniem klasycznego równania dyfuzji:

$$\frac{\partial \tilde{P}}{\partial t} = \Delta x D \frac{\partial^2 \tilde{P}}{\partial x^2}.$$

Choć powyższe równanie jest często wykorzystywane w modelowaniu matematycznym, nie wszystkie zjawiska dyfuzji można opisać w ten sposób. Do tej pory zakładaliśmy, że przeskok cząsteczki odbywa się w równych odstępach czasu oraz cząsteczka pokonuje zawsze tę samą odległość. Ponadto kolejne skoki są od siebie niezależne. Co, gdy któreś z tych założeń nie zostanie spełnione? Wówczas mówimy, że mamy do czynienia z **dyfuzją anomalną**. Dzieje się tak na przykład wtedy, gdy cząsteczka zatrzymuje się na pewien czas, zanim przeskoczy dalej. W takiej sytuacji cząsteczki rozprzestrzeniają się wolniej, niż zakłada to klasyczny opis dyfuzji – i mówimy, że mamy do czynienia z **subdyfuzją**. Przyjrzyjmy się następującemu przykładowi takiej sytuacji.

Błona komórkowa oddziela wnętrze komórki od świata zewnętrznego oraz odpowiada za przekazywanie informacji ze środowiska do wnętrza komórki. Transport dyfuzyjny na błonie komórkowej pełni kluczowe funkcje w przekazywaniu sygnału i sposobie, w jaki komórki oddziałują ze swoim otoczeniem. Biorąc pod uwagę, że błona komórkowa jest płynna, można by oczekiwać, że cząsteczki białek będą szybko dyfundować przez błonę, tak aby odpowiednie reakcje mogły zachodzić jak najsprawniej. Nic bardziej mylnego.

Na początku 2005 roku na Uniwersytecie Nagoya w Japonii naukowcy przeprowadzili następujący eksperyment: śledzili pojedynczą cząsteczkę białka w błonie plazmatycznej żywych komórek. Obrazowanie wideo cząsteczek fluorescencyjnych ujawniło, że cząsteczki te spędzają stosunkowo długi czas uwięzione między przeszkodami o wielkości nanometrów w cytoszkielecie aktynowym komórki. Symulację trajektorii ruchu białka, które pokonuje przeszkodę o powierzchni 120 nm^2, utworzoną przez cytoszkielet komórki, możemy zobaczyć na rysunku 4a. Eksperymentalne trajektorie białek w błonie plazmatycznej żywej komórki widoczne są z kolei na obrazku 4b.

Anomalna dyfuzja pojawia się też wtedy, gdy cząsteczka przez dość długi czas nie zmienia kierunku, w którym się porusza. Wtedy cząsteczki rozprzestrzeniają się szybciej, niż przewiduje to klasyczna dyfuzja. Zjawisko takie nazywamy **superdyfuzją**. Na rysunku 5 przedstawiona została trajektoria ruchu małpki z rodzaju czepiaków w lesie na meksykańskim Półwyspie Jukatan. Jak widać, poszczególne skoki małpki są różnej długości. Taki proces dyfuzyjny zachodzi szybciej niż normalna dyfuzja – mamy do czynienia z superdyfuzją.

Subdyfuzja zachodzi również podczas przepływu elektronów w półprzewodnikach amorficznych w kserokopiarce. Z kolei za pomocą superdyfuzji można rozsądnie opisać trajektorię lotu albatrosów. Przykładów jest wiele, co prowadzi do jednego wniosku: **anomalna dyfuzja w naturze jest normalna**!

Klub 44 F

Termin nadsyłania rozwiązań: 31 VII 2025

Czołówka ligi zadaniowej **Klub 44 F**
po uwzględnieniu ocen rozwiązań zadań
784 ($WT = 2{,}6$), 785 ($WT = 3$)
z numeru 10/2024

Jacek Konieczny (Poznań)	40,87
Tomasz Wietecha (Tarnów)	17 – 40,40
Jan Zambrzycki (Białystok)	4 – 29,34
Andrzej Nowogrodzki (Chocianów)	3 – 27,49

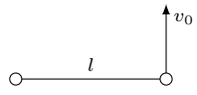
Zadania z fizyki nr 798, 799

Redaguje Elżbieta ZAWISTOWSKA

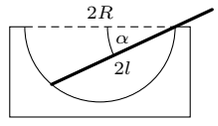
798. Dwie bardzo małe jednakowe kulki związane nieważką, nierozciągliwą nicią leżą na powierzchni poziomej (rys. 1). Jednej z kulek nadano prędkość v_0 skierowaną pionowo w górę. Jaka powinna być wartość tej prędkości, aby druga kulka nie oderwała się od poziomej powierzchni, a nić przez cały czas była naciągnięta? Po jakim torze porusza się wtedy pierwsza kulka? Tarcie kulki o podłoże jest zaniedbywalne.

799. Elektron krąży po orbicie kołowej w jednorodnym polu magnetycznym. Indukcja pola magnetycznego zostaje powoli zwiększona trzy razy, w czasie wielokrotnie przewyższającym okres obrotu. Ile razy zmieni się w tym czasie promień orbity elektronu?

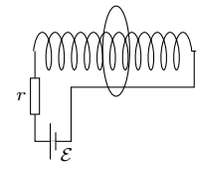
Rys. 1



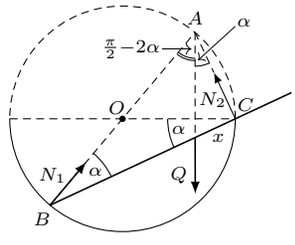
Rys. 2



Rys. 3



Rys. 4



Rozwiązania zadań z numeru 1/2025

Przypominamy treść zadań:

790. Jednorodny pręt o długości $2l$ opiera się na krawędzi nieruchomej, półkolistej czaszy o promieniu R (rys. 2). Jaki kąt α tworzy pręt z płaszczyzną poziomą w położeniu równowagi? Tarcie zaniedbujemy.

791. O jaką wielkość zmieni się natężenie prądu w kołowej pętli z nadprzewodnika, gdy nałożymy ją na długą zwojnicę podłączoną do baterii o sile elektromotorycznej $\mathcal{E}$ (rys. 3). Całkowity opór obwodu ze zwojnicą wynosi r, liczba zwojów N, współczynnik samoindukcji zwojnicy L_0, a pętli L. Indukcję wzajemną zaniedbujemy.

790. Na pręt działa siła ciężkości Q oraz siły reakcji N_1 i N_2 (rys. 4). Gdy nie ma tarcia, siła reakcji jest prostopadła do powierzchni, po której ślizga się punkt styczności. N_1 jest prostopadła do powierzchni czaszy, czyli działa wzdłuż promienia, N_2 jest prostopadła do pręta. W położeniu równowagi proste, wzdłuż których działają siły przyłożone do pręta, przecinają się w jednym punkcie, bo ich moment wypadkowy względem dowolnego punktu wynosi 0. Z rysunku 4:

$$(1)\quad |BC| = 2R\cos\alpha, \quad x = 2R\cos\alpha - l, \quad |OC| = R = x\cos\alpha + R\sin\left(\frac{\pi}{2} - 2\alpha\right),$$

stąd otrzymujemy równanie:

$$(2)\qquad 4R\cos^2\alpha - l\cos\alpha - 2R = 0.$$

Ponieważ kąt α leży w pierwszej ćwiartce, wybieramy dodatnie rozwiązanie równania (2):

$$(3)\qquad \cos\alpha = \frac{\left(l + \sqrt{l^2 + 32R^2}\right)}{8R}.$$

Z warunku $\cos\alpha \leqslant 1$ otrzymujemy warunek na maksymalną długość pręta $2l \leqslant 4R$. Minimalna długość pręta, dla której możliwa jest jeszcze opisana równowaga, odpowiada sytuacji, gdy pręt opiera się na krawędzi czaszy swoim prawym końcem. Wtedy $x = l$ i zgodnie z (1)

$$2R\cos\left(\alpha_{\max}\right) = 2l_{\min}.$$

Podstawiając do tego równania warunek równowagi (3), otrzymujemy

$$2l_{\min} = 2R\sqrt{2/3}.$$

Odpowiadająca tej minimalnej długości wartość graniczna kąta określona jest warunkiem

$$\cos\alpha_{\max} = \tfrac{l_{\min}}{R} = \sqrt{2/3}.$$

Podsumowując, opisany w zadaniu stan równowagi jest możliwy, gdy długość pręta spełnia warunek:

$$2R\sqrt{2/3} < 2l < 4R,$$

a kąt w stanie równowagi określa wzór (3).

Jeżeli $L = 2l > 4R$, to środek ciężkości pręta znajduje się poza krawędzią czaszy i pręt z niej wypada. Gdy pręt jest zbyt krótki, ześlizguje się do wnętrza czaszy.

791. Niech I_0 oraz I oznaczają początkowe i końcowe natężenie prądu w pętli. Natężenie prądu w zwojnicy nie zmienia się i wynosi $\frac{\mathcal{E}}{r}$, co daje strumień przez jeden zwój $\frac{L_0\mathcal{E}}{rN}$. Strumień ten przenika nadprzewodzącą pętlę nałożoną na zwojnicę. Całkowity strumień ϕ przez pętlę, zgodnie z prawem Faradaya, spełnia równanie $0 = -\frac{d\phi}{dt}$, gdzie w lewej części mamy spadek napięcia na zerowym oporze nadprzewodnika. Zatem całkowity strumień pola magnetycznego przez pętlę pozostaje stały: $\phi = LI_0 = \text{const}$. Przy zmianie zewnętrznego pola magnetycznego w pętli pojawia się prąd indukcyjny, którego pole magnetyczne kompensuje zmianę strumienia pola magnetycznego. Zatem

$$LI \pm \frac{L_0\mathcal{E}}{rN} = LI_0, \quad \text{albo} \quad I_0 - I = \pm\frac{L_0\mathcal{E}}{LrN}.$$

Dwuznaczność we wzorze związana jest z dwiema możliwościami wzajemnej orientacji pól magnetycznych zwojnicy i pętli. Jednakowej orientacji odpowiada znak $+$, przeciwnej znak $-$. W pierwszym przypadku prąd w pętli maleje, w drugim rośnie.

Klub 44 M

$\otimes\sqrt{\oint}!=44$

Termin nadsyłania rozwiązań: 31 VII 2025

Czołówka ligi zadaniowej **Klub 44 M** po uwzględnieniu ocen rozwiązań zadań 887 ($WT = 1{,}69$) i 888 ($WT = 1{,}64$) z numeru 10/2024

Mikołaj Pater		46,28
Witold Bednarek	Łódź	45,33
Tomasz Wietecha	Tarnów	45,31
Krzysztof Zygan	Lubin	42,03
Andrzej Kurach	Ryjewo	38,67
Andrzej Daniluk	Warszawa	37,89
Michał Warmuz	Żywiec	36,54
Marcin Kasperski	Warszawa	35,64
Grzegorz Wiączkowski		34,61
Krzysztof Kamiński	Pabianice	33,54
Janusz Olszewski	Warszawa	33,10
Jędrzej Biedrzycki		32,29
Marian Łupieżowiec	Gliwice	31,29

Klubowym nowicjuszem nie jest żaden z trzech Panów; Weteranem – każdy z nich; niektórzy z imponującym stażem. Magiczną linię 44 p. przekraczają: pan Mikołaj Pater – po raz czwarty; pan Witold Bednarek – po raz dziesiąty; pan Tomasz Wietecha – po raz piętnasty!

Zadania z matematyki nr 901, 902

Redaguje Marcin E. KUCZMA

901. Trapez równoramienny $ABCD$ jest wpisany w okrąg Ω o średnicy AB. Przekątne trapezu, długości d, przecinają się w punkcie P. Okrąg styczny do odcinków PC, PD i do krótkiego łuku CD (okręgu Ω) ma promień r. Okrąg wpisany w trójkąt ABP ma promień $3r$. Obliczyć stosunek r/d.

902. Dla liczby naturalnej n niech $w(n)$ oznacza największy całkowity wykładnik, dla którego $n!$ dzieli się przez $10^{w(n)}$, i niech $f(n) = 10^{-w(n)}n!$. Udowodnić, że dla każdej liczby naturalnej m spełniona jest zależność $f(5^m) \equiv 2^m \pmod 5$.

Zadanie 902 zaproponował pan Cezary Głowacz z Bonn.

Rozwiązania zadań z numeru 1/2025

Przypominamy treść zadań:

893. Punkty A, B, C, D, E leżą w tym porządku na linii prostej, przy czym $CA = CE$, $CB = CD$. Poza tą prostą, po jednej jej stronie, leżą punkty K i L takie, że trójkąty AKB i DLE mają ostre kąty przy wierzchołkach A, B i D, E, a suma miar tych czterech ostrych kątów wynosi 180°. Proste KB i LD przecinają się w punkcie N; proste AK i EL przecinają się w punkcie M; punkty M, N leżą po różnych stronach prostej KL, a ponadto $MN \perp AE$. Dowieść, że $CK = CL$.

894. Wyznaczyć wszystkie trójki liczb całkowitych (x, y, z) spełniające równanie

$$\frac{x + y + xyz}{yz + 1} = \frac{2025}{44}.$$

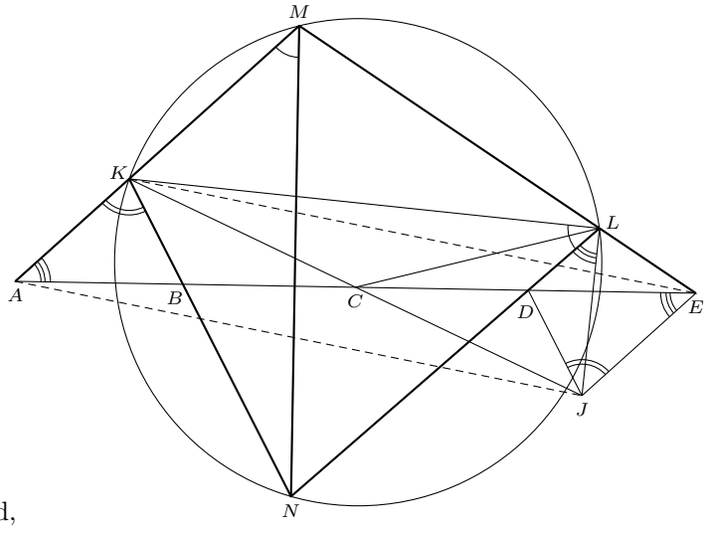
893. Rachunek kątów w trójkątach AKB i DLE pokazuje, że

$$\sphericalangle AKB + \sphericalangle DLE = 180^\circ. \tag{1}$$

Stąd wniosek, że czworokąt $KMLN$ ma okrąg opisany, wobec czego

$$\sphericalangle NLK = \sphericalangle NMK. \tag{2}$$

Przyjmijmy (b.s.o.), że punkt L leży bliżej prostej AE niż punkt K. Konfiguracja punktów i kątów jest wówczas jak na rysunku.



Uzupełniamy trójkąt AKE do równoległoboku $AKEJ$; punkt C jest jego środkiem symetrii. Trójkąty AKB i EJD są symetryczne względem C. Zatem $\sphericalangle AKB = \sphericalangle EJD$. Stąd, wobec (1), $\sphericalangle EJD + \sphericalangle DLE = 180^\circ$, co oznacza, że także czworokąt $JDLE$ ma okrąg opisany. Dostajemy równość

$$\sphericalangle JLD = \sphericalangle JED = \sphericalangle KAB. \tag{3}$$

Dodajemy (2) i (3) (uwzględniając, że $\sphericalangle NLK + \sphericalangle JLD = \sphericalangle JLK$):

$$\sphericalangle JLK = \sphericalangle NMK + \sphericalangle KAB.$$

Suma po prawej stronie wynosi 90° (dzięki założeniu $MN \perp AE$). Tak więc trójkąt JLK jest prostokątny. Punkt C jest środkiem przeciwprostokątnej JK. Stąd, ostatecznie, $CK = CL$.

894. Oznaczmy: $w = yz + 1$ (jest to liczba względnie pierwsza z y). Zadaną równość przepisujemy tak:

$$\frac{xw + y}{w} = \frac{2025}{44}.$$

To równość dwóch nieskracalnych ułamków. Muszą mieć równe liczniki i mianowniki, ewentualnie ze znakiem zmienionym na przeciwny. Więc na pewno $w = \pm 44$. Stąd $yz = w - 1 \in \{43, -45\}$, wobec czego $|y| \leqslant 45$, $|z| \leqslant 45$.

Przyrównanie liczników: $xw + y = \pm 2025$. Pamiętając, że $w = \pm 44$, mamy

$$y = \pm 2025 \mp 44x \equiv \pm 1 \pmod{44}.$$

To zawęża poszukiwanie do następujących par (w, y): $(44, 1), (44, -1), (44, 43), (44, -43), (-44, 1), (-44, -1), (-44, 45), (-44, -45)$. Z wyjściowego równania mamy

$$x = \frac{2025}{44} - \frac{y}{w}.$$

Z wypisanych ośmiu par (w, y) jedynie pierwsza, czwarta, szósta, ósma dają (przy użyciu ostatniego wzoru) całkowite wartości x: odpowiednio $46, 47, 46, 45$. Wartość $z = (w - 1)/y$ wynosi, odpowiednio, $43, -1, 45, 1$.

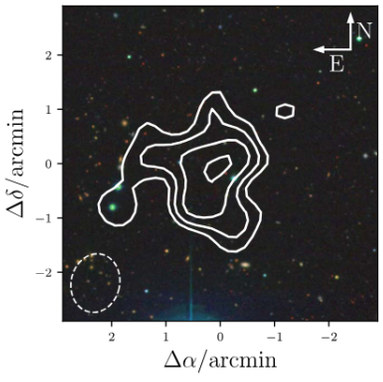
Badane równanie może więc być spełnione jedynie przez cztery trójki (x, y, z) – i faktycznie jest spełnione, co łatwo sprawdzić wprost:

$$(46, 1, 43),\ (47, -43, -1),\ (46, -1, 45),\ (45, -45, 1).$$

Regulamin Ligi znajduje się na naszej stronie: www.deltami.edu.pl/klub-44/regulamin/

Astronomia to pod wieloma względami badanie światła – w każdej długości fali – docierającego do nas z pobliskich gwiazd i odległych galaktyk. Jednak według standardowego modelu kosmologicznego (najlepszej teorii opisującej Wszechświat) większość masy w naszym Wszechświecie to ciemna materia, czyli materiał, który nie emituje ani nie odbija światła. Jak więc mamy jej szukać? Cóż, ta sama teoria przewiduje, że ciemna materia tworzy tzw. *halo ciemnej materii*, czyli regiony grawitacyjnie związanej materii. W ogólności, jeżeli takie zagęszczenia są duże, to znajdują się w nich galaktyki, a nawet całe gromady galaktyk – wtedy stosunkowo łatwo* jest sprawdzić, gdzie ciemna materia się znajduje. Jednak mogą też istnieć małe (oczywiście w porównaniu do tych wcześniejszych) zagęszczenia ciemnej materii, w których nie ma nawet gwiazd. Wtedy po prostu nie wiemy o ich istnieniu. Są to tzw. *ciemne halo*. Nie wszystko jednak stracone, w takich małych zagęszczeniach ciemnej materii może znajdować się zimny gaz (głównie wodór). Ten zimny gaz sam z siebie nie *świeci*, ale może odbijać światło w zakresie fal radiowych. Więc bingo, mamy plan obserwacji. Poszukajmy ciemnych halo, zwanych Obłokami Neutralnego Wodoru o Ograniczonej Jonizacji (RELHIC).

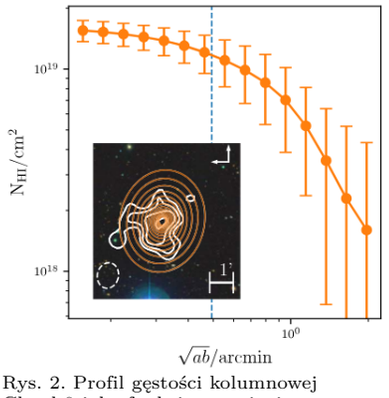
*„Łatwo” tzn. trzeba zaobserwować miliony galaktyk, opisać ich rozkład, dodać teorię opisującą rozkład ciemnej materii i spróbować je jakoś ze sobą połączyć. Można też zrobić kosmologiczne symulacje komputerowe.



Rys. 1. Izokontury gęstości kolumnowej wodoru HI nałożone na zdjęcie optyczne obserwowanego obszaru nieba

Naukowcy z Włoch i Kanady przyjrzeli się w szczególności jednemu obłokowi zimnego gazu – Cloud-9. Obłok ten został odkryty w 2023 roku, kiedy zespół astronomów zauważył nadmiar gazu neutralnego wodoru (HI) w pobliżu galaktyki spiralnej M94. Odkrycia dokonano za pomocą radioteleskopu FAST, który nie ma najlepszej rozdzielczości. Dlatego teraz postanowiono ponownie przyjrzeć się Cloud-9, tym razem z wykorzystaniem większego radioteleskopu VLA (Very Large Array).

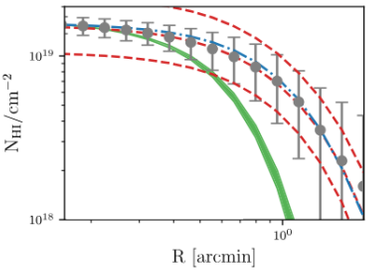
Okazało się, że Cloud-9 ma dość dziwny kształt. Prawdopodobnie spowodowany oddziaływaniami grawitacyjnymi z większą pobliską galaktyką M94, zgniatającymi lub rozciągającymi chmurę gazu (rys. 1).



Rys. 2. Profil gęstości kolumnowej Cloud-9 jako funkcja promienia efektywnego R_{eff}

Ale czy jest tam ciemna materia?

Aby to ustalić, musimy porównać kolumnowy rozkład gęstości masy, który obserwujemy (rys. 2), z teoretycznym rozkładem, jaki dawałaby ciemna materia i wodór. Musimy niestety założyć, że poza tymi dwoma składnikami w obłoku nie ma niczego innego (co nie musi być prawdą). Oczywiście nie w pełni rozumiemy, czym jest ciemna materia, wiemy jednak, że oddziałuje grawitacyjnie ze zwykłą materią, i potrafimy przewidzieć, jak te dwa składniki wpłynęłyby na kształt i rozkład gęstości w obłoku.



Rys. 3. Kolumnowy profil gęstości Cloud-9 (szare punkty) oraz przewidywania modelu (zielona linia) niestety się nie zgadzają

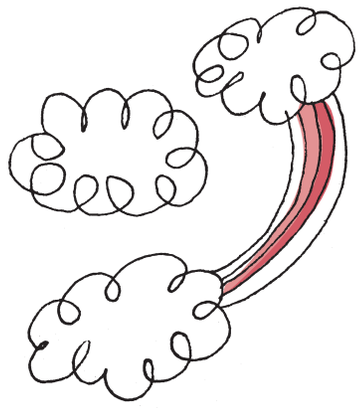
Niestety model (zielona linia na rys. 3) nie zgadza się z obserwacjami (szare punkty na rys. 3) i nie możemy na chwilę obecną definitywnie stwierdzić, czy Cloud-9 jest lub nie jest *ciemnym halo*. Jest jednak kilka rzeczy, które astronomowie mogą zrobić. Po pierwsze, teoretycy mogą przeprowadzić dokładniejsze symulacje rozkładu masy w *ciemnych halo*. Z kolei obserwatorzy mogą zrobić lepsze obserwacje, ponieważ jest szansa, że w Cloud-9 są gwiazdy, tylko zbyt słabe, abyśmy mogli je wcześniej zaobserwować. Na przykład w pobliżu Drogi Mlecznej znajduje się wiele bardzo słabych galaktyk karłowatych, które są małe i emitują bardzo mało światła. Dopiero w ciągu ostatnich kilku lat opracowaliśmy teleskopy, które mogą je obserwować. Cloud-9 może być taką galaktyką karłowatą.

Prawdopodobnie więc będziemy musieli trochę poczekać na ostateczną odpowiedź na temat natury Cloud-9, ale tak czy inaczej naukowcy są podekscytowani. Albo jest to pierwsze bezgwiezdne halo ciemnej materii, albo jest to najdalsza ultra słaba galaktyka karłowata, jaką kiedykolwiek wykryto! Dlatego zdecydowanie warto mieć ją na oku.

Anna DURKALEC

Zakład Astrofizyki, Departament Badań Podstawowych, Narodowe Centrum Badań Jądrowych

Na podstawie: Alejandro Benítez-Llambay, Rajeshwari Dutta, Michele Fumagalli, and Julio F. Navarro et al. 2024, „Examining the Nature of the Starless Dark Matter Halo Candidate Cloud-9 with Very Large Array Observations”, ApJ, 973 61.



W maju Słońce kończy szybką wędrówkę na północ. 20 dnia miesiąca przekroczy ono równoleżnik $+20°$ deklinacji w drodze na północ, i od tego momentu do przesilenia letniego w czerwcu zwiększy wysokość górowania jedynie o 3,5°. W drugiej części miesiąca Słońce chowa się na tyle płytko pod horyzont, że pojawia się zjawisko tzw. białych nocy astronomicznych, czyli niebo nie ciemnieje do końca i słabsze obiekty trudniej dostrzec.

Również pod koniec maja zaczyna się trwający niecałe 2,5 miesiąca sezon na dwa zjawiska atmosferyczne: obłoki srebrzyste i łuk okołohoryzontalny. Pierwsze z nich to zawieszone wysoko w atmosferze chmury, które są oświetlone przez światło słoneczne nawet w nocy. Drugie natomiast to mała, lecz intensywna tęcza kilkanaście stopni nad południową częścią nieboskłonu. Niestety, żeby mogła się ona pojawić, Słońce musi przebywać co najmniej 58° ponad horyzontem, co oznacza, że szansa na to zjawisko jest u nas tylko w godzinach okołopołudniowych.

Na początku miesiąca warto spoglądać w niebo zarówno wieczorem, jak i rano. Na niebie wieczornym ekliptyka tworzy wciąż całkiem duży kąt z widnokręgiem, jednak w drugiej części miesiąca zaczyna się on zmniejszać. W tej części sfery niebieskiej znajdują się dwie jasne planety Układu Słonecznego: Jowisz i Mars. Obie planety jednak najlepsze okresy widoczności mają już niestety za sobą. Jowisz dąży do czerwcowej koniunkcji ze Słońcem, stąd można go obserwować jedynie w pierwszej połowie miesiąca, i to na niezbyt ciemnym niebie. Początkowo planeta około godziny 22 zajmuje pozycję na wysokości niewiele ponad 10°, ale szybko zbliży się do widnokręgu i zginie w zorzy wieczornej. W tym czasie jej jasność wynosi -2^m, a średnica tarczy $34''$. Do końca okresu widoczności Jowisz przetnie linię łączącą gwiazdy El Nath i ζ Tau, stanowiące rogi tego zodiakalnego zwierzęcia. 1 maja do odszukania Jowisza można wykorzystać Księżyc w fazie 22%, który znajdzie się w odległości 16° na godzinie 11 względem planety. Księżyc odwiedzi Jowisza również 28 maja, gdy w fazie 4% zawiśnie 5° nad planetą.

Czerwona Planeta w maju pokona 15° na tle gwiazdozbioru Raka, ale pod koniec miesiąca przejdzie do Lwa. Mars zacznie miesiąc 0,5° na północny zachód od gwiazdy η Cnc, stanowiącej północno-zachodni róg trapezu otaczającego jasną gromadę otwartą gwiazd M44. Do samej gromady Mars zbliży się 4 maja, gdy przejdzie niewiele ponad 0,5° na północ od jej środka. Dzień wcześniej 2,5° od Marsa pokaże się Księżyc w fazie 42%. W tym czasie jasność Czerwonej Planety spadnie z $+1$ do $+1{,}3^m$, ale jej tarcza nie zmaleje już dużo, zmieni średnicę z $6''$ do $5''$.

Na niebie porannym, jak co roku, promieniują meteory z roju η-Akwarydów. Są to bardzo szybkie meteory, ich prędkość zderzenia z atmosferą Ziemi wynosi 66 km/s, a promieniują od 19 kwietnia do 28 maja, z maksimum aktywności około 6 maja. Radiant roju znajduje się niecałe 2° na południowy wschód od gwiazdy η Aqr i wschodzi dopiero po godzinie 2, by nieco ponad godzinę później osiągnąć wysokość 10° nad wschodnim widnokręgiem. Niskie położenie radiantu skutkuje tym, że u nas da się dostrzec zaledwie kilka do kilkunastu z prognozowanych ponad 50 zjawisk na godzinę. Warto jednak wybrać się na ich obserwacje, gdyż są one bardzo jasne i często pozostawiają widoczne przez dłuższy czas smugi. A znajdujący się na niebie wieczornym Księżyc nie przeszkodzi w obserwacjach.

2 maja przez opozycję względem Słońca przejdzie planetoida (4) Westa. Jest to najjaśniejsza planetoida na naszym niebie, ale ze względu na dość znaczną eliptyczność jej orbity w różnych latach osiąga ona różne zbliżenie do naszej planety, a co za tym idzie – różną jasność. W tym roku opozycja Westy należy do tych korzystniejszych, dlatego na przełomie kwietnia i maja planetoida osiągnie jasność $+5{,}7^m$, czyli porównywalnie do Urana. A zatem na ciemnym niebie można ją dostrzec gołym okiem, ale na pewno w jej odszukaniu wśród gwiazd tła pomoże lornetka albo inny sprzęt optyczny. Westa w maju pokona na niebie około 6,5° na pograniczu gwiazdozbiorów Wagi i Panny, przechodząc od pozycji jakieś 1,5° na zachód od gwiazdy 4. wielkości 16 Lib do około 3,5° na północny wschód od ι Vir. Westa góruje około północy na wysokości przekraczającej 35° nad widnokręgiem.

Wracając do Księżyca: 4 maja przejdzie on przez I kwadrę, a dobę później zbliży się na 1° do Regulusa, najjaśniejszej gwiazdy Lwa. W nocy z 9 na 10 maja jego tarcza zwiększy fazę do 93% i dotrze on w okolice Spiki, najjaśniejszej gwiazdy Panny, zbliżając się doń na 4°. 12 maja Srebrny Glob przejdzie przez pełnię w Wadze, zaś dwa dni później dotrze do gwiazdozbioru Skorpiona, zbliżając się do Antaresa na odległość 2°.

Po pełni Srebrny Glob jest widoczny słabo ze względu na niskie nachylenie ekliptyki do widnokręgu. 20 maja przejdzie on przez ostatnią kwadrę, a 24 maja spotka się z Wenus, zmniejszając wtedy fazę do 13%. Niestety oba ciała pokażą się około 5° nad horyzontem, mimo że planeta 1 czerwca osiągnie maksymalną elongację zachodnią, przekraczającą 46°. W opisywanym momencie jej tarcza świeci blaskiem $-4{,}4^m$, przy średnicy około $26''$ i fazie 45%.

Ariel MAJCHER

Rozwiązania zadań ze strony 7

Rozwiązanie zadania F 1119.
Powietrze jest mieszaniną gazów dwuatomowych: azotu (N_2) i tlenu (O_2). W podanych warunkach oba gazy doskonale spełniają równania gazu doskonałego. Ciśnienie p w kontenerze jest sumą ich ciśnień cząstkowych, a więc spełnione jest równanie:

$$p_0 V = nRT_0,$$

w którym n oznacza sumaryczną liczbę moli azotu i tlenu. Oba gazy mają takie samo molowe ciepło właściwe w przemianie w stałej objętości: $c_V = \frac{5}{2}R$. Podniesienie temperatury gazów w kontenerze do $T = 293$ K wymaga więc dostarczenia ciepła Q równego:

$$Q = nc_V(T - T_0) = \frac{5p_0V(T - T_0)}{2T_0}.$$

Liczbowo: $Q = 185$ kJ.

Rozwiązanie zadania F 1120.
Woda jest cieczą nieściśliwą, wobec tego prędkość opadania powierzhni wody $v(h)$ i prędkość jej wypływu dolnym otworkiem $v(0)$ związane są warunkiem wynikającym z prawa zachowania masy wody:

$$\pi R^2 v(h) = \pi r^2 v(0).$$

W opisanych warunkach możemy z dobrym przybliżeniem pominąć wpływ lepkości wody i posłużyć się równaniem Bernoulliego:

$$\frac{v(h)^2}{2} + gh + \frac{p(h)}{\rho} = \frac{v(0)^2}{2} + \frac{p(0)}{\rho}.$$

Przyjęliśmy, że h oznacza wysokość nad środkiem otworka, a ρ jest gęstością wody (stałą w całym naczyniu), a $p(h)$ i $p(0)$ oznaczają ciśnienie na zewnątrz naczynia na wysokości h i na poziomie otworka. Podstawiamy związek $v(h)$ i $v := v(0)$ wynikający z równania ciągłości do równania Bernoulliego i otrzymujemy:

$$\frac{p(h) - p(0)}{\rho} + gh = \frac{1}{2}v^2\left(1 - \frac{r^4}{R^4}\right).$$

Ostatecznie otrzymujemy odpowiedź:

$$v = \sqrt{\frac{2((p(h) - p(0))/\rho + gh)}{1 - r^4/R^4}}.$$

Zwykle różnica ciśnień atmosferycznych na wysokości h jest zaniedbywalnie mała, i można ją pominąć. Stosunek czwartych potęg promieni też zwykle jest bardzo mały, i można go pominąć. Oba te przybliżenia prowadzą do znanego wzoru Torricellego: $v = \sqrt{2gh}$.

Uwaga: otrzymany wzór opisuje prędkość wypływu w środku otworka. W rzeczywistości prędkości wypływu zbiegają się nieco w kierunku środka otworka, co powoduje zmniejszenie strumienia wypływającej wody w stosunku do wartości $\pi r^2 v$ o czynnik $\alpha < 1$ zależny od kształtu otworka – i dla otworka kołowego ten czynnik wynosi $\alpha \approx 0{,}62$, co należałoby uwzględnić w równaniu ciągłości.

Rozwiązanie zadania M 1816.
Odpowiedź: Tak.
Wielomian

$$P(x) = (1 - x)^{2026} - x^{2026} + \frac{1}{2}$$

spełnia warunki zadania.

Rozwiązanie zadania M 1817.
Udowodnimy przez indukcję, że istnieje dokładnie 3^n liczb n-cyfrowych podzielnych przez 2^n, których cyfry należą do zbioru $\{2, 3, 4, 5, 6, 7\}$.

Dla $n = 1$ teza jest jasna, w zbiorze $\{2, 3, 4, 5, 6, 7\}$ są tylko trzy liczby parzyste.

Załóżmy, że teza jest spełniona dla n. Liczbę spełniającą założenia stwierdzenia nazwijmy *dobrą*. Rozważmy $(n + 1)$-cyfrową liczbę dobrą i usuńmy jej pierwszą cyfrę. Otrzymana liczba n-cyfrowa jest również dobra, gdyż operacja usunięcia pierwszej cyfry x jest równoważna odjęciu liczby $x \cdot 10^n$, która jest podzielna przez 2^n.

Z drugiej strony, dopisując z lewej strony cyfrę x do dobrej liczby n-cyfrowej $y \cdot 2^n$, dostajemy liczbę

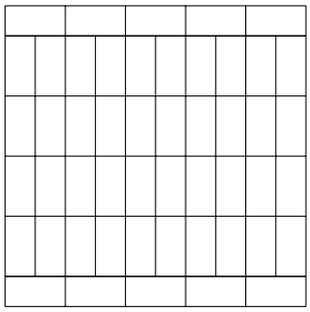
$$y \cdot 2^n + x \cdot 10^n = 2^n(y + x \cdot 5^n).$$

Uzyskana liczba jest $(n + 1)$-cyfrową liczbą podzielną przez 2^n, której cyfry należą do zbioru $\{2, 3, 4, 5, 6, 7\}$ i która jest podzielna przez 2^{n+1} wtedy i tylko wtedy, gdy $x + y$ jest parzyste. Zauważmy jednak, że dla parzystej liczby y jako x możemy przyjąć jedynie 2, 4 lub 6, a dla nieparzystego y jedynie 3, 5 lub 7. Oznacza to, że dobrych liczb $(n + 1)$-cyfrowych jest dokładnie 3 razy więcej niż dobrych liczb n-cyfrowych.

Rozwiązanie zadania M 1818.
Odpowiedź: 10.
Rozważmy kwadraty A_1, A_3, …, A_9 o wymiarach, odpowiednio, 1×1, 3×3, …, 9×9, których lewy dolny róg pokrywa się z lewym dolnym rogiem planszy. Dla każdego z kwadratów A_i $(i = 1, 3, 5, \ldots, 9)$ istnieje kostka domina X_i przecinająca jego bok (ponieważ kwadraty o nieparzystym wymiarze nie mogą zostać wypełnione kostkami domina). Łatwo zauważyć, że X_i leży wówczas wewnątrz kwadratu 2×2 z podziału. Dostaliśmy zatem 5 kostek domina wewnątrz kwadratów 2×2.

Podobnie, biorąc pod uwagę kwadraty B_1, B_3, …, B_9 o wymiarach 1×1, 3×3, …, 9×9, których prawy górny róg pokrywa się z prawym górnym rogiem planszy, znajdujemy kolejnych 5 kostek domina Y_j $(j = 1, 3, 5, \ldots, 9)$ o żądanej własności. Wobec tego najmniejsza możliwa liczba kostek domina spełniających warunki zadania jest nie mniejsza niż 10.

Następujący rysunek pokazuje, że liczbę 10 kostek domina jesteśmy w stanie zrealizować.



Zachłanność czasem popłaca

Bartłomiej BZDĘGA Uniwersytet im. A. Mickiewicza w Poznaniu

Algorytm zachłanny to taki, który dokonuje wyborów, jakie w aktualnej chwili (*lokalnie*) wydają się najlepsze, natomiast nie jest jasne, czy są one słuszne w sensie *globalnym*, gdy szukamy rozwiązania optymalnego. Choć nie jest to regułą, to niektóre algorytmy zachłanne dają optymalne rozwiązania, i o tym będzie w tym kąciku.

Przykład 1. Mamy banknoty o nominałach 10^k, $2\cdot 10^k$ i $5\cdot 10^k$ *pengő* dla $k = 0, 1, 2, \ldots$ Chcemy wypłacić nimi n *pengő* dla pewnej liczby naturalnej n. Robimy to w ten sposób, że za każdym razem, gdy zostało jeszcze do wypłacenia m *pengő*, wybieramy banknot z największym nominałem nieprzekraczającym m.

Przykład 2. Chcemy dojechać z miasta A do miasta B. Nawigacja prowadzi nas według następującej reguły: udaj się do miasta najbliższego aktualnej pozycji, spośród tych, w których jeszcze nie byłeś.

Pozostawiam Czytelnikowi uzasadnienie, że algorytm przedstawiony w pierwszym przykładzie daje optymalne rozwiązanie ze względu na liczbę wykorzystanych banknotów, a algorytm z przykładu drugiego nie jest optymalny ze względu na przebyty dystans.

Zadania

1. Dla danego wielokąta $\mathcal{W}$ niech $s(\mathcal{W})$ oznacza sumę kwadratów długości jego boków. Udowodnić, że jeśli $\mathcal{W}$ jest wielokątem wypukłym, to można wskazać takie trzy jego wierzchołki A, B, C, że $s(\triangle ABC) \geqslant s(\mathcal{W})$. (XI Wielkopolska Liga Matematyczna)
2. Dana jest liczba całkowita $n \geqslant 2$ oraz ciąg $n-1$ znaków mniejszości i większości. Wykazać, że liczby $1, 2, \ldots, n$ można tak wstawić między znaki, aby wszystkie nierówności były spełnione (na przykład dla $n = 5$ i ciągu znaków $(<, >, >, <)$ mamy $4 < 5 > 2 > 1 < 3$). (III WLM)
3. Liczby naturalne $k, n \geqslant 2$ spełniają warunek $1 + \frac{1}{2} + \ldots + \frac{1}{n} < k$. Dowieść, że zbiór $\{\frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}\}$ można podzielić na k podzbiorów, z których każdy ma sumę elementów nie większą niż 1.
4. Zbiór nazywamy *wolnym od sum*, jeśli każde dwa jego różne podzbiory mają różne sumy elementów. Niech k będzie liczbą całkowitą dodatnią. Dowieść, że zbiór o więcej niż 3^k elementach ma $(k+1)$-elementowy podzbiór wolny od sum. (LXII OM)
5. Wyznaczyć najmniejszą stałą c o następującej własności: Dla każdego całkowitego dodatniego n w sumie $1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ można zmienić część znaków $+$ na $-$ w taki sposób, by otrzymać wyrażenie o wartości bezwzględnej nieprzekraczającej $\frac{c}{n^2}$. (XV WLM)
6. Rozstrzygnąć, czy w kole można zmieścić nieskończony zbiór parami rozłącznych kół, które mają nieskończoną sumę obwodów.

Problem otwarty

7. Czy w zadaniu 3 zawsze możliwy jest podział na $k-1$ podzbiorów?

Wskazówki do zadań

1. Wybieramy trzy kolejne wierzchołki X, Y, Z – tak by $|\sphericalangle XYZ| \geqslant 90^\circ$ (jest to możliwe, gdy wielokąt ma co najmniej cztery boki). Jeśli $\mathcal{W}'$ jest wielokątem powstałym z $\mathcal{W}$ przez zastąpienie boków XY i YZ bokiem XZ, to $s(\mathcal{W}') \geqslant s(\mathcal{W})$.
2. Postawmy 1 na pierwszym miejscu, a dalej będziemy dobierać liczby całkowite (niekoniecznie dodatnie) tak, by nierówności były zachowane; dla „$>$” największa możliwa, a dla „$<$” – najmniejsza. Otrzymamy n kolejnych liczb całkowitych, które trzeba będzie jeszcze tylko powiększyć o pewną stałą.
3. Wystarczy umieścić $\frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{k+1}$ w osobnych podzbiorach, a każdy kolejny element zbioru $\{\frac{1}{k+2}, \ldots, \frac{1}{n}\}$ dodawać do tego spośród k podzbiorów, w którym suma jest najmniejsza. Przykład metody nie wprost, że zawsze się do jakiegoś „zmieści”.
4. Przypuśćmy, że mamy zbiór $X = \{x_1, x_2, \ldots, x_k\}$ wolny od sum, i chcemy powiększyć go o nowy element y. Jest to możliwe dokładnie wtedy, gdy dla dowolnych podzbiorów $A, B \subseteq X$ zachodzi $y \neq \sum_{a\in A} a - \sum_{b\in B} b = \sum_{i=1}^{k} \varepsilon_i x_i$, przy czym $\varepsilon_i \in \{-1, 0, 1\}$. To oznacza, że co najwyżej 3^k liczb może zaszkodzić zbiorowi X.
5. Szukana stała jest $c = \frac{35}{12}$ i jest ona osiągana dla $n = 5$. Niech S_n będzie najmniejszą możliwą wartością bezwzględną utworzonego wyrażenia. Można wykazać indukcyjnie, że dla $n \geqslant 7$ zachodzi nierówność $S_n < \frac{1,3}{n^2}$. Krok indukcyjny z n do $n+2$ otrzymujemy przez dodanie $\pm\frac{1}{n+1} \mp \frac{1}{n+2}$, w zależności od znaku.
6. Zachodzi $1 + \frac{1}{2} + \frac{1}{3} + \ldots = \infty$. Koła o promieniach $\frac{1}{2^k}, \frac{1}{2^k+1}, \ldots, \frac{1}{2^{k+1}-1}$ można zmieścić w prostokącie o wymiarach $\frac{1}{2^{k-1}} \times 2$.

KONKURS PTM IM. WITOLDA WILKOSZA

na najlepszą studencką pracę popularyzującą matematykę

Na Konkurs można nadsyłać prace mające na celu popularyzację matematyki

Termin zgłoszeń: **30 września 2025**

Więcej informacji na stronie
https://ok-ptm.im.uj.edu.pl/wilkosz.php

Organizator Konkursu

rok zał. 1919 ptm

Oddział Krakowski
Polskiego Towarzystwa
Matematycznego

Sponsor Konkursu

UNIWERSYTET JAGIELLOŃSKI
W KRAKOWIE

Wydział Matematyki i Informatyki