



Nakład: 3500 egz.

$h=6,63 \cdot 10^{-34} \cdot \nu$ $J \cdot s$ $\pi=3,141592\dots$
NR 12 (535) 2018
CENA 4 ZŁ VAT 5%
PL ISSN 0137-3005 | NR IND 35-550 X
MIESIĘCZNIK
www.deltami.edu.pl



deltami

MATEMATYKA – FIZYKA – ASTRONOMIA – INFORMATYKA

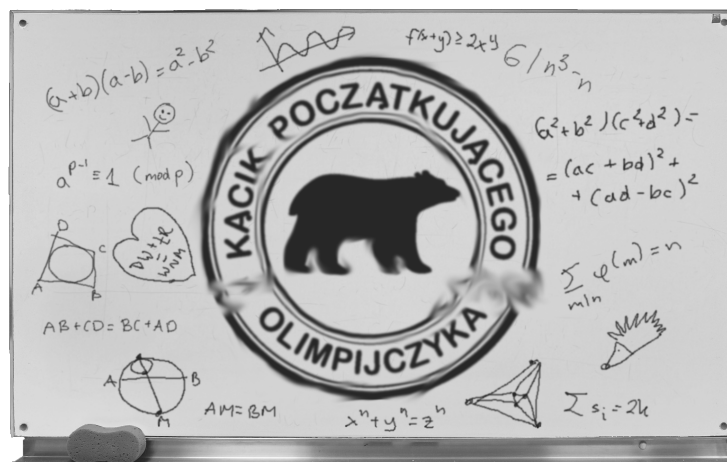
**GDZIE SĄ CI
WSZYSCY OBCY?**
str. 1



SPIS TREŚCI NUMERU 12 (535)

Gdzie są ci wszyscy obcy? <i>Anna Durkalec</i>	str. 1
Problem izomorfizmu grafów <i>Lukasz Kowalik</i>	str. 2
 Zadania	str. 3
Nadprzewodnictwo wysokotemperaturowe <i>Andrzej Wiśniewski</i>	str. 4
Wyniki XL Konkursu Uczniowskich Prac z Matematyki imienia Pawła Domańskiego	str. 5
Ciemna energia – czym jest i czy jest? <i>Maciej Bilicki</i>	str. 6
Jak wyciągnąć $\sqrt{2}$ modulo n ? <i>Mariusz Skalba</i>	str. 8
„Co jest grane” w Teorii Gier <i>Tadeusz Płatkowski</i>	str. 10
Mnożenie nie tylko macierzy <i>Marcin Mucha</i>	str. 11
Zaciemnianie programów <i>Tomasz Kazana</i>	str. 13
Perkolacje <i>Piotr Miłoś</i>	str. 14
Interpretacje teorii kwantów <i>Jan Chwedeńczuk</i>	str. 15
Rozróżnianie słów <i>Wojciech Czerwiński</i>	str. 16
Problem samotnego kolarza <i>Jarosław Grytczuk</i>	str. 18
Informatyczny kącik olimpijski (122): <i>Zalesianie</i>	str. 20
Klub 44	str. 21
Skąd się wzięło siedem?	str. 21
Prosto z nieba: Klimat z Kosmosu	str. 22
Niebo w grudniu	str. 22
Aktualności	str. 24
Nierogaczyna wysokich energii	str. 24
 Kolorowa płaszczyzna <i>Joanna Jaszewska</i>	str. 25

W najbliższym numerze
rozpoczynamy nową matematyczną rubrykę.



Miesięcznik *Delta* – matematyka, fizyka, astronomia, informatyka jest wydawany przez Uniwersytet Warszawski przy współpracy towarzystw naukowych: Polskiego Towarzystwa Matematycznego, Polskiego Towarzystwa Fizycznego, Polskiego Towarzystwa Astronomicznego i Polskiego Towarzystwa Informatycznego.

Komitet Redakcyjny: dr Waldemar Berej, dr Piotr Chrzastowski-Wachtel, dr Krzysztof Ciesielski – wiceprzewodniczący, prof. dr hab. Bożena Czerny, dr Andrzej Dąbrowski, prof. dr hab. Marek Demiański, prof. dr hab. Krzysztof Diks, dr Tomasz Greczyło, prof. dr hab. Paweł Idziak, dr hab. Agnieszka Janiuk, dr hab. Marcin Kiraga, prof. dr hab. Andrzej Majhofer, prof. dr hab. Zbigniew Marciniak, dr hab. Zygmunt Mazur, dr Adam Michalec, dr Zdzisław Pogoda, dr Paweł Preś, prof. dr hab. Wojciech Rytter, prof. dr hab. Paweł Strzelecki.

Redaguje kolegium w składzie: Wiktor Bartol, Michał Bejger, Szymon Charzyński – z-ca red. nac., Wojciech Czerwiński, Tomasz Kazana, Piotr Kaźmierczak, Krystyna Kordos – sekr. red., Marek Kordos – red. nac., Kamila Łyczek, Katarzyna Małek, Łukasz Rajkowski, Anna Rudnik, Krzysztof Rudnik.

Adres do korespondencji:
Instytut Matematyki UW, Redakcja *Delt*y, ul. Banacha 2, pokój 4020, 02-097 Warszawa
e-mail: delta@mimuw.edu.pl tel. 22-55-44-402.

Okladki i ilustracje: Anna Ludwicka Graphic Design & Serigrafia.

Skład systemem \TeX wykonała Redakcja.

Wydrukowano w Drukarni Greg, ul. Górczewska 216, p. 101, 01-460 Warszawa.

PRENUMERATA
Garmond Press: www.garmondpress.pl
Kolporter: www.kolporter.com.pl (tylko instytucje)
RUCH S.A.: www.ruch.com.pl, infolinia 804-200-600
Prenumerata realizowana przez RUCH S.A.:
 Cena prenumeraty w 2019 roku wynosi 4 zł za egzemplarz.

Zamówienia na prenumeratę w wersji papierowej można składać bezpośrednio na stronie www.prenumerata.ruch.com.pl

Ewentualne pytania prosimy kierować na adres e-mail: prenumerata@ruch.com.pl lub kontaktując się z Centrum Obsługi Klienta RUCH pod numerem: 801 800 803 lub 22 693 70 00 – czynne w dni robocze w godzinach 7⁰⁰–17⁰⁰. Koszt połączenia wg taryfy operatora.

Numery archiwalne (od 1987 r.) można nabyć w Redakcji osobiście lub listownie.
 Strona internetowa (w tym artykuły archiwalne, linki itd.): deltami.edu.pl
 Można nas też znaleźć na [facebook.com/Delta.czasopismo](https://www.facebook.com/Delta.czasopismo)
 Wydawca: Uniwersytet Warszawski

Gdzie są ci wszyscy obcy?

Anna DURKALEC*

* Narodowe Centrum Badań Jądrowych

Dyskusje o obcych cywilizacjach wzmagają się i przygasają z różną częstotliwością. Zazwyczaj dzieje się to przy okazji *egzotycznych* odkryć astronomicznych. No i w sumie nie ma czemu się dziwić. Temat jest fascynujący! A brak dowodów na istnienie życia poza Ziemią tylko pobudza naszą wyobraźnię. Szukamy jednak igły w stogu siana. A robimy to w zupełnej ciemności, na nieskończenie wielkim polu, trzymając w ręku świeczkę, z głupią miną mrucząc *cip cip cip* w nadziei, że igła nas usłyszy, zrozumie i zareaguje... bo, tak po prawdzie, to nie wiemy, jak wygląda.

Gdzie szukamy życia?

Zacznijmy od poszukiwań *życia* (lub oznak jego istnienia) w najszerszym możliwym znaczeniu tego słowa. Tu pojawia się pierwszy z licznych problemów. Jak określić, czym jest życie? Google w swojej wszechwiedzy oferuje wiele rozbudowanych definicji. Problem leży jednak w tym, że definicje te dotyczą życia obserwowanego na Ziemi. Nie mamy pojęcia, jak rozszerzyć nasze poszukiwania o *cokolwiek innego*, co hipotetycznie mogło powstać *gdziekolwiek indziej*. Przeszukując Wszechświat, dysponujemy więc wyłącznie teoriami opisującymi powstanie i rozwój życia podobnego nam (szerzej, podobnego ziemskiemu) i tylko na takim się skupiamy. Nie pomaga fakt, że spektrum poszukiwań rozciąga się od cząsteczek pochodzenia organicznego po... inteligentne obce cywilizacje międzygalaktyczne.

Naszym najlepszym kandydatem jest, jak na razie, Mars. Głównie dlatego, że znajduje się bardzo blisko. Ma również przewagę nad naszym drugim sąsiadem – Wenus. Nie jest pokryty gęstymi chmurami siarki i oferuje dużo bardziej znośne temperatury. Niestety, mimo gruntownych poszukiwań wciąż nie znaleźliśmy na nim oznak życia. Mars jest planetą w całości zamieszkaną przez roboty.

W szerszej perspektywie polujemy na planety podobne Ziemi – skaliste i orbitujące wokół rodzimej gwiazdy w odległości pozwalającej na istnienie wody w stanie ciekłym. W tym momencie zaobserwowano ich 13 (40, jeżeli polujemy trochę kryteria). Teoretycznie na każdej z nich moglibyśmy zamieszkać (raczej niewygodnie), więc mogło tam również rozwinąć się życie podobne ziemskiemu.

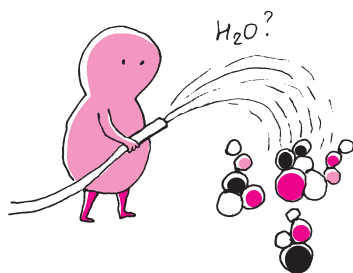
Dzięki tym obserwacjom wiemy, że warunki do powstania życia są raczej powszechne. Nasza planeta nie jest wyjątkowa, a znalezienie obcych form życia to tylko kwestia czasu. I może odrobiny szczęścia.

Inteligentne obce cywilizacje

A co z obcymi z prawdziwego zdarzenia? Superinteligentnymi istotami, które opanowały całe galaktyki? No bo przecież powinny gdzieś tam być? Prawda?

Wystarczy spojrzeć na liczby. Szacuje się, że w obserwowalnym Wszechświecie jest przynajmniej 10^{11} galaktyk, w każdej z nich znajduje się od 10^{10} do nawet 10^{12} gwiazd. Od jakiegoś czasu wiemy, że zdecydowana większość tych gwiazd ma swoje własne układy planetarne. Część z tych planet jest nawet podobna do Ziemi. Na każdej z nich mogło więc rozwinąć się życie. Co więcej, mogło ono powstać zdecydowanie wcześniej niż na naszej planecie. Ba! Nawet przed uformowaniem się Słońca. Hipotetyczna obca cywilizacja, powstała miliardy lat temu, miała więc wystarczająco dużo czasu, by do tej pory skolonizować różne układy planetarne, a nawet całe galaktyki. Szacuje się, że od momentu skonstruowania statku kosmicznego, zdolnego do podróży międzygwiazdnych, skolonizowanie Drogi Mlecznej zajmie ludzkości tylko 2 miliony lat. To naprawdę niewiele w skali Wszechświata.

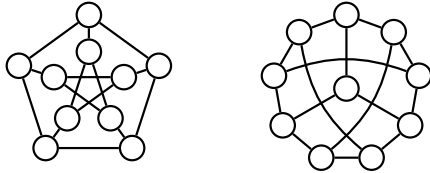
Dlaczego więc obserwujemy dokładnie 0 obcych cywilizacji międzygalaktycznych? Gdzie oni wszyscy są? Czy życie we Wszechświecie, w szczególności to inteligentne, jest aż tak wyjątkowe? Na te pytania nikt nie zna odpowiedzi. Może nasze metody poszukiwań i związane z nimi założenia są zbyt prymitywne i ograniczone? A może Wszechświat jest martwy i pusty, a my jesteśmy w nim zupełnie sami?



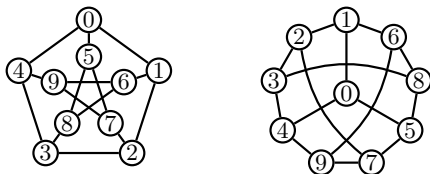
Problem izomorfizmu grafów

Łukasz KOWALIK*

Spójrzmy na dwa grafy na poniższym rysunku. Wyglądają zupełnie inaczej, prawda?



A jednak to tylko złudzenie. Tak naprawdę to jest ten sam graf, ale inaczej narysowany. Istotnie, poniżej ponumerowaliśmy wierzchołki obu grafów od 0 do 9 i łatwo można sprawdzić, że w obu przypadkach wierzchołek o danym numerze ma takie same numery sąsiadów.



Izomorfizm grafów $G = (V_G, E_G)$ i $H = (V_H, E_H)$ to dowolna bijekcja $f: V_G \rightarrow V_H$, taka że dowolne dwa wierzchołki $u, v \in V_G$ sąsiadują w G wtedy i tylko wtedy, gdy $f(u)$ i $f(v)$ sąsiadują w H . Gdy izomorfizm z G do H istnieje, mówimy, że grafy G i H są izomorficzne. Przykład izomorfizmu grafów widzimy na rysunku powyżej.

Informatyk od razu zapyta o algorytm rozstrzygający, czy dane dwa grafy są izomorficzne. Oznaczmy $n = |V_G| = |V_H|$ (gdy ostatnia równość nie zachodzi, problem jest banalny). Algorytm wynikający wprost z definicji sprawdza wszystkie $n!$ bijekcji i działa w czasie $O(n! \cdot n^2)$. Ale czy istnieje algorytm wielomianowy? To niewinne pytanie jest jednym z największych problemów otwartych współczesnej informatyki.

Oczytany Czytelnik zapewne zna wiele innych problemów grafowych, dla których algorytm wielomianowy nie jest znany: problem klikli, problem cyklu Hamiltona, problem kolorowania. Są to problemy NP-zupełne, a rozwiązanie jednego z nich w czasie wielomianowym od razu implikuje takie rozwiązanie dla pozostałych (oraz tysięcy innych nazwanych problemów z klasy NP). Co ciekawe, nie wiemy, czy problem izomorfizmu grafów jest NP-zupełny! Mamy nawet istotne powody, aby podejrzewać, że tak nie jest (przeczyłoby to kilku znanym hipotezom). Gdy autor tego artykułu był studentem, znany był jeszcze jeden problem o podobnym statusie: testowanie pierwszości liczb, w 2002 roku został on jednak rozwiązany w czasie wielomianowym. Czy ten sam los czeka izomorfizm grafów? Aktualny rekord świata, który ustanowił Laszlo Babai dwa lata temu, to algorytm działający w czasie $n^{O((\log n)^c)}$, dla pewnej stałej c .

Zanim porwiemy się na trudny problem, warto zrozumieć jego szczególne, być może prostsze, przypadki. Jedną z najprostszych klas grafów są drzewa (grafy spójne bez cykli). Jak sprawdzić, czy dwa drzewa, T_1 i T_2 , są izomorficzne? Niech v będzie dowolnym wierzchołkiem T_1 . Rozpatrzmy wszystkie n możliwości ustalenia $w = f(v)$. Możemy ukorzenić T_1 w v , tzn. uznać, że v jest korzeniem, a dla dowolnego innego wierzchołka u sąsiad u na (jedynej) ścieżce do v jest ojcem u . Podobnie ukorzeniamy T_2 w w . Naszym celem będzie przypisanie każdemu ukorzenionemu drzewu identyfikatora (wyrażenia nawiasowego) tak, aby drzewa były izomorficzne wtedy i tylko wtedy, gdy mają te same identyfikatory. Wówczas wystarczy porównać identyfikatory T_1 i T_2 . Drzewo składające się z pojedynczego wierzchołka dostaje identyfikator $()$. Identyfikator drzewa powstaje przez a) posortowanie identyfikatorów poddrzew korzenia, b) sklejanie ich w uzyskanej w kolejności w jedno słowo, c) dodanie symbolu $($ na początku i symbolu $)$ na końcu. Na przykład, drzewo \wedge zakodujemy jako $((()())())$, zakładając, że w naszym porządku sortowania nawias otwierający poprzedza nawias zamykający. Czytelnik Pracowity na pewno z łatwością wykaże przez indukcję, że istotnie tylko izomorficzne drzewa dają ten sam identyfikator dla pewnej wartości $w = f(v)$. Tak uzyskany algorytm jest wielomianowy, a kosztem dodatkowego wysiłku można tę złożoność zmniejszyć nawet do liniowej.

Istnieją znacznie bardziej złożone klasy grafów niż drzewa, dla których problem izomorfizmu grafów ma wielomianowe rozwiązanie. Jedną z nich są grafy planarne, tzn. takie, które można narysować na płaszczyźnie bez przecięć krawędzi. Algorytm opiera się na twierdzeniu Whitneya, mówiącemu, że jeśli graf planarny jest 3-spójny (nie da się usunąć dwóch wierzchołków tak, aby uzyskać graf, który nie jest spójny), to można go narysować na sferze w jeden tylko sposób. Dokładniej, każdy rysunek można przekształcić w inny za pomocą ciągłego odwzorowania sfery w sferę. Takie odwzorowania nie zmieniają np. cyklicznej kolejności sąsiadów wierzchołka, a więc gdy mamy już na sferze narysowane dwa grafy i zgadniemy, jak izomorfizm odwzorowuje wierzchołki dowolnej wybranej krawędzi uv , to pozostałe wartości izomorfizmu są wyznaczone jednoznacznie (najpierw wyznaczymy obrazy sąsiadów v , potem sąsiadów sąsiadów v , itd.). Graf ma rysunek na sferze wtedy i tylko wtedy, gdy jest planarny, a przejście od 3-spójnych grafów planarnych do dowolnych planarnych nie jest trudne. Inny słynny wynik to grafy o stopniu ograniczonym przez stałą d : w 1983 roku Babai i Luks podali algorytm działający w czasie $n^{O(d)}$, korzystając z zaawansowanych narzędzi teorii grup.

Na szczęście w praktyce jest dużo lepiej niż w teorii. Rozważmy następujący algorytm. Na początku wszystkie wierzchołki G i H otrzymują ten sam kolor. Niech $c(v)$ oznacza kolor v . Następnie dla każdego wierzchołka v tworzymy multizbiór (tj. zbiór z powtórzeniami) kolorów jego sąsiadów $S(v)$ i zapamiętujemy parę $(c(v), S(v))$. Pokolorujemy teraz graf na nowo w ten sposób, by dwa wierzchołki miały ten sam kolor tylko wtedy, gdy utworzyły wcześniej tę samą parę $(c(v), s(v))$. Postępujemy w ten sposób tak długo, dopóki zwiększa się liczba kolorów. Jeśli multizbiory kolorów wierzchołków G i H są inne, mamy pewność, że G i H nie są izomorficzne (dlaczego?). Zauważmy, że już po pierwszym kroku algorytm ten rozróżni grafy

o innych posortowanych ciągach stopni wierzchołków. Łatwo wykazać, że poprawnie rozróżnia on drzewa. Z drugiej strony, nie rozróżnia grafów regularnych. Okazuje się jednak, że można ten pomysł uogólnić, kolorując wszystkie ciągi k wierzchołków. Jest to *algorytm Weisfeilera–Lehmana wymiaru k* i świetnie sprawdza się w praktyce. Już wymiar $k = 3$ wystarcza, aby rozróżnić grafy planarne. Niestety, okazuje się, że aby rozróżnić dowolne grafy w pesymistycznym przypadku potrzeba wymiaru co najmniej liniowego od n , a więc nie tędy droga do rozwiązania naszego problemu otwartego. Na szczęście pesymistyczne przypadki zdarzają się niezwykle rzadko w rzeczywistych danych.



Zadania

Redaguje Łukasz BOŻYK

M 1585. Na ile sposobów można rozmieścić $3n$ kamieni na szachownicy $n \times n$ w taki sposób, aby w każdym wierszu i w każdej kolumnie znalazły się dokładnie trzy kamienie i były one rozłożone na co najwyżej dwóch polach?

Rozwiązanie na str. 4

M 1586. Kostkę postawiono na stole w taki sposób, że odległości jej wierzchołków od stołu to 0, 1, 2, 3, 4, 5, 6, 7. Oblicz długość jej krawędzi.

Rozwiązanie na str. 5

M 1587. Wyznaczyć wszystkie pary dodatnich liczb całkowitych (n, p) o tej własności, że p jest liczbą pierwszą większą od n oraz $n^2 + np + p^2$ jest kwadratem liczby całkowitej.

Rozwiązanie na str. 4

Przygotował Andrzej MAJHOFER

F 965. W miejscu tłustej plamy kartka robi się „przezroczysta”. Fakt ten wykorzystuje się do budowy prostego fotometru – przyrządu do porównywania natężenia światła emitowanego przez dwa źródła. Kartkę papieru z tłustą plamą w jej środku należy oświetlić prostopadle, z dwóch stron, dwoma źródłami światła – nazwijmy je A i B . Odległości źródeł od kartki dobieramy tak, aby (przy prostopadłej obserwacji) zniknęła różnica jasności plamy i reszty kartki. Wówczas natężenia światła źródeł mają się do siebie, w przybliżeniu, jak kwadraty ich odległości od kartki: $I_A/I_B = (L_A/L_B)^2$. Wspomniane przybliżenie polega na założeniu, że tłusta plama przepuszcza całe padające na nią światło, a reszta kartki całkowicie je odbija. Jak należy zmodyfikować metodę pomiaru, żeby uzyskać poprawną wartość I_A/I_B bez tego założenia?

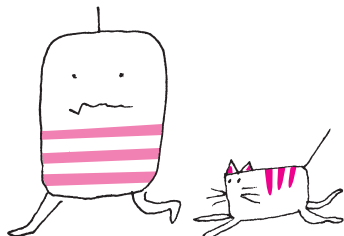
Rozwiązanie na str. 6

F 966. Samochód jadący w obszarze zabudowanym, po suchej drodze (współczynnik tarcia $f_0 = 0,6$) z maksymalną dozwoloną prędkością $v_0 = 50$ km/godz. zatrzymuje się tuż przed pieszym. Z jaką prędkością v uderzyłby w pieszego, gdyby:

a) jechał z prędkością $v_1 = 60$ km/godz.

b) jechał z prędkością v_0 , ale droga była mokra i współczynnik tarcia zmalałby do $f_1 = 0,4$?

Rozwiązanie na str. 9



Nadprzewodnictwo wysokotemperaturowe

*Instytut Fizyki PAN

Andrzej WIŚNIEWSKI*

Nadprzewodnictwo, jedno z najbardziej interesujących zjawisk fizycznych, zostało odkryte stosunkowo dawno – w roku 1911. Ciągłe jednak fascynuje wielu fizyków, zarówno eksperymentatorów, jak i teoretyków. Jego istotą jest to, że w nadprzewodniku poniżej pewnej temperatury, nazywanej temperaturą krytyczną (T_c), opór elektryczny oraz indukcja magnetyczna spadają do zera. Nawet w najlepszych przewodnikach (metalach) przepływowi prądu towarzyszy opór elektryczny, a więc i straty energii. Elektrony – nośniki prądu – są rozpraszane, na skutek zderzeń zmieniają prędkość lub kierunek ruchu. Dlaczego tak się dzieje? Metal możemy sobie wyobrazić jako sieć krystaliczną dodatnio naładowanych jonów, pomiędzy którymi poruszają się elektrony. Jony drgają wokół swoich położeń równowagi. Zderzenia elektronów z drgającymi jonami są podstawową przyczyną rozpraszania elektronów. Amplituda drgań jonów maleje ze spadkiem temperatury. Opór elektryczny maleje, gdy maleje temperatura, jednak może on osiągnąć zerową wartość dopiero w najniższej możliwej w przyrodzie temperaturze: 0 K. Jednak zerowy opór w nadprzewodnikach stwierdza się nawet w tak „wysokich” temperaturach jak 135 K. W tej temperaturze na pewno drgania sieci jonów mają dużą amplitudę i elektrony muszą znaleźć jakiś „chytry” sposób, żeby uniknąć rozpraszania.



Rozwiązanie zadania M 1585.

Odpowiedź: Na $(n!)^2$ sposobów.

Wiersze i kolumny szachownicy nazwijmy *rzędami*, a zbiór n pól szachownicy po jednym w każdym rzędzie – *rozsympem*. Rozsymp można wybrać na dokładnie $n!$ sposobów (np. w i -tym wierszu wybieramy na $n + 1 - i$ sposobów kolumnę, do której należy pole).

Zauważmy, że układ kamieni spełniający warunki zadania ma w każdym rzędzie albo dokładnie jedno pole z trzema kamieniami, albo dokładnie dwa pola, na których leżą odpowiednio jeden i dwa kamienie. Co więcej, zarówno zbiór pól zawierających 1 lub 3 kamienie, jak i zbiór pól zawierających 2 lub 3 kamienie, jest rozsympem. To oznacza, że z każdym rozłożeniem kamieni można związać (uporządkowaną) parę rozsympów.

Z drugiej strony, mając parę rozsympów, możemy na polach pierwszego z nich ustawić po jednym kamieniu, a na polach drugiego – dołożyć po dwa kamienie. Uzyskany w ten sposób układ będzie spełniał warunki zadania. Ostatecznie więc takich układów jest tyle co par rozsympów, czyli $(n!)^2$.



Rozwiązanie zadania M 1587.

Niech m będzie taką dodatnią liczbą całkowitą, że $m^2 = n^2 + np + p^2$, czyli

$$(m - n)(m + n) = p(n + p).$$

Z nierówności

$$m^2 = n^2 + np + p^2 < (n + p)^2$$

uzyskujemy $m < n + p$, czyli $m - n < p$. W szczególności liczba $m - n$ nie jest podzielna przez p , skąd wobec podzielności iloczynu $(m - n)(m + n)$ przez p uzyskujemy $p | m + n$. Ponadto skoro $n < p$, to

$$p < m < m + n < 2n + p < 3p,$$

skąd $m + n = 2p$, czyli $m = 2p - n$.

Zatem

$$(2p - n)^2 = n^2 + np + p^2,$$

co po uproszczeniu przybiera postać $5n = 3p$ i wobec pierwszości liczby p prowadzi do wniosku, że $(n, p) = (3, 5)$. Jest to jedyna para o zadanych własnościach.

Stwierdzenie, na czym polega ten „chytry” sposób, zajęło fizykom ponad 40 lat. Dopiero w połowie lat pięćdziesiątych XX w. została opracowana, przez trzech fizyków amerykańskich: Bardeena, Coopera i Schriffiera, teoria wyjaśniająca mechanizm nadprzewodnictwa (otrzymali za to w 1973 r. Nagrodę Nobla). Nazywa się ją w skrócie teorią BCS, od pierwszych liter nazwisk jej twórców.

Podstawą teorii BCS jest zaskakujący pomysł, że w nadprzewodniku elektrony łączą się w pary. Pomysł ten jest zaskakujący dlatego, że elektrony mają taki sam ujemny ładunek – powinny się więc odpychać, a nie łączyć w pary. Elektrony odpychają się, oczywiście, na skutek oddziaływania kulombowskiego, ale w kryształach istnieje pomiędzy nimi dodatkowe oddziaływanie przyciągające. Jest ono związane z oddziaływaniem elektronów z siecią krystaliczną. Można to sobie wyobrazić w ten sposób, że w trakcie swojego ruchu elektron poprzez oddziaływanie przyciągające deformuje rozkład ładunków dodatnio naładowanych jonów tworzących sieć krystaliczną. Elektron, który znajdzie się w pobliżu, odczuwa to zaburzenie sieci i jest przez nie przyciągany. W ten sposób, za pośrednictwem sieci, dwa elektrony będą się przyciągać. To oddziaływanie może być silniejsze niż oddziaływanie odpychające. Ponieważ drgania sieci krystalicznej nazywamy fononami – taki mechanizm łączenia elektronów w pary nazywamy fononowym.

Zjawisko nadprzewodnictwa występuje w wielu materiałach. W większości przypadków T_c są niskie, często bliskie temperatury 0 K (0 K = $-293,15^\circ\text{C}$). Jakie materiały wykazują nadprzewodnictwo? Wykazuje je większość metali, jednakże dopiero poniżej temperatury rzędu kilku kelwinów. Najwyższą temperaturę krytyczną wśród metali, $T_c = 9,2$ K, ma niob (Nb). Nadprzewodnictwo wykazuje wiele stopów, najwyższą T_c ma stop Nb_3Ge – wynosi ona 23,3 K. Przez wiele lat była to najwyższa temperatura krytyczna. W roku 1986 odkryto nową klasę materiałów wykazujących nadprzewodnictwo. Nazwano te materiały nadprzewodnikami wysokotemperaturowymi, określenie to należy traktować z pewną rezerwą. Nazywamy tak materiały, których temperatura krytyczna jest znacznie wyższa od temperatury „starych”, konwencjonalnych, nadprzewodników. Ciągłe są to jednak, z punktu widzenia życia codziennego, temperatury niskie. Jak stwierdzono w 1993 roku, najwyższa znana obecnie T_c nadprzewodnika wysokotemperaturowego $\text{HgBa}_2\text{Ca}_2\text{Cu}_3\text{O}_{8+x}$ wynosi 135 K czyli -138°C (pod ciśnieniem atmosferycznym), pod wysokim ciśnieniem T_c tego związku wzrasta do 164 K. Od roku 1993 nie znaleziono materiału, który pod ciśnieniem normalnym wykazywałby wyższą T_c .

Za przełomowe dla nadprzewodników wysokotemperaturowych można uznać dwa odkrycia – pierwsze, dokonane w 1986 roku przez Szwajcarów, Alexa Mullera i Georga Bednorza (Nagroda Nobla w 1987 r.). Stwierdzili oni występowanie



Rozwiązanie zadania M 1586.

Niech A_i będzie wierzchołkiem kostki, odległym od stołu o i . Oznaczmy długość krawędzi kostki przez x . Łatwo zauważyć, że odcinki A_0A_1 , A_0A_2 oraz A_0A_4 muszą być krawędziami sześcianu (wynika to z faktu, że jeśli krawędziami są A_0A_i i A_0A_j , to $A_0A_iA_{i+j}A_j$ jest ścianą). Niech x będzie długością krawędzi sześcianu. Dobierzmy układ współrzędnych tak, by $A_1 = (x, 0, 0)$, $A_2 = (0, x, 0)$ i $A_4 = (0, 0, x)$. Oznaczmy przez A'_i rzut prostokątny punktu A_i na prostą prostopadłą do stołu, przechodzącą przez A_0 ; wówczas $|A_0A'_i| = i$. Przyjmijmy $A'_1 = (a, b, c)$, wtedy $A'_2 = (2a, 2b, 2c)$ i $A'_4 = (4a, 4b, 4c)$. Korzystając z twierdzenia Pitagorasa dla trójkątów prostokątnych $A_0A'_iA_i$ dla $i = 1, 2, 3$ dostajemy

$$\begin{cases} (a-x)^2 + b^2 + c^2 + 1 = x^2 \\ 4a^2 + (2b-x)^2 + 4c^2 + 4 = x^2 \\ 16a^2 + 16b^2 + (4c-x)^2 + 16 = x^2. \end{cases}$$

Wykorzystując powyższe równości oraz $a^2 + b^2 + c^2 = 1$, dostajemy $ax = 1$, $bx = 2$ i $cx = 4$. Po podniesieniu ostatnich trzech równości do kwadratu i zsumowaniu, otrzymamy $x^2 = 1^2 + 2^2 + 4^2$, zatem $x = \sqrt{21}$.

nadprzewodnictwa w ceramicznym materiale tlenkowym zawierającym lantan, bar, miedź i tlen – $(\text{La,Ba})_2\text{CuO}_{4-x}$. Temperatura krytyczna wynosiła 35 K, była więc istotnie większa niż poprzedni „rekord”. Znaczenie ich odkrycia polegało jednak przede wszystkim na tym, że zwrócono uwagę na nową grupę materiałów, zupełnie nie „podejrzewaną” o to, że może wykazywać nadprzewodnictwo. W krótkim czasie, na początku roku 1987, Amerykanin Paul Chu odkrył nadprzewodnictwo w związku $\text{YBa}_2\text{Cu}_3\text{O}_{7-x}$. W tym przypadku kluczowa jest wartość $T_c = 92$ K. Z punktu widzenia zastosowań jest to odkrycie przełomowe. Jest to bowiem temperatura wyższa od temperatury ciekłego azotu, która wynosi 77 K. Aby wykorzystać w praktyce nadprzewodnik (na przykład do przesyłania prądu bez strat), konieczne jest utrzymywanie go przez cały czas w temperaturze niższej od T_c . Oznacza to, że nadprzewodnik konwencjonalny musi być zanurzony w ciekłym helu, natomiast nadprzewodnik $\text{YBa}_2\text{Cu}_3\text{O}_{7-x}$ może być zanurzony w ciekłym azocie. Jest to różnica zasadnicza. Ciekły hel jest dużo droższy i dużo mniej dostępny od ciekłego azotu, jego wytwarzanie, przechowywanie, przelewanie do zbiorników jest dużo bardziej skomplikowane niż w przypadku azotu.

Zostały przebadane różne materiały wykazujące nadprzewodnictwo w temperaturach wyższych od temperatury ciekłego azotu. Wiemy o tych materiałach już dosyć dużo. Ciągłe jednak nie znamy odpowiedzi na dwa podstawowe, związane zresztą ze sobą, pytania. Jaki jest mechanizm nadprzewodnictwa wysokotemperaturowego? Wiadomo, że nośnikami prądu są pary elektronów, nie jest jednak jasne, jaki jest mechanizm łączenia się elektronów w pary. Teoria BCS, która tłumaczyła to dobrze w przypadku nadprzewodników klasycznych, nie wystarcza. Drugie pytanie: jaka jest możliwa najwyższa temperatura krytyczna w tej grupie materiałów, czy możliwe jest nadprzewodnictwo w temperaturze pokojowej? Też na razie pozostaje bez odpowiedzi. A odpowiedzi na te pytania są na wagę Nagrody Nobla.

Eksperyment przeprowadzony w 2015 r. pokazał jednak, że rekordową obecnie temperaturę krytyczną, $T_c = 203$ K, wykazuje... siarkowodór (H_2S). Tyle że stan nadprzewodzący obserwuje się tylko pod ogromnymi ciśnieniami około 150 GPa (ciśnienie w jądrze Ziemi wynosi około 360 GPa). Co ciekawe, za nadprzewodnictwo w tak wysokiej temperaturze odpowiedzialny jest klasyczny – fononowy mechanizm łączenia się elektronów w pary Coopera.

Końcowa uwaga: zjawisko nadprzewodnictwa możemy traktować jak coś egzotycznego – niskie temperatury, wysokie ciśnienia... Jednak tak naprawdę, to temperatury i ciśnienia, do których przyzwyczailiśmy się na Ziemi, są wyjątkowo egzotyczne. Stan nadprzewodzący może być więc dużo bardziej fundamentalnym stanem materii, niż się nam wydaje.

Protokół posiedzenia Jury XL Konkursu Uczniowskich Prac z Matematyki im. Pawła Domańskiego

Jury Konkursu Uczniowskich Prac z Matematyki w składzie: Andrzej Komisarki – przewodniczący jury, Bartłomiej Bzdęga, Adam Dzedzej, Andrzej Grzesik, Kamila Łyczek, Zdzisław Pogoda po wysłuchaniu w dniu 27 września 2018 roku prezentacji prac dopuszczonych do finału, biorąc pod uwagę dobór tematów, treść prac i sposób ich przedstawienia, postanowiło, co następuje:

- Złoty medal i nagrodę w wysokości 1500 zł otrzymuje Stanisław Hauke *Czworokąty bliźniacze* (XIV LO im. Stanisława Staszica w Warszawie, opiekun Waldemar Pompe).
- Srebrny medal i nagrody w wysokości 1000 zł otrzymują Filip Rękawek *O trójkątach kappa i ich własnościach* (Katolickie Liceum Ogólnokształcące im. C. K. Norwida w Garwolinie, opiekun Michał Szurek) oraz Mariusz Trela *Kolorowanie prostych w \mathbb{F}_{p^2}* (V LO w Krakowie, opiekun Dominik Burek).

- Brązowy medal i nagrodę w wysokości 500 zł otrzymuje Paweł Sawicki *Hexapawn wydłużony* (III LO w Gdyni im. Marynarki Wojennej RP, opiekun Wojciech Tomalczyk).

Finalista: Jakub Szulc *O wielomianach symetrycznych* (Zespół Szkół Uniwersytetu Mikołaja Kopernika Gimnazjum i Liceum Akademickie w Toruniu, opiekun Daniel Strzelecki).

Finaliści i opiekunowie prac otrzymują również nagrody rzeczowe ufundowane przez: Wydawnictwa Uniwersytetu Warszawskiego, Wydawnictwo PWN, Wydawnictwo Szkolne Omega, Wydawnictwo Aksjomat.

Prace nadsyłane na Konkurs powinny być samodzielnie przygotowanymi przez uczniów opracowaniami, zawierającymi nowe wyniki lub nowe twórcze ujęcie tematu. Szczegółowy regulamin Konkursu znajduje się na stronie deltami.edu.pl. Termin nadsyłania prac w kolejnej edycji konkursu to 30 kwietnia 2019 roku.

Ciemna energia – czym jest i czy jest?

Maciej BILICKI*

* Uniwersytet w Lejdzie,
Narodowe Centrum Badań Jądrowych

Konieczność istnienia ciemnej materii (patrz np. Δ_{18}^{11}) to nie koniec niespodzianek, jakie przyszykowały nam obserwacje Wszechświata. Od 20 lat wiemy, że dla pełnego wyjaśnienia składu kosmosu musimy dodać również ciemną energię. To ona miałaby być odpowiedzialna za odkryte w 1998 roku przyspieszanie ekspansji Wszechświata. Oznaczana w równaniach literą Λ i zwana w swej najprostszej formie stałą kosmologiczną, ta forma energii miałaby zaiste niespotykane właściwości: ujemne ciśnienie i stałą gęstość mimo zwiększania się objętości przestrzeni. To ona tworzy przeciwagę dla wyłącznie przyciągającej grawitacji (która spowalnia ekspansję), a ponieważ ciemnej energii jest odpowiednio dużo (w przeliczeniu na gęstość masy-energii), od kilku miliardów lat zaczęła ona dominować w globalnym bilansie i tempo rozszerzania się Wszechświata wzrasta zamiast maleć.

Odkrycie przyspieszającej ekspansji było zaskoczeniem, natomiast sama obecność Λ w równaniach opisujących Wszechświat już nie. Pojawia się ona już w pierwszych pracach Einsteina na temat ogólnej teorii względności jako stała równań. Z matematycznego punktu widzenia Λ może mieć dowolną wartość, w tym 0; faktyczna wartość Λ ma jednak duży wpływ na jej fizyczną interpretację. Opracowując pierwszy relatywistyczny model kosmologiczny, Einstein uważał, że równania powinny zapewnić statyczność kosmosu w największych skalach (odkrycie, że galaktyki od nas „uciekają”, przyszło dopiero kilka lat później). Zauważył, że odpowiednio dobierając (dodatnią) wartość Λ , kompensując tym samym obecność materii, uzyska Wszechświat statyczny. Wkrótce potem Eddington wykazał jednak, że taki model kosmologiczny jest niestabilny na najmniejsze zaburzenia, a odkrycie ucieczki galaktyk przez Sliphera i innych (ujęte przez Hubble’a w związek $d \propto v_{rec}$), wykluczyło poprawność modelu Wszechświata statycznego.

Einstein początkowo nie zdawał sobie sprawy, że dla $\Lambda = 0$, czyli w modelu kosmologicznym zawierającym tylko materię, występuje albo kontrakcja, albo ekspansja Wszechświata – co pokazali dopiero Friedman oraz niezależnie Lemaître kilka lat później. Gdy prace Friedmana i Lemaître’a zdobyły już uznanie wśród ówczesnych kosmologów, sam Einstein wraz z de Sitterem zaproponowali model kosmologiczny z zerową Λ i odpowiednio dobraną gęstością materii (gęstością „krytyczną”), który rozszerzał się od „punktu zerowego” ze stopniowo malejącym tempem ekspansji, zbiegającym do zerowego po nieskończonym czasie. Ten model był „modny”, czy wręcz uważany za poprawny, aż do końca lat 1990 z braku rozstrzygających dowodów obserwacyjnych.

Po odkryciu ekspansji Wszechświata i zrozumieniu, że jest ona możliwa również we Wszechświecie wypełnionym wyłącznie materią, Einstein ponoć uznał wprowadzenie Λ za „największą pomyłkę swojego życia” (*biggest blunder*). Historycy nauki i biografowie Einsteina spierają się, czy rzeczywiście tak uważał; stwierdzenie to pochodzi z książki George’a Gamowa, znanego z rozpowszechniania podkoloryzowanych anegdot – Gamow miał być jedynym świadkiem tego wyznania Einsteina. Na ironię zakrawa fakt, że Λ „powróciła” kilka dekad później, i to raczej początkowe nieuwzględnienie możliwości ekspansji („narzucającej” się przy modelowaniu Wszechświata rozwiązaniami równań Einsteina) należy uznać za, być może, największą pomyłkę tego genialnego uczonego.

Jednak niesłuszne byłoby sądzić, że od momentu zakwestionowania statycznego modelu Einsteina aż do końca XX wieku nikt nie rozważał niezerowej wartości Λ . Pojawia się ona zarówno w rozważaniach Friedmana, jak i Lemaître’a (a także Edingtona, de Sittera i innych) już w latach 1920. W szczególności Lemaître badał modele o różnych wartościach Λ i gęstości materii (jako że te dwa składniki wystarczą do opisu zawartości obecnego Wszechświata w największych skalach). To w jego rozważaniach pojawia się uznawany dziś za



Rozwiązanie zadania F 965.

Przyjmijmy, że dla plamy współczynnik transmisji wynosi T , a odbicia R . Niech dla reszty kartki odpowiednie współczynniki wynoszą r i t . Plama „znika”, gdy źródło A jest w odległości L_A , a źródło B , w odległości L_B od kartki (patrzmy od strony A). Mamy wówczas (oświetlenia obu części kartki są równe):

$$\frac{rI_A}{L_A^2} + \frac{tI_B}{L_B^2} = \frac{RI_A}{L_A^2} + \frac{TI_B}{L_B^2},$$

czyli

$$\frac{r-R}{L_A^2} I_A = \frac{T-t}{L_B^2} I_B.$$

Zamieńmy teraz miejscami źródła światła (obserwujemy kartkę z tej samej strony) i wyznaczmy nowe odległości, dla których plama „znika”: l_A i l_B . Otrzymujemy analogiczne równania (B jest teraz od strony obserwatora):

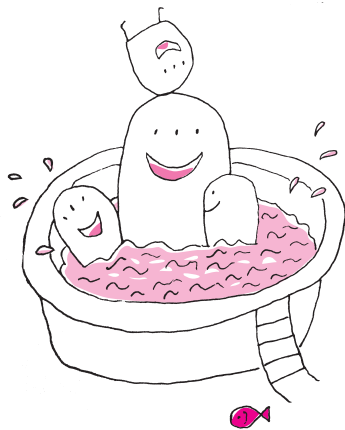
$$\frac{r-R}{l_B^2} I_B = \frac{T-t}{l_A^2} I_A.$$

Po podzieleniu stronami (z obserwacji wiemy, że odpowiednie różnice współczynników są różne od zera) otrzymujemy:

$$\frac{I_A}{I_B} = \frac{L_A l_A}{L_B l_B}.$$

Ze względu na sposób produkcji papieru obie strony kartki różnią się i drugi, niezależny pomiar możemy uzyskać po odwróceniu kartki i powtórzeniu procedury.

Przedstawiony tu fotometr został zaproponowany przez Roberta Wilhelma Bunsena w roku 1843, a ulepszony sposób jego użycia podał D.W. Lewis w *Nature* 40, 174 (1889).



Profesor Roman Juszkiewicz wraz z wieloma współpracownikami badał pod koniec XX w. wielkoskalowe pola prędkości swoistych – odstępstwa od jednorodnej ekspansji wynikające z lokalnych zagęszczeń materii. Roman Juszkiewicz miał znaczący udział w opracowaniu aparatu teoretycznego zastosowanego następnie do (skąpych wtedy) danych obserwacyjnych. Te analizy dały niezależne przesłanki, iż gęstość materii wynosi znacznie poniżej krytycznej. Pola prędkości są jednak „nieczule” na stałą kosmologiczną, tak więc potrzebne były obserwacje supernowych i mikrofalowego promieniowania tła, by połączyć wszystko w jedną całość – Λ CDM.

standardowy model zapoczątkowany „punktem zerowym”, zwanym dziś Wielkim Wybuchem, po którym następuje spowalniająca ekspansja (era dominacji promieniowania, a następnie materii), która potem przyspiesza (era dominacji stałej kosmologicznej).

Jednak oprócz teoretycznych rozważań Lemaître’a i innych prekursorów kosmologii, Λ przez wiele dekad nie była potrzebna do wyjaśnienia (skąpych) obserwacji – skoro wiadomo było, że Wszechświat się rozszerza, i można to ująć modelem tylko z materią, to brzytwa Ockhama każe nam przyjąć $\Lambda = 0$. Sytuacja jednak zaczęła się zmieniać w latach 1980. Najpierw Alan H. Guth, Andrej Linde i inni zaproponowali, że w pierwszych mikrosekundach swojego istnienia (tj. zaraz po „punkcie zero” w modelu Wielkiego Wybuchu) Wszechświat doświadczył eksponencjalnej ekspansji – „inflacji”. Była to próba wyjaśnienia kilku problemów kosmologicznych, takich jak jednorodność Wszechświata w największych skalach – większych niż obszary powiązane przyczynowo-skutkowo, gdyby inflacji nie było. Co ciekawe, taka eksponencjalna ekspansja jest świetnie opisywana modelem de Sittera zawierającym dodatnią Λ i zaniedbywalną gęstość materii. Związek tej „inflacyjnej Λ ” z dzisiejszą ciemną energią jest niejasny, ale raczej nie są one tym samym, bo inflacja się zakończyła jakieś 10^{-32} s po Wielkim Wybuchu, po czym przez kilka miliardów lat w kosmosie dominowała materia.

W kontekście dyskusji o ciemnej energii ważne jest, że jednym z głównych przewidywań teorii inflacyjnej jest globalna płaskość przestrzenna Wszechświata. Innymi słowy, kosmos w największych skalach powinien według teorii inflacji mieć geometrię euklidesową. To tłumaczy popularność modelu Einsteina–de Sittera: płaskiego, zawierającego tylko materię, przez ostatnie dwie dekady XX wieku. Jednak nie wszystkie obserwacje potwierdzały prawdziwość modelu o gęstości równej krytycznej. Badania choćby wielkoskalowych przepływow galaktyk – ze znaczącym udziałem Romana Juszkiewicza – wskazywały, że materii jest za mało, by Wszechświat „domknąć” do gęstości krytycznej. Pogodzenie tego z przewidywaniami inflacji jest możliwe, gdy gęstość materii-energii domknie się do wartości krytycznej dodatnią Λ .

Stąd też i obserwacje odległych supernowych Ia – „świec standardowych” – prowadzone przez Perlmuttera, Riessa i Schmidta, pokazujące, że ekspansja przyspiesza zamiast zwalniać – padły na podatny grunt i doprowadziły do powstania modelu zwanego dziś Λ CDM (gdzie CDM to zimna ciemna materia). Zgodność tego modelu z obserwacjami została od tej pory potwierdzona wieloma różnymi testami. Jednym z najważniejszych jest analiza właściwości mikrofalowego promieniowania tła, która pozwala zarówno z dużą dokładnością ustalić globalną krzywiznę przestrzeni (wynoszącą zero – płaskość), jak i średnią gęstość materii (wynoszącą około 30% gęstości krytycznej). Już te dwa fakty pokazują, że konieczny jest model z $\Lambda > 0$, dopełniającą gęstość masy-energii do wartości krytycznej. Obrazu dopełniają inne dane, choćby bardziej dziś dokładne niż pod koniec XX wieku pomiary tempa ekspansji Wszechświata w funkcji czasu kosmicznego, już nie tylko z supernowych, ale i tzw. barionowych oscylacji akustycznych. Wszystkie one pokazują jednoznacznie, że ekspansja kosmosu przyspiesza.

„Jednoznacznie” to jednak nawet we współczesnej „kosmologii precyzyjnej” duże słowo. Głównym problemem z ciemną energią pozostaje fakt, że nie mamy zupełnie pojęcia, czym mogłaby być w fizycznym sensie. O ile ciemną materię próbuje się wyjaśnić w oparciu o dobrze ugruntowane hipotezy (takie jak cząstki elementarne wykraczające poza model standardowy), to ciemna energia modelowana jest głównie fenomenologicznie. Uznaje się ją za jakiś rodzaj „energii próżni” i w oparciu o obserwacje astronomiczne próbujemy nałożyć ograniczenia na jej równanie stanu. Jak dotąd, ograniczenia te są bardzo słabe i wiemy jedynie, że jest to zgodne w granicach (dużych) błędów z $p = -\rho$, czyli stałą kosmologiczną – najprostszą teoretycznie formą ciemnej energii, dla której ten związek nie zmienia się z czasem. Rozwija się jednak wiele innych modeli, począwszy od „kwintesencji” i jej podobnych (równanie stanu zmienne

Większość modeli kosmologicznych, w tym Λ CDM, zakłada, że Wszechświat w odpowiednio dużych skalach jest jednorodny i izotropowy, dzięki czemu możemy przyjąć wiele symetrii i opisywać go prostą metryką Friedmana–Lemaître’a–Robertsona–Walkera. Niektórzy kosmologowie twierdzą jednak, że jest to nadmierne uproszczenie i właśnie to założenie prowadzi do „artefaktu”, jakim jest przyspieszająca ekspansja, pisaliśmy o tym w Δ_{16} . W niektórych z modeli „niejednorodnych” nie można globalnie zdefiniować średniej krzywizny czy gęstości, przez co inaczej interpretuje się w nich obserwacje np. supernowych (takie jak związek odległości z przesunięciami ku czerwieni).

w czasie), po zmodyfikowaną grawitację, w której w skrajnych przypadkach Λ nie ma w równaniach w ogóle, jest za to „piąta siła” – dodatkowe oddziaływanie, w wyniku którego grawitacja jest słabsza na bardzo dużych kosmicznych skalach, co skutkuje przyspieszającą ekspansją. Niektórzy natomiast twierdzą, że żadna modyfikacja grawitacji nie jest konieczna, należy natomiast zrewidować nasz opis Wszechświata jako jednorodnego i izotropowego. Według tego rodzaju modeli przyspieszanie ekspansji jest pozorne, a to, że je „widzimy”, wynika ze zbyt uproszczonego modelu, w którym obserwacje są interpretowane.

Zarówno modele zmodyfikowanej grawitacji, jak i te zakładające znaczące niejednorodności, mają swoje wady, na pewno nie mniejsze niż standardowy model kosmologiczny, jakim jest Λ CDM. A ponieważ żadne obserwacje kosmologiczne nie wskazują obecnie na znaczne odstępstwa od modelu standardowego (a w każdym razie nie widać, aby jakiś inny model lepiej je wyjaśniał), brzytwa Ockhama odcina wszystko, co nie jest Λ CDM. Czy to się zmieni w najbliższych latach, gdy nowe, większe i głębsze przeglądy kosmosu staną się rzeczywistością? Czy ambitne programy, takie jak Euclid, LSST, JWST czy SKA, przybliżą nas do wyjaśnienia zagadki Λ , czy wręcz przeciwnie?

Jak wyciągnąć $\sqrt{2}$ modulo n ?

Mariusz SKAŁBA*

* Instytut Matematyki, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Niech n będzie liczbą nieparzystą. Pytamy, czy istnieje taka liczba całkowita x , że

$$(1) \quad x^2 \equiv 2 \pmod{n}?$$

Jeśli ta kongruencja ma rozwiązanie całkowite x , to na pewno istnieje rozwiązanie $x_1 \in \{0, 1, \dots, n-1\}$. Wtedy liczba $x_2 = n - x_1$ też jest rozwiązaniem. Jak jednak rozstrzygnąć, czy kongruencja (1) w ogóle ma rozwiązania?

W przypadku, gdy $n = p$ jest liczbą pierwszą, dysponujemy praktycznym algorytmem, który rozstrzyga, czy kongruencja (1) ma rozwiązanie – oparty jest on na tzw. **kryterium Eulera**. Jest ono ściśle związane z **małym twierdzeniem Fermata**. To słynne twierdzenie mówi, że jeśli x nie dzieli się przez liczbę pierwszą p , to wówczas

$$x^{p-1} \equiv 1 \pmod{p}.$$

Jeśli kongruencja (1) ma rozwiązanie x , to możemy napisać

$$2^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p},$$

a zatem ostatecznie

$$(2) \quad 2^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Kryterium Eulera stanowi, że powyższe rozumowanie można odwrócić: jeśli zachodzi kongruencja (2), to kongruencja (1) ma rozwiązanie. Warto w tym miejscu dodać, że potęgowanie a^k modulo n łatwo wykonać efektywnie nawet wtedy, gdy liczby n oraz k są ogromne! Oto zarys metody. Najpierw zapisujemy wykładnik k w układzie dwójkowym:

$$k = 2^{m_1} + 2^{m_2} + \dots + 2^{m_l}, \quad \text{gdzie } m_1 < m_2 < \dots < m_l = \lfloor \log_2 k \rfloor.$$

Ponieważ

$$a^k = a^{2^{m_1}} \cdot a^{2^{m_2}} \cdot \dots \cdot a^{2^{m_l}},$$

więc wystarczy wykonać m_l kolejnych podnoszeń do kwadratu, a na koniec $l-1$ mnożeń – wszystkie operacje wykonujemy modulo n , a więc na liczbach mniejszych od n .

Zalóżmy teraz, że liczba 2 przeszła test Eulera. Nasuwa się teraz pytanie: jak znaleźć x spełniające kongruencję (1)?

Jeśli $p \equiv 3 \pmod{4}$, to wystarczy przyjąć

$$x \equiv 2^{\frac{p+1}{4}} \pmod{p}.$$

Pokazuje to poniższy rachunek

$$x^2 \equiv 2^{\frac{p+1}{2}} \equiv 2^{\frac{p-1}{2}} \cdot 2^1 \equiv 2 \pmod{p}$$

(na mocy (2)).

Jeżeli natomiast $p \equiv 1 \pmod{4}$, to nieco komplikując powyższą metodę (szczegóły pominiemy), można obliczyć x spełniające (1), o ile mamy do dyspozycji taką liczbę s , że kongruencja

$$(3) \quad x^2 \equiv s \pmod{p}$$

nie ma rozwiązań. Taką liczbę s nazywamy *nieresztą kwadratową modulo p* . Łatwo udowodnić, że w ciągu liczb $1, 2, \dots, p-1$ jest dokładnie $(p-1)/2$ niereszt. Dla pozostałych liczb s z powyższego ciągu kongruencja (3) ma rozwiązanie – nazywamy je *resztami kwadratowymi modulo p* . I tak np. dla $p = 7$ liczby $1, 2, 4$ są resztami kwadratowymi, a liczby $3, 5, 6$ nieresztami kwadratowymi. Natomiast dla $p = 11$ nieresztą kwadratową to $2, 6, 7, 8, 10$, a reszty kwadratowe to $1, 3, 4, 5, 9$. Nieresztą kwadratową s , której używamy we wzmiarkowanym powyżej algorytmie pierwiastkowania modulo p , łatwo znaleźć praktycznie nawet dla bardzo dużych liczb pierwszych p . Wystarczy mianowicie wylosować liczbę $s \in \{1, 2, \dots, p-1\}$ i sprawdzić, czy jest nieresztą kwadratową, stosując, na przykład, kryterium Eulera. W przypadku niepowodzenia losujemy i testujemy inną liczbę s . Prawdopodobieństwo wylosowania nieresztą w każdej próbie wynosi $1/2$, a zatem przeciętnie bardzo szybko znajdziemy nieresztę. Jest to przykład **algorytmu zrandomizowanego**. Rzucając 20 razy symetryczną monetą, możemy, oczywiście, wyrzucić same *reszty* (niektórzy mówią *reszki*), ale prawdopodobieństwo tego jest małe.

A może lepiej testować po kolei liczby $s = 1, 2, 3, \dots$, aż do skutku, czyli do napotkania nieresztą? Niech więc $N(p)$ oznacza najmniejszą nieresztą kwadratową modulo p . Najlepszy wynik bezwarunkowy pochodzi od D.A. Burgessa

$$N(p) < p^{\frac{1}{4\sqrt{\varepsilon}} + \varepsilon}$$

dla każdego $\varepsilon > 0$ i $p > p_0(\varepsilon)$. Natomiast przy założeniu **uogólnionej hipotezy Riemanna N.C.** Ankeny pokazał oszacowanie znacznie lepsze

$$N(p) < C(\log p)^2 \text{ dla pewnej stałej } C > 0.$$

Tak więc prymitywny algorytm testowania kolejnych liczb s jest (warunkowo) bardzo efektywny.

Podsumujmy nasze dotychczasowe rozważania: jeśli moduł n jest liczbą pierwszą, to w zasadzie potrafimy poradzić sobie zarówno z rozstrzygnięciem, czy 2 jest resztą kwadratową modulo n , jak i ze znalezieniem wszystkich rozwiązań kongruencji (1) w zbiorze $\{1, 2, \dots, n-1\}$ (są dwa takie rozwiązania).

A jak jest dla liczb złożonych n ? Rozpatrzmy najprostszy przypadek, gdy $n = pq$ jest iloczynem dwóch różnych liczb pierwszych. Do dzisiaj nie jest znana żadna efektywna uniwersalna metoda rozstrzygnięcia, czy kongruencja (1) ma rozwiązanie. Załóżmy jednak, że dobra wróżka rzekła: *Tak, kongruencja (1) jest rozwiązalna, a Twoje zadanie to znaleźć jej wszystkie rozwiązania x w zbiorze $\{1, 2, \dots, n-1\}$* . Załóżmy dalej, że jakimś *cudem* wypisaliśmy wszystkie (cztery – wynika to z chińskiego twierdzenia o resztach) rozwiązania kongruencji (1):

$$1 \leq x_1 < x_2 < x_3 < x_4 \leq pq - 1.$$

Ponieważ kongruencja $y^2 \equiv 2 \pmod{p}$ ma dokładnie dwa rozwiązania y_1, y_2 w zbiorze $\{1, 2, \dots, p-1\}$, więc dla pewnych $1 \leq i < j \leq 3$ mamy $x_i \equiv x_j \pmod{p}$, a zatem liczba $x_j - x_i$ dzieli się przez p . Oczywiście, $x_j - x_i$ nie dzieli się przez $n = pq$, gdyż $1 \leq x_j - x_i < pq - 2$. A zatem

$$\text{NWD}(x_j - x_i, n) = p.$$

Liczyby $\text{NWD}(x_2 - x_1, n)$, $\text{NWD}(x_3 - x_2, n)$, $\text{NWD}(x_3 - x_1, n)$ potrafimy obliczyć, bardzo efektywnie stosując najsłynniejszy algorytm na świecie – algorytm Euklidesa. W ten sposób znaleźliśmy nietrywialny dzielnik p liczby $n = pq$. Najbardziej pomógł nam *cud* (a nie wróżka). Tym samym naszkicowaliśmy główną myśl dowodu twierdzenia, że kompletne rozwiązanie kongruencji (1) dla modułu złożonego n jest co najmniej tak trudne, jak rozkład n na czynniki pierwsze. Natomiast samo tylko rozstrzygnięcie, czy (1) ma rozwiązanie, wydaje się istotnie łatwiejsze niż rozkład na czynniki, ale jak już wspomnieliśmy wcześniej, nikt nie umie zrobić efektywnie nawet tego.



Rozwiązanie zadania F 966.

Zatrzymanie pojazdu następuje, gdy praca wykonana przez siły tarcia równa jest początkowej energii kinetycznej pojazdu:

$$\frac{mv_0^2}{2} = mgfs,$$

gdzie m oznacza masę pojazdu, g – przyspieszenie ziemskie, a s drogę przebytą do zatrzymania.

- a) Gdy prędkość początkowa v_1 jest większa od v_0 , to podczas hamowania na drodze s energia kinetyczna zmaleje o wartość odpowiadającą prędkości v_0 i po przebyciu drogi s pojazd będzie poruszał się z prędkością

$$v = \sqrt{v_1^2 - v_0^2}.$$

Dla $v_1 = 60$ km/godz. i

$v_0 = 50$ km/godz., $v = 33,17$ km/godz.

- b) W przypadku mokrej nawierzchni pojazd podczas hamowania na drodze s straci tylko f_1/f_0 część swojej energii kinetycznej. Jego prędkość po przybyciu drogi s wyniesie więc:

$$v = v_0 \sqrt{1 - \frac{f_1}{f_0}}.$$

Dla $v_0 = 50$ km/godz., $f_1 = 0,4$ i $f_0 = 0,6$, $v = 28,87$ km/godz.

„Co jest grane” w Teorii Gier

Tadeusz PŁATKOWSKI*

Teoria Gier (TG), traktowana jako dział matematyki, służy do wyjaśniania zachowań ludzi, zwierząt, przebiegu różnorodnych procesów w przyrodzie, ekonomii, medycynie, zachowania podmiotów w polityce, w sieciach społecznych, czyli – ogólniej – służy do opisu interakcji między różnego typu obiektami. Procesy te są na tyle złożone, że istniejące modele teoriogrowe nie przystają na ogół do obserwowanych sytuacji. Przykładem jest *równowaga Nasha*, która stanowi matematyczny opis stabilnego układu. Jednak w rzeczywistych sytuacjach ludzie nieczęsto grają strategiami tworzącymi taką równowagę. Jednym z największych wyzwań TG jest stworzenie modeli zachowań, które w zadowalającym stopniu są zgodne z obserwacjami, mają odpowiedni potencjał predykcyjny oraz możliwości testowania. Rozbieżności ilustruje np. gra „Ultimatum”. W jednym z wariantów gracz otrzymuje pewną kwotę i musi zaproponować wybraną przez siebie jej dodatnią część drugiemu graczowi. Jeżeli ten ją przyjmie, następuje podział, jeżeli nie, to obaj nic nie dostają. W przypadku skończonej liczby propozycji równowaga (zwana doskonałą) polega na tym, że pierwszy gracz proponuje najniższą możliwą kwotę, drugi zgadza się na wszystko (zawsze jest to dla niego opłacalne). Przeprowadzone eksperymenty pokazały, że proponowana suma była istotnie wyższa od najniższej możliwej. Znaczące rozbieżności między teorią a eksperymentami obserwuje się także w sytuacjach modelowanych innymi klasycznymi grami, np. w grze „W Stonogę”, czy w „Dylemacie Więźnia”.

Jest wiele powodów, dla których opis równowagowy nie przystaje do rzeczywistości, np. ograniczona racjonalność decydentów, niepewność dotycząca wypłat w grze, uwzględnianie przez graczy nie tylko swojego wyniku, ale też wyników innych uczestników gry; ponadto gracze mogą popełniać błędy, mogą być motywowani altruizmem, intuicją, wiarą, różnorodnymi emocjami, takimi jak zawiść, złośliwość, strach przed ryzykiem, a w przypadku gier powtarzalnych np. strachem przed odwzajemnianiem, czy troską o swoją reputację. Co więcej, zmiana wypłat, która nie zmienia równowag Nasha, może powodować istotne zmiany w decyzjach graczy. I odwrotnie, istotna zmiana wypłat może nie wpływać na ich decyzje. Mimo powyższych i innych ograniczeń równowaga Nasha (jak i inne koncepcje równowagi, np. *równowaga Bayesa-Nasha*, *równowaga korelacyjna*) jest użytecznym pojęciem, będącym obiektem intensywnych badań, np. w *grach dynamicznych*, *stochastycznych* oraz w *algorytmicznej teorii gier*, w której otwartym problemem jest opracowanie i implementacja przyjaznych obliczeniowo algorytmów wyznaczania równowag (lub stanów im bliskich) dla układów złożonych z bardzo wielu oddziałujących między sobą obiektów. Problemy takie mają bardzo często wysoką złożoność obliczeniową i występują zarówno w *grach strategicznych* (np. przy wyznaczaniu równowag Nasha), jak i w *grach koalicyjnych* (w których jedno z najbardziej popularnych rozwiązań, *wartość Shapleya*, wymaga uwzględnienia wszystkich podzbiorów zbioru graczy, co w przypadku wielkich układów przekracza obecne możliwości obliczeniowe). Coraz częściej TG jest używana do konstrukcji i analizy modeli wieloagentowych, do opisu aukcji lub szerzej: do projektowania mechanizmów (*mechanism design*) i ogólniej do badań nad sztuczną inteligencją.

Popularnym powiedzeniem jest, że wiek XXI to „wiek sieci”. Teoria gier jest istotnym elementem opisu różnego typu sieci, np. społecznościowych i komunikacyjnych. Węzłami sieci są gracze, krawędzie opisują ich wzajemne interakcje. Gry na sieciach modelują zachowania w sieciach społecznych, rozchodzenie się plotek, powstawanie zatorów komunikacyjnych, ataki na sieci komputerowe, ataki terrorystyczne albo – odwracając rolę – próby rozbicia sieci terrorystycznych np. przez analizę znaczenia, siły oddziaływania członków grup terrorystycznych, tworzących strukturę sieciową (Δ_{16}^1).

Powstanie i ewolucja Internetu były źródłem nowych modeli teoriogrowych i ciekawych problemów matematycznych. W 2003 roku został zaproponowany



model Internetu, w którym węzły sieci są graczami, krawędzie – połączeniami, a użyteczność gracza (w tym przypadku koszt połączeń) jest mierzona długością i liczbą połączeń z innymi graczami. Autorzy przeanalizowali istnienie i własności równowag Nasha, przedstawili listę otwartych problemów, z których do dziś tylko kilka doczekało się rozwiązania. Otwartym problemem jest w szczególności pytanie, czy istnieją i jakie mają własności procesy dynamiczne, prowadzące do równowag (w tym i w późniejszych modelach tworzenia sieci).

Ważnym typem modeli teoriogrowych, stosowanych do wyjaśniania rzeczywistych zachowań, są modele uczenia, w których gracze zmieniają strategie w zależności od wypłat swoich i innych graczy, prowadzące do równowagi Nasha, np. „Replikator” czy „Gra fikcyjna” (*fictitious play*). Jednakże, m.in. w wyniku rozwoju ekonomii eksperymentalnej i po uwzględnieniu osiągnięć psychologii, stało się jasne, że ludzie zachowują się inaczej, niż przewidują modele uczenia.

Jednym z intrygujących problemów, który do tej pory nie ma powszechnie akceptowanego rozwiązania, jest zagadnienie ewolucji kooperacji w grupach ludzkich, w których interakcje są opisywane formalizmem TG. Najczęściej stosowanymi modelami takich sytuacji są *dylematy społeczne*, w szczególności „Dylemat Więźnia” i (w przypadku wielu graczy) „Dylemat Wspólnych Zasobów”. Można przewidywać, że nowe modele będą w szerszym stopniu uwzględniały wzmiankowane wyżej aspekty behawioralne i neurobiologiczne takich interakcji.

Czytelnikowi pragnącemu rozszerzyć swoją wiedzę w obszarze problemów otwartych TG polecamy:

- [1] A. Fabrikant et al., *On a network creation game*, PODC '03 (2003) 347-351;
- [2] N. Nisan, T. Roughgarden, E. Tardos, V.V. Vazirani, *Algorithmic Game Theory*, (2007) Cambridge;
- [3] Y. Shoham, K. Leyton-Brown, *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations*, (2008) Cambridge Univ. Press;
- [4] E. Elkind, K. Leyton-Brown, *Algorithmic Game Theory and Artificial Intelligence*, AI Magazine, 31, 4 (2010);
- [5] M. Shubik, *The Present and Future of Game Theory*, Discussion Paper 1808 (2011);
- [6] V. Fragnelli, G. Gambarelli, *Open problems in the theory of cooperative games*, IGTR, 15 2, 3 (2013);
- [7] M.O. Jackson, Y. Zenou, *Games on Networks, Handbook of Game Theory with Economic Applications* (2015) Elsevier;
- [8] E. Maskin, *How Can Cooperative Game Theory Be Made More Relevant to Economics?* Open Problems in Mathematics, J.F. Nash, Jr., M.Th. Rassias (eds.), Springer Int. Publ. (2016).

Mnożenie nie tylko macierzy

Marcin MUCHA*

*Instytut Informatyki, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Tematem tego artykułu jest mnożenie macierzy, ale zaczniemy od problemu nieco prostszego – mnożenia wielomianów. Niech A i B będą wielomianami stopnia n , $A(x) = \sum_{i=0}^n a_i x^i$, $B(x) = \sum_{i=0}^n b_i x^i$. Iloczynem A i B jest wielomian $C(x) = \sum_{i=0}^{2n} c_i x^i$, gdzie $c_i = \sum_{0 \leq k \leq i} a_k b_{i-k}$ (przyjmujemy $a_k = b_k = 0$ dla $k > n$).

Mnożenie wielomianów za pomocą tego wzoru wymaga rzędu n^2 operacji. Okazuje się jednak, że można to zrobić szybciej. Jako pierwszy zauważył to Anatolij Karatsuba już w 1960 roku. Algorytm Karatsuby opiera się na następującym spostrzeżeniu. Rozważmy iloczyn wielomianów szczególnie prostej postaci:

$$(a_n x^n + a_0)(b_n x^n + b_0) = a_n b_n x^{2n} + (a_n b_0 + b_n a_0) x^n + a_0 b_0.$$

Wydaje się, że do obliczenia współczynników wyniku potrzebne są cztery mnożenia, ale wystarczą trzy, gdyż

$$a_n b_0 + b_n a_0 = (a_0 + a_n)(b_0 + b_n) - a_0 b_0 - a_n b_n.$$

W ogólnym przypadku, aby pomnożyć dwa wielomiany A, B stopnia $2n - 1$, zapisujemy A następująco:

$$A(x) = \sum_{0 \leq i < n} a_i x^i + x^n \left(\sum_{0 \leq i < n} a_{i+n} x^i \right),$$

i analogicznie B , a następnie korzystamy z wyprowadzonej właśnie tożsamości. Sprowadzamy w ten sposób jedno mnożenie wielomianów stopnia $2n - 1$ do

Co ciekawe, sztuczka zmniejszania liczby mnożeń była znana już Gaussowi, który używał jej do mnożenia liczb zespolonych za pomocą trzech mnożeń.

Pracujemy teraz z wielomianami, których współczynniki same są wielomianami. Zachęcamy Czytelnika do sprawdzenia, że nie prowadzi to do żadnych nieprzewidzianych trudności.

trzech mnożeń oraz dwóch odejmowań wielomianów stopnia $n - 1$. Proces ten można kontynuować rekurencyjnie. Liczbę operacji arytmetycznych, wykonywanych przez uzyskany w ten sposób algorytm, opisuje równanie $T(2n - 1) = 3T(n - 1) + O(n)$, którego rozwiązaniem jest $T(n - 1) = O(n^{\log_2 3})$, gdzie $\log_2 3 \approx 1,585$. Jeśli początkowe stopnie nie są postaci $2^k - 1$, należy je sztucznie zwiększyć, nie zmieniając rzędu liczby operacji.

Istnieją też inne efektywne algorytmy mnożenia wielomianów. Najszybszy z nich korzysta z szybkiej transformaty Fouriera i wymaga $O(n \log n)$ operacji arytmetycznych. Warto zwrócić uwagę, że algorytmów tych można używać także do mnożenia liczb, wstawiając za współczynniki wielomianów cyfry liczb, które chcemy pomnożyć. Poprawność tej procedury łatwo uzasadnić – wystarczy podstawić za x bazę systemu, w którym liczymy, np. $x = 10$. Zarówno algorytm Karatsuby, jak i inne szybkie algorytmy mnożenia liczb/wielomianów są używane w praktyce. Wiele bibliotek implementuje kilka różnych algorytmów i wybiera właściwy w zależności od rozmiaru mnożonych liczb.

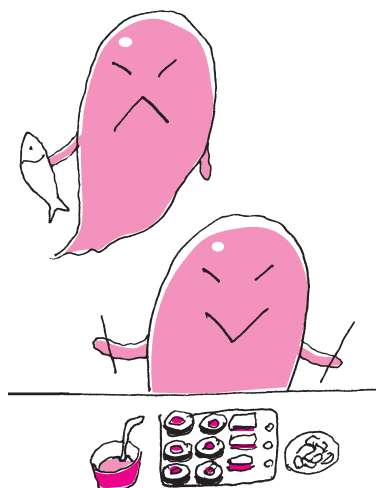
Przejdźmy teraz do głównego tematu tego artykułu, czyli mnożenia macierzy. Niech A i B będą macierzami $n \times n$, $A = (a_{i,j})$, $B = (b_{i,j})$. Iloczynem A i B jest macierz $C = (c_{i,j})$, gdzie $c_{i,j} = \sum_{k=1}^n a_{i,k} b_{k,j}$. Jak łatwo sprawdzić, mnożenie macierzy za pomocą tej definicji wymaga rzędu n^3 operacji. W 1969 roku Strassen zadziwił świat naukowy odkryciem algorytmu, który mnoży macierze za pomocą $O(n^{\log_2 7})$ operacji, gdzie $\log_2 7 \approx 2,81$. Algorytm ten opiera się na pomysłe podobnym do algorytmu Karatsuby. Strassen znalazł mianowicie metodę mnożenia dwóch macierzy 2×2 za pomocą 7 mnożeń zamiast 8, które wykonuje algorytm naiwny. Aby móc zastosować algorytm Strassena rekurencyjnie, wystarczy zauważyć, że jeśli każdą z macierzy A , B oraz $C = AB$ podzielimy na cztery identycznych rozmiarów kwadratowe bloki, to zachodzi:

$$\begin{pmatrix} C_{1,1} & C_{1,2} \\ C_{2,1} & C_{2,2} \end{pmatrix} = \begin{pmatrix} A_{1,1}B_{1,1} + A_{1,2}B_{2,1} & A_{1,1}B_{1,2} + A_{1,2}B_{2,2} \\ A_{2,1}B_{1,1} + A_{2,2}B_{2,1} & A_{2,1}B_{1,2} + A_{2,2}B_{2,2} \end{pmatrix}.$$

Oznacza to, że można takie macierze blokowe mnożyć tak, jakby bloki były liczbami. W połączeniu ze sztuczką Strassena pozwala to zredukować mnożenie macierzy $(2n) \times (2n)$ do 7 mnożeń macierzy $n \times n$ i pewnej, zupełnie nieistotnej, liczby dodawań takich macierzy. Złożoność uzyskanego w efekcie algorytmu rekurencyjnego opisuje równanie $T(2n) = 7T(n) + O(n^2)$, którego rozwiązaniem jest wspomniana wcześniej złożoność $T(n) = O(n^{\log_2 7})$.

Po odkryciu Strassena sądzono, że znalezienie algorytmu o złożoności $O(n^2 \log n)$ lub podobnej jest tylko kwestią czasu. Stało się jednak inaczej. Przez kolejnych dwadzieścia lat rozwinięto niezwykle wyrafinowaną metodologię konstrukcji algorytmów mnożenia macierzy, wyrażoną w języku algebry tensorowej. W ramach tej teorii zaproponowano wiele algorytmów mnożenia macierzy, najszybszym z nich jest opublikowany w roku 1980 algorytm Coppersmitha i Winograda o złożoności $O(n^{2,38})$. Od tamtego czasu powstały nowe, dużo bardziej eleganckie teorie, m.in. interpretacja znanych algorytmów w języku działań grup. Parametry algorytmu Coppersmitha i Winograda zostały też zoptymalizowane, w efekcie uzyskano złożoność $O(n^{2,37})$. Pytanie o algorytm o złożoności niemal kwadratowej pozostaje nadal jednym z najbardziej fundamentalnych otwartych problemów algorytmiki.

Nie jest to jednak jedyny otwarty problem związany z mnożeniem macierzy. Mnożenie macierzy jest niezwykle często wykorzystywane w praktyce, choćby w implementacji warstw gęstych w tak ostatnio popularnych sieciach neuronowych. Pomimo to żadna z popularnych zoptymalizowanych implementacji nie korzysta z omawianych tu algorytmów. Powody ku temu są dwa. W przypadku najszybszych asymptotycznie algorytmów stała ukryta w notacji dużego O ma monstrualne rozmiary, przez co są one bezużyteczne w praktyce. Z kolei w przypadku wolniejszych asymptotycznie algorytmów, np. algorytmu Strassena, rekurencyjna struktura utrudnia efektywne zarządzanie pamięcią podręczną procesora (cache), które jest kluczowym elementem efektywnych implementacji. Czy istnieją naprawdę szybkie algorytmy mnożenia macierzy?



Zaciemnianie programów

Tomasz KAZANA

Każdy młody adept sztuki programowania pewnie nie raz słyszał od swych mentorów, że program nie tylko musi działać poprawnie i szybko, ale też musi być napisany w sposób czytelny. Studentów uczy się więc nie tylko języków programowania, algorytmów czy struktur danych, ale też próbuje się im przekazać prawidłowe nawyki dotyczące *stylu* programowania.

Buntownicy, jak zawsze, idą w drugą stronę. Od roku 1984 organizowany jest konkurs *International Obfuscated C Code Contest* na napisanie możliwie nieczytelnego programu w języku C. Na marginesie umieściliśmy zgłoszenie Nicolasa Ollingera, które w roku 2001 (ex aequo z Jasonem Orendorffem) zdobyło główną nagrodę. Czytelnik Chorobliwie Zawzięty może sprawdzić, że ten program realizuje działanie siła Eratostenesa.

Problem zaciemniania programów jednak wybiega daleko poza obszar sztubackich żartów.

Zaciemnianie (fachowo: obfuskacja) kodu źródłowego programu to jedno z ważnych wyzwań kryptologii. Motywacja do badania tego problemu jest chyba dość jasna. Dla zapewnienia bezpieczeństwa danych (albo z powodów czysto biznesowych) czasem autor programu chce tylko umożliwić jego wykonywanie komuś innemu, ale wcale nie chce ujawniać szczegółów jego działania. W dobie Internetu takie założenie trywialnie można zrealizować w modelu klient-serwer. Wystarczy założyć, że kod pewnego programu P znany jest tylko serwerowi, a jeśli użytkownik chce wykonać P na danych D , to powinien wysłać D do serwera, a ten obliczy i odeśle mu $P(D)$. Problem obfuskacji jest jednak trudniejszy. Chcemy mieć własność jak wyżej, ale w świecie *off-line*. Innymi słowy: zakładamy, że użytkownik przechowuje sam kod programu P , a i tak najlepsze, co może zrobić, by poznać jego działanie, to uruchamiać P na różnych danych i odczytywać wyniki. Chcielibyśmy, aby kod był tak zagmatwany, żeby każda próba jego obejrzenia i wyciągnięcia jakichś bardziej ogólnych wniosków musiała kończyć się niepowodzeniem.

```
1 #define n ((e[+a]-42)/(9-f[d+1])?
2 #define o printf("%c",c[\" 01./:\\\"]);
3 char e[]=\"*3<HRZcir+300kakt;=QXds*\?HRZcir*7HNZ'i19JS\\p*H[m1:CJSz*>H['mr25\
4 \\?Hx,P,B2Gs-?KfzRdviIseyCR-ISeu.<Evr+9+P,z.4PfizIdv0?HRZcir6GPis=Mu*3HRZcir*HZi
5 1JS\\vpy*?H[m1Jsey*DH[*3&Ziu-@*3HZiu-@*3HZiu-<q]qJJS\\vpy:[m1CJSeny06I[m*4?HRZcir,\\
6 \\?*6HRZcir1J]q2K*H[m2K*H[m20K]qt0@WZDK]q,]q1JS\\vpy[m1:Jsey+ [m*3<HRZcir13ct,\\
7 =Gvs*3<HRZcir1J]qz*HF*AHZ;D&K]qua0=02:K]q]q1CJS\\vpy[m1:JS&D;+3:BIOSY'eg1lqtz&\\
8 \\177.0249<==EJMUY'ejov#8590CJOXZbfhlnrxy&+.57=@IMR['.'bcfmmq!#),@\" ,*f,
9
10 int main(int j,char *k[]) {
11     int a,b,c,d,g,h,i=19;
12     printf(\" \");
13     for(g=0|f=(char *)calloc(80+(h=atoi(1[k])),1)]i=1; g<=h; g++) {
14         if ((g>30)&&(f[i-2]+f[i-1]=0)) i++;
15         for(d=c=0; d<i; d++) {
16             o f[d]=(e[b=c*9,b+=c=d{f}],((a=(a+345+b)+b/19*85-33-b/40*12-b/80*4) [e
17 -42)/(9-f[d+1])?n n n n n 0:a:a:a:a:a:a:a:a] :42)%; }
18             o if (0|f[i-1]) printf(\"\\n/6i \",g); else printf(\"\\n \"); } }
```

Jak w całej kryptologii, początkowo do problemu zaciemniania kodu podchodzono w sposób nieformalny (czy raczej: niematematyczny). To znaczy definicje problemu były nieostre, a rozwiązania dyskutowane były wyłącznie na poziomie intuicyjno-inżynierskim. Sprawę zmieniła słynna prorocza praca *New Directions in Cryptography* Diffiego i Hellmana z roku 1976, w której (między innymi) podjęto próbę sformalizowania pojęcia obfuskacji programu. Konkretnie: niech $O(P)$ oznacza próbę zaciemnienia programu P . Powiemy, że $O(P)$ jest rzeczywiście obfuskacją P , gdy (1) dla każdego wejścia, P oraz $O(P)$ dają ten sam wynik oraz (2) dla każdego (wielomianowego) użytkownika A istnieje taki symulator S (czyli po prostu pewien wielomianowy program), że:

$$A(O(P)) \approx S^P,$$

gdzie: $A(O(P))$ oznacza wynik działania A na danym kodzie $O(P)$, a S^P oznacza wynik działania S , który ma dostęp do serwera takiego, jak w akapicie wyżej (czyli obliczającego na żądanie wartości programu P). Wyniki programów nie muszą być deterministyczne, stąd znaczek „ \approx ” oznacza tutaj bliskość rozkładów możliwych wyników. Intuicyjnie ta definicja głosi, że użytkownik A , który ma pełny dostęp do kodu $O(P)$, nie ma specjalnej przewagi nad użytkownikiem dysponującym tylko

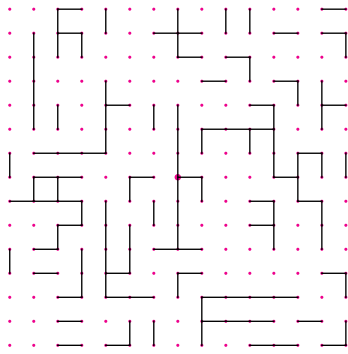
dostępem do serwera, skoro ten drugi może symulować (w czasie wielomianowym i z dużą dokładnością) wynik obliczeń tego pierwszego.

Marzeniem kryptologów przez wiele lat pozostawał uniwersalny kompilator, który dla każdego programu potrafiłby wyznaczyć jego nową wersję, zaciemnioną według definicji wyżej. Niestety, w roku 2001 Barak et al. udowodnili, że taka uniwersalna konstrukcja nie może istnieć. Na długi czas ostudziło to zapal środowiska. Jednak przełom pojawił się w roku 2013, gdy kolejna grupa badaczy, pracując ze słabszą wersją definicji obfuskacji (*indistinguishability obfuscation*, w skrócie iO), wskazała (bez dowodu) obiecującego kandydata na uniwersalny kompilator. Od tamtej pory ruszyła lawina. Znamy już wiele uniwersalnych kompilatorów iO, dowodliwie poprawnych przy różnych, mniej lub bardziej egzotycznych założeniach. Znamy też wiele zastosowań, pokazujących, że sama definicja (nieprezentowana w tym tekście) iO nie jest za słaba w praktyce. Wciąż jednak wiele bardzo ważnych pytań w tej dziedzinie pozostaje bez odpowiedzi. Przede wszystkim:

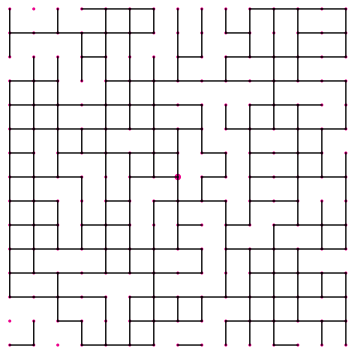
Czy istnieje uniwersalny kompilator zaciemniający (w sensie iO), poprawny przy standardowych założeniach (a więc np. o istnieniu funkcji jednokierunkowych)?

Perkolacje

Piotr MIŁOŚ*



Rys. 1. Woda płynie wzdłuż czarnych linii.



Rys. 2

Może być to zaskakujące, ale wiele problemów matematycznych łatwiej opisuje się w przypadku nieskończonym. Także dla perkolacji łatwiej jest je analizować na nieskończonym grafie.

$0 < p_c < 1$ dla dowolnej kraty \mathbb{Z}^d , $d \geq 2$. Dla małych p zbiory krawędzi otwartych są skończone, a dla p bliskich 1 istnieje (jeden) zbiór nieskończony.

Istotnie, w pierwszym kroku możemy wyjść w 4 kierunkach. Następnie w każdym kroku mamy do wyboru trzy kierunki dalszego podążania (cofanie nie wydłuża ścieżki).

W przypadku $p = 1/3$ to rozumowanie daje trywialne szacowanie $4/3$ na szansę połączenia środka z brzegiem. Symulacja komputerowa pokazuje, że dla $n = 7$ szansa ta wynosi około 8% (przykładowy rezultat takiej symulacji pokazany jest na pierwszym rysunku).

Wyobraźmy sobie porowaty materiał, może to być gleba, a może to być... ubita kawa w kawiarni. Czy przez ten materiał można przesączyć wodę? Intuicyjnie wiemy, że jest to możliwe w przypadku kawy, ale już w przypadku gleby zależy od jej rodzaju, a dokładniej – od struktury „porów wolnej przestrzeni”. W roku 1957 matematycy angielscy, Simon Broadbent i John Hammersley, zaproponowali probabilistyczny model opisujący materiały porowate. Pomimo prostoty definicji model ten (zwany *perkolacjami*) okazał się fascynującym tematem badań. Wspomnijmy, że, między innymi, za wyniki dotyczące perkolacji Stanisław Smirnow został nagrodzony w 2010 roku najwyższym matematycznym wyróżnieniem, Medalem Fieldsa.

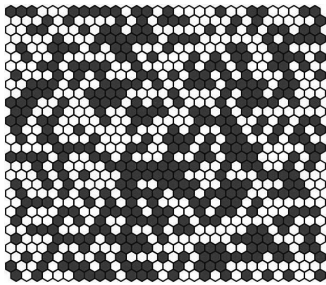
Czym jest perkolacja? Wyobraźmy sobie stronę zeszytu w kratkę. Każda jej krawędź może być otwarta („przepuszczająca wodę”) lub zamknięta („nieprzepuszczająca wody”). O otwarciu krawędzi decydujemy w sposób losowy, rzucając kostką sześcienną. Rozważmy dwa przypadki. W pierwszym z nich otwieramy krawędź, gdy na kostce wypadnie 1 lub 2. Rysunek 1 przedstawia przykładowy rezultat takiego losowego doświadczenia – jak widać, nie istnieje otwarta ścieżka z góry na dół, którą woda mogłaby przepłynąć. W drugim przypadku otwieramy krawędź, gdy na kostce wypadnie jedna z liczb 1, 2, 3, 4. Intuicyjnie łatwo stwierdzić, że szansa przepłynięcia wody gwałtownie rośnie, co ilustruje drugi rysunek. Wspomniani już Broadbent i Hammersley przekuli powyższe intuicje w abstrakcyjny model matematyczny. Rozważmy nieskończony graf regularny (może to być nieskończona kartka w kratkę, czyli graf \mathbb{Z}^2). Każdą z jego krawędzi otwieramy niezależnie z pewnym prawdopodobieństwem $p \in (0, 1)$. Kluczowe w teorii perkolacji jest pytanie „jakie jest prawdopodobieństwo, że krawędzie otwarte łączą się w nieskończony zbiór?”. Intuicyjnie jest oczywiste, że szansa ta zwiększa się wraz ze wzrostem p . Sugeruje to istnienie takiego prawdopodobieństwa krytycznego p_c , że dla $p < p_c$ nie ma nieskończonego zbioru otwartego (woda nie może przepływać), a dla $p > p_c$ taki zbiór ma szansę powstać. Jednym z pierwszych osiągnięć teorii perkolacji było pokazanie, że prawdopodobieństwo krytyczne dla \mathbb{Z}^2 jest nietrywialne, mianowicie, że $0 < p_c < 1$.

Pokażemy teraz szkic argumentu pokazującego, że dla \mathbb{Z}^2 mamy $p_c \geq 1/3$. Rozważmy kwadrat na kartce papieru o boku $2n + 1$, czyli zbiór $\{-n, -n + 1, \dots, n - 1, n\}^2$. Zastanówmy się, czy środek tego kwadratu jest połączony za pomocą krawędzi otwartych z jakimś punktem brzegu. Jeśli tak, to istnieje ścieżka o długości n złożona z krawędzi otwartych, zaczynająca się w $(0, 0)$ (np. będąca częścią ścieżki otwartej do brzegu). Zauważmy, że liczbę wszystkich ścieżek o długości n możemy oszacować przez $4 \cdot 3^{n-1}$. Szansa na to, że każda z krawędzi takiej ścieżki jest otwarta, wynosi p^n (korzystamy z założenia o niezależności). Jeden z podstawowych wyników teorii prawdopodobieństwa mówi, że szansa na otwarcie przynajmniej jednej ścieżki jest mniejsza niż suma prawdopodobieństw otwarcia poszczególnych ścieżek, co w naszym przypadku wynosi $\frac{4}{3} \cdot (3p)^n$. W ostatnim kroku obserwujemy, że liczba ta jest bardzo mała, gdy $p < 1/3$, a n jest duże. W związku z tym łatwo uwierzyć (a także matematycznie wykazać), że każdy z połączonych zbiorów krawędzi otwartych będzie wtedy skończony. Nasze rozważania pokazują zatem, że $p_c \geq 1/3$.

Podobny, choć trudniejszy, argument pokazuje, że dla p bliskich jedynki nieskończony zbiór otwarty zawierający $(0, 0)$ ma szansę powstać. Zachęcamy Czytelnika do próby uzasadnienia tego faktu. Kluczową obserwacją jest to, że jeśli zbiór jest skończony, to istnieje „pętla” otaczająca $(0, 0)$, przecinająca jedynie zamknięte krawędzie.

Główną trudnością w analizie perkolacji są nietrywialne zależności geometryczne. Jednocześnie są one źródłem wielu ciekawych fenomenów sprawiających, że

*Instytut Matematyki, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski



Przykład perkolacji na plastrze miodu. Woda płynie przez pola ciemne.

perkolacje są interesującym modelem. W naszej analizie badaliśmy „oddzielnie” ścieżki długości n , tymczasem wiele z nich się pokrywa. Mimo że przedstawione argumenty można poprawić, uzyskanie wartości p_c wymagało znacznie bardziej zaawansowanych metod, których opracowanie trwało 20 lat i zostało uwieńczone dowodem Harrego Kestena pokazującym, że $p_c = 1/2$.

Uzyskanie dokładnych wartości prawdopodobieństwa krytycznego dla innych grafów często jest niemożliwe. Zaskakująco nie przeszkadza to w badaniu zachowania perkolacji w punkcie krytycznym. Jest to najbardziej aktywne pole rozwoju teorii (te zagadnienia były badane przez Smirnowa). Mimo że wykazano to ściśle w małej ilości przypadków, spodziewamy się, że zachowanie w dużej skali w tym punkcie zależy głównie od wymiaru grafu (na przykład zachowanie perkolacji na „kartce w kratkę” będzie podobne jak na „plastrze miodu”). Fenomen ten, zwany uniwersalnością, jest przedmiotem intensywnych badań, poprzez swoje związki z innymi dziedzinami matematyki. Zapewne w najbliższych latach doprowadzi do nowych fascynujących wyników.

Interpretacje teorii kwantów

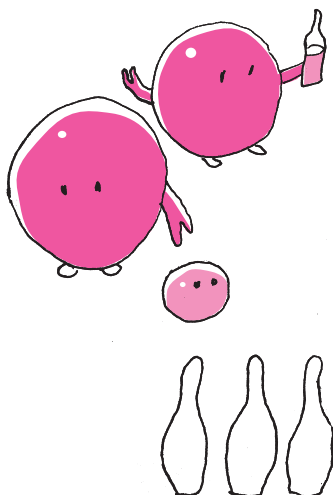
Jan CHWEDEŃCZUK*

*Instytut Fizyki Teoretycznej, Wydział Fizyki, Uniwersytet Warszawski

Drobne pęknięcia fundamentów mechaniki klasycznej i klasycznej elektrodynamiki, które objawiły się w drugiej połowie XIX wieku, doprowadziły do niewyobrażalnego przełomu naukowego i technologicznego. Narodziła się mechanika kwantowa, a opowieść o jej sformułowaniu i zaprzęgnięciu do realizacji naszych potrzeb to historia triumfu ludzkiego umysłu – narządu, który pierwotnie służył przede wszystkim do gonienia mamuta. Trudno wymienić wszystkie korzyści, jakie na co dzień czerpiemy ze znajomości tej teorii. Układy scalone w każdym komputerze czy telefonie komórkowym oparte są na tranzystorach półprzewodnikowych, których konstrukcja wymaga znajomości kwantowej teorii ciała stałego. Tenże telefon prawdopodobnie umożliwia komunikację w ramach systemu GPS, który działa dzięki precyzyjnej znajomości jednostki czasu. Kiedyś sekundę definiowało się jako ułamek doby ziemskiej, współczesna sekunda to 9 192 631 770 okresów oscylacji elektronu w wyniku przejścia między dwoma poziomami energetycznymi w atomie cezu 133 [1]. W przyszłości jednostka czasu oparta będzie na jeszcze bardziej egzotycznym zjawisku kwantowym – okresowy sygnał pochodzić będzie od przejścia między dwoma poziomami energetycznymi w samym jądrze atomowym, tym razem atomu toru 229 [2]. Oscylacje takie wzbudza się laserem, który stanowi jeszcze jeden przykład spożytkowania zjawisk kwantowych. Laser znajduje zastosowanie w medycynie, odtwarzaczach płyt CD czy w laboratoriach badawczych. Wszystko wskazuje na to, że najbliższe lata przyniosą rozkwit technologii kwantowych, o ile tylko globalny konflikt bądź dramatyczne zmiany klimatyczne nie zahamują rozwoju cywilizacyjnego. Grafen, fuzja jądrowa, czy nano-technologie – przyszłość rysuje się kwantowo.

Oprócz zastosowań technologicznych ważny jest filozoficzny aspekt teorii kwantów i jej wpływ na nasze rozumienie otaczającego świata. W klasycznym ujęciu cząstka (na przykład elektron albo piłka tenisowa) porusza się po trajektorii zdeterminowanej przez działające nań siły. Mechanika kwantowa nie dopuszcza istnienia dokładnie określonych trajektorii. W zamian opisuje cząstki za pomocą funkcji falowej, która pozwala na „współistnienie” wielu położeń i pędów naraz. To tak, jakby rysować tor cząstki na kartce grubym flamastrem, a nie cienkopisem. Teoria kwantów określa, jak gruba jest kreska i po jakiej krzywej podąża, ale nie dopuszcza, by flamaster był nieskończenie cienki, jak to ma miejsce w przypadku klasycznym.

Skoro funkcja falowa jest „rozmyta”, to można by przyjąć, że mechanika kwantowa przewiduje, że cząstka jest w wielu miejscach naraz. I tu zaczynają się schody – albowiem takie stwierdzenie jest jawnie sprzeczne z wynikami obserwacji empirycznych. Ilekroć bowiem spojrzymy na obiekt fizyczny, jest on dobrze zlokalizowany w przestrzeni. Innymi słowy, elektron jest punkcikiem



zarejestrowanym przez detektor, a nie rozmytą obszerną plamą czy zbiorem rozsianych punktów. Stąd wniosek o fundamentalnym znaczeniu – zdaje się, że obserwator nie ma dostępu do funkcji falowej. A skoro tak, to jak rozumieć ten obiekt matematyczny?

Z pomocą przychodzą *interpretacje* mechaniki kwantowej [3]. Wśród nich prym wiodzie interpretacja kopenhaska [4], sformułowana w latach dwudziestych XX w. przez Nielsa Bohra i Wernera Heisenberga. Mówi ona, że funkcja falowa określa prawdopodobieństwo, z jakim można znaleźć cząstkę w danym miejscu i chwili czasu. Stąd jej rozmyty kształt, gdyż prawdopodobieństwo, w odróżnieniu od dobrze określonej trajektorii, może rozciągać się na całe obszary. Każdy akt obserwacji prowadzi do „kolapsu funkcji falowej” – cząstka lokalizuje się w pewnym punkcie. To, gdzie ją znajdziemy, jest zupełnie przypadkowe. Możemy jedynie określić, znając funkcję falową, z jakim prawdopodobieństwem wypadnie dany wynik.

Zauważmy, że w ramach tej interpretacji mechaniki kwantowej funkcja falowa nie opisuje realnego świata fizycznego, lecz jedynie dostarcza prawdopodobieństw zdarzeń w tym świecie. Interpretacja kopenhaska nie odpowiada na pytanie, jaki jest świat, gdy nikt nie patrzy i kim jest obserwator. Niemniej to podejście do teorii kwantów daje doskonałą zgodność z doświadczeniem – funkcja falowa w pełni opisuje wszystkie statystyczne własności układów kwantowych. Ponadto jest to najpowszechniejsza, budząca najmniej kontrowersji i najczęściej nauczana interpretacja mechaniki kwantowej.

Literatura

- [1] *Base unit definitions: Second – NIST*.
- [2] Lars von der Wense et al. *Nature*, 533(7601):47, 2016.
- [3] Wikipedia, „*Interpretations of quantum mechanics*”.
- [4] Wikipedia, „*Copenhagen interpretation*”.
- [5] Wikipedia, „*Many-worlds interpretation*”.
- [6] Wikipedia, „*De Broglie–Bohm theory*”.

A może w wyniku pomiaru nie dochodzi do kolapsu funkcji falowej? Może obserwator widzi cząstkę we wszystkich możliwych konfiguracjach naraz? Mówimy, że tworzy on z badanym obiektem stan splątany – koreluje się z wszelkimi wynikami dopuszczanymi przez funkcję falową i wchodzi w stan superpozycji. Dlaczego zatem obserwator nie jest świadomy współistnienia wielu wyników pomiaru, lecz wręcz przeciwnie – ma wrażenie, jakby realizowała się tylko jedna możliwość? Zwolennicy tego podejścia do mechaniki kwantowej, zwanego interpretacją wielu światów [5], argumentują, że ciężko jest zaobserwować superpozycję dużych obiektów (detektorów czy patrzących ludzi), lecz gdybyśmy mieli taką możliwość, powinniśmy dostrzec kamerę „naraz” widzącą badany obiekt w różnych położeniach. Interpretacja wielu światów rozwinięta została przez Hugh Everetta w roku 1957, jej orędownikiem jest wybitny polski fizyk Wojciech Żurek, do tego grona należał Stephen Hawking.

Wielu fizyków i filozofów głowiło się nad teorią kwantów, stąd też mnogość jej interpretacji. Warto tu wspomnieć o koncepcji Louisa de Broglie’a i Davida Bohma (interpretacja bohmowska [6]), nadającej funkcji falowej element realności. Są też podejścia zahaczające o mistycyzm, łączące mechanikę kwantową z buddyzmem, a nawet z okultyzmem. Jakakolwiek jest prawda, jedno jest niewątpliwe: nie ma zgody co do tego, jak interpretować teorię kwantów – fundamentalną teorię mikroświata.

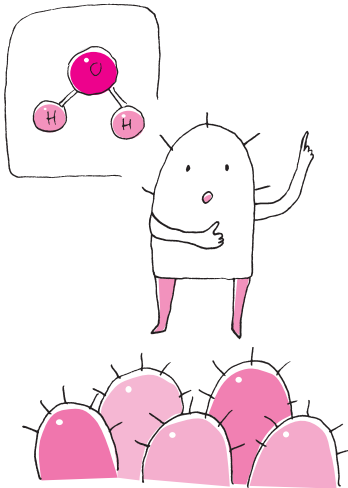
Rozróżnianie słów

Wojciech CZERWIŃSKI

Żeby przedstawić problem otwarty, o którym chcemy opowiedzieć, przypomnimy intuicję stojącą za pojęciem automatu skończonego, które zresztą niedawno pojawiło się w migawce informatycznej w *Delcie* 5/2018.

Deterministyczny automat skończony ma zbiór stanów Q , z których jeden jest początkowy, a niektóre są akceptujące. Taki automat czyta słowo wejściowe od lewej do prawej. Zaczyna przed pierwszą literą i jest wtedy w stanie początkowym. Następnie, w zależności od litery w słowie, którą aktualnie widzi i stanu, w którym jest, uaktualnia swój stan i przesuwa się w prawo po słowie. Jeśli po przeczytaniu ostatniej litery automat znajduje się w stanie akceptującym, to akceptuje słowo wejściowe, a w przeciwnym razie je odrzuca.

Przykładowo automat może akceptować słowa, których długość przystaje do 2 modulo 5. Wówczas naturalnym zbiorem stanów jest $Q = \{0, \dots, 4\}$, stan



początkowy to 0, a stan akceptujący jest tylko jeden, mianowicie 2. Automat, niezależnie od litery w słowie, przechodzi ze stanu q do stanu $(q + 1) \bmod 5$. Inny automat akceptuje słowa nad $\{a, b\}$, które na pozycjach przystających do 3 modulo 7 mają w sumie parzyste wiele liter a . Pamięta on, jaka jest reszta modulo 7 aktualnej pozycji oraz jaka jest parzystość liczby a , które do tej pory widział na interesujących go pozycjach. A zatem zbiór stanów to $Q = \{0, \dots, 7\} \times \{0, 1\}$. Stan początkowy to $(1, 0)$, bo zaczynamy od litery na pozycji 1 i bez zobaczonych a . Stany akceptujące to wszystkie postaci $(i, 0)$, gdyż akceptujemy, gdy liczba a na istotnych pozycjach jest parzysta, niezależnie od tego, jaka jest długość słowa. Jeśli automat widzi a w stanie $(3, c)$, to przechodzi do $(4, (c + 1) \bmod 2)$. W przeciwnym przypadku automat, niezależnie od tego, co widzi, przechodzi ze stanu (q, c) do $((q + 1) \bmod 7, c)$. Taki automat nazwiemy $\mathcal{A}_{3,7}$.

Możemy już sformułować problem rozróżniania słów. Pyta on, jakie jest takie minimalne $k \in \mathbb{N}$, że dla każdych dwóch różnych słów u, v o długości co najwyżej n istnieje automat o co najwyżej k stanach, który rozróżnia u i v , tj. jedno z nich akceptuje, a drugie odrzuca.

Zauważmy najpierw, że, oczywiście, istnieje pewien taki automat. Istotnie, łatwo skonstruować automat, który akceptuje tylko słowo u , a więc odrzuca v . A zatem pytanie o najmniejszy taki automat ma w ogóle sens. Powyższy automat ma jednak $|u| + 1$ stanów, czyli pesymistycznie $n + 1$. Problem rozróżniania słów został postawiony w 1986 roku przez Goralčika i Koubeka, którzy pokazali, że zawsze da się stworzyć automat wielkości $o(n)$.

Zauważmy najpierw, że rozróżnianie słów u i v różnej długości jest stosunkowo proste. Wtedy wystarczy, by automat obliczał długość słowa modulo pewna liczba wielkości $O(\log n)$. Nietrudno to udowodnić, a jeszcze prościej uwierzyć. Istotnie, aby $|u|$ i $|v|$ dawały te same reszty modulo wszystkie liczby $1, 2, \dots, k$, to liczba $|u| - |v|$ musi dzielić się przez NWW($1, 2, \dots, k$), co, jak dość łatwo wykazać, jest wykładnicze względem k . Zatem do rozróżnienia wystarczy k rzędu $\log n$. Okazuje się też, że jeśli umiemy rozróżniać słowa nad alfabetem dwuliterowym, powiedzmy $\{a, b\}$, to umiemy rozróżniać słowa nad dowolnym skończonym alfabetem automatami tej samej wielkości.

Niestety, dla słów u i v równej długości, nawet nad alfabetem $\{a, b\}$, nie jest już tak prosto. Najmocniejszy obecnie jest rezultat Robsona z 1989 roku, który pokazał, że dowolne dwa słowa da się rozróżnić pewnym automatem wielkości $O(n^{2/5}(\log n)^{3/5})$. Przy tym nie są znane pary słów, które rzeczywiście wymagają tak dużych automatów. Najtrudniejsze znane przykłady potrzebują jedynie automatów wielkości rzędu $\log n$. A więc wciąż możliwe jest, że każde dwa słowa, nawet tej samej długości, da się rozróżnić automatem wielkości $O(\log n)$.

Ciekawy jest trochę późniejszy wynik Robsona, z 1996 roku. Pokazał on, że każde dwa różne słowa równej długości nad alfabetem $\{a, b\}$ można rozróżnić automatem $\mathcal{A}_{d,m}$ dla $d, m = O(\sqrt{n})$, podobnym do przedstawionego wyżej $\mathcal{A}_{3,7}$. Akceptuje on słowa mające na pozycjach przystających do d modulo n parzyste wiele liter a . To daje ograniczenie $O(\sqrt{n})$, gorsze od $O(n^{2/5}(\log n)^{3/5})$, ale za to rozważane automaty są bardzo proste.

Od 1996 roku nie ma żadnych postępów w tej sprawie. Amerykański informatyk, pracujący teraz w Waterloo, Jeffrey Shallit, zaoferował w 2014 roku nagrodę 100 funtów brytyjskich każdemu, kto poprawi wynik Robsona z 1989 roku. Warto podkreślić, że rozróżnianie słów jest problemem zupełnie innego kalibru niż izomorfizm grafów i mnożenie macierzy. Moim zdaniem jest to problem potencjalnie w zasięgu pasjonata informatyki bez wielkiego doświadczenia w badaniach. Dodatkowo jest on elegancko sformułowany, jego rozwiązanie może przynieść nowe metody lub zrozumienie głębszych zagadnień, a luka między $O(n^{2/5}(\log n)^{3/5})$ a $\log n$ jest intrygująca. Dlatego zachęcam Czytelników Żądnych Wyzwań do przyjrzenia się sprawie.

Problem samotnego kolarza

Jarosław GRZYTCZUK*

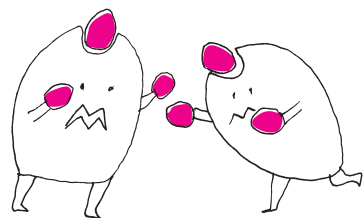
Na torze w kształcie okręgu o obwodzie jednostkowym ściga się n kolarzy. Każdy pędzi z inną, ale stałą prędkością. Wystartowali z tego samego punktu, jadą w tym samym kierunku. Jest ciemno, nic nie widać, choć oko wykol. Dlatego każdy kolarz ma w rowerze włączoną lampę przednią, która oświetla otwarty łuk toru długości $\frac{1}{n}$. Kolarz jest *samotny*, jeżeli w pewnej chwili nie widzi przed sobą nikogo ani nikt inny nie oświetla go z tyłu.

Hipoteza 1. *Każdy kolarz będzie kiedyś samotny.*

Tę melancholijną hipotezę postawił Jörg Michael Wills w roku 1967, w kontekście aproksymacji diofantycznych. Dla $n = 1$ jest ona trywialnie prawdziwa. Dla $n = 2$ jest niemal oczywista: w pewnym momencie dwaj kolarze pędzący z różnymi prędkościami muszą znaleźć się na końcach średnicy toru, wtedy obydwaj staną się samotni. Ale dla $n = 3$ zadanie nie jest już całkiem banalne (zachęcamy Czytelnika do przeprowadzenia ścisłego dowodu hipotezy). Do dzisiaj hipoteza została potwierdzona jeszcze dla $n = 4, 5, 6, 7$. Stopień komplikacji w kolejnych przypadkach rośnie, np. dowód hipotezy dla sześciu kolarzy rozciąga się na niemal pięćdziesięciu stronach wydruku.

Co tedy robić? George Pólya radzi: *Dla każdego problemu, którego nie potrafisz rozwiązać, istnieje łatwiejszy problem, którego też nie będziesz potrafił rozwiązać. Znajdź go.*

Może osłabić lampy w rowerach? Nietrudno dowieść, że przy lampach o zasięgu dwukrotnie mniejszym hipoteza jest prawdziwa. Najpierw zauważmy, że nie tracimy ogólności przy zmniejszeniu lub zwiększeniu wszystkich prędkości o tę samą wartość. Możemy zatem przyjąć, że jeden z kolarzy, dowolnie wybrany, pędzi z prędkością zero, czyli właściwie stoi w punkcie startu. Po wyzerowaniu wybranego kolarza mogą się pojawić kolarze z ujemnymi prędkościami, czyli jadący do tyłu. Tych należy zastąpić jadącymi w tym samym tempie do przodu. Zabieg ten nie ma znaczenia dla samotności stojącego kolarza.



To rozumowanie prowadzi do nieco innego, acz równoważnego sformułowania wyjściowego problemu. Przypuśćmy, że w punkcie startu kolarzy stoi lampa oświetlająca łuk otwarty o rozpiętości $\alpha > 0$. Kolarze jadą z prędkościami dodatnimi w tym samym kierunku. Lampy w rowerach są wygaszone. Czekamy na moment, w którym żadnego kolarza nie będzie w oświetlonym łuku. Przy założeniu, że ściga się n kolarzy i $\alpha = \frac{1}{n+1}$, Hipoteza 1 może być sformułowana w jeszcze bardziej posępny, ale równoważny, sposób.

Hipoteza 2. *Cały peleton zniknie kiedyś w ciemności.*

Obliczymy teraz, jak długo pojedynczy kolarz przebywa w oświetlonym łuku podczas całego wyścigu. Niech v będzie liczbą całkowitą dodatnią wyrażającą prędkość kolarza (nietrudno uzasadnić, że ograniczenie do liczb całkowitych nie zmniejsza ogólności zagadnienia). Przyjmijmy zatem, że kolarz pokonuje v okrążeń toru w jednostce czasu. Po jej upływie wszyscy kolarze znajdują się ponownie razem w punkcie startu. Możemy więc przyjąć, że wyścig kończy się w tym momencie, gdyż nic nowego na torze już się nie wydarzy. Zgodnie ze wzorem na drogę w ruchu jednostajnym czas przejazdu kolarza przez łuk długości 2α wynosi $\frac{2\alpha}{v}$. W ciągu całego wyścigu takich przejazdów jest dokładnie v , przy czym na jeden z nich składa się pierwszy i ostatni przejazd przez połowę świetlnego łuku. Stąd łączny czas przejazdu kolarza przez rejon światła to 2α . Wielkość ta jest niezależna od v , co nie jest chyba zaskakujące: szybszy kolarz szybciej mknie przez rejon światła, ale za to częściej weń wpada. Jeżeli przyjmijmy teraz, że $\alpha = \frac{1}{2n}$, to widzimy, że całkowity czas, w którym przynajmniej jeden kolarz był w łuku

świetlnym, wynosi co najwyżej 1. W rzeczywistości nie może być on równy 1, gdyż początkowo wszyscy kolarze są w pobliżu lampy. Musi zatem istnieć moment, w którym cały peleton zginie w gęstym mroku.

Wyobraźmy sobie teraz, że możemy regulować moc lampy, zwiększając stopniowo jej zasięg, począwszy od rozpiętości $\alpha = \frac{1}{2n}$. Zjawisko znikania peletonu w mroku będzie zapewne zachodzić przy delikatnym zwiększeniu mocy, ale pytanie jak długo? Hipoteza 2 mówi, że aż do $\alpha = \frac{1}{n+1}$. Tej ostatniej granicy nie da się już przekroczyć, co widać na przykładzie n kolarzy jadących z prędkościami $1, 2, \dots, n$. Jak dotąd, nikomu nie tylko nie udało się zbliżyć do hipotetycznej granicy, ale wręcz znacząco oddalić się od początkowej rozpiętości $\alpha = \frac{1}{2n}$. Nie wiadomo nawet tego, czy Hipoteza 2 zachodzi przy $\alpha = \frac{1}{(2-\epsilon)n}$ dla jakiegokolwiek $\epsilon > 0$. Najlepszy obecnie rezultat, należący do Terrenca Tao, potwierdza ją jedynie dla dostatecznie dużych n przy $\alpha = \frac{1}{2n} + \frac{c \log n}{(n \log \log n)^2}$, gdzie c jest stałą dodatnią. Inną prostą konsekwencją powyższych dywagacji jest taki oto dziwny fakt. Jak wykazaliśmy, całkowity czas pobytu każdego kolarza w rejonie światła wynosi 2α , niezależnie od jego prędkości. Składa się on z rozłącznych odcinków czasowych. Jeżeli $\alpha = \frac{1}{n+1}$, to suma długości wszystkich tych odcinków wynosi $\frac{2n}{n+1} < 2$. Co to znaczy? Pokolorujmy odcinki czasowe każdego kolarza innym kolorem, powiedzmy, kolorem jego koszulki. Mamy więc kolekcję odcinków w n kolorach pokrywających jakoś jednostkowy przedział czasu. Całkowita suma ich długości jest mniejsza od 2. Musi zatem istnieć punkt pokryty co najwyżej jednym kolorem. Jest to punkt w czasie, w którym co najwyżej jeden kolarz znajduje się w rejonie światła. Udowodniliśmy w ten sposób następujące twierdzenie.

Twierdzenie 1. *W każdym peletonie istnieje kolarz, którego dyskwalifikacja gwarantuje zniknięcie pozostałych kolarzy w mroku.*

Niestety, nie wiemy, który to kolarz. Gdyby teza twierdzenia zachodziła dla dowolnie wybranego kolarza, oznaczałoby to, że Hipoteza 2 jest prawdziwa przy $\alpha = \frac{1}{n+2}$, co w porównaniu ze wspomnianym rezultatem Tao byłoby zaiste rewelacją. Powyższe twierdzenie skłania do następującego osłabienia Hipotezy 1, o które zapytał Joel Spencer.

Hipoteza 3. *W każdym peletonie istnieje kolarz, który będzie kiedyś samotny.*

Jest rzeczą zadziwiającą, że mimo tak znacznego osłabienia tezy, wszak zamieniliśmy kwantyfikator ogólny na egzystencjalny, niczego istotnego nie udało się udowodnić.

Na koniec przedstawimy jednak pewien nieprawdopodobny wynik, który budzi nadzieję na ostateczne zwycięstwo. Rozważmy sytuację, w której prędkości kolarzy wybieramy losowo ze zbioru $\{1, 2, \dots, N\}$. Niech P_N oznacza prawdopodobieństwo, że taki losowy peleton spełnia Hipotezę 2.

Jeżeli jest ona prawdziwa, to, oczywiście, $P_N = 1$ dla każdego $N \geq n$. Powiemy, że Hipoteza 2 jest *prawie na pewno* prawdziwa, jeżeli $\lim_{N \rightarrow \infty} P_N = 1$.

Poniższe twierdzenie, udowodnione przez Sebastiana Czerwińskiego, pokazuje, że dużo silniejsza wersja Hipotezy 2 jest prawie na pewno prawdziwa.

Twierdzenie 2. *Losowy peleton prawie na pewno zniknie w ciemności, nawet jeżeli prawie cały tor jest oświetlony.*

Mamy tu na myśli, że Hipoteza 2 jest prawie na pewno prawdziwa przy $\alpha = \frac{1}{2} - \epsilon$, dla każdego $\epsilon > 0$. Twierdzenie to wzmocnił i uogólnił Noga Alon, upraszczając przy okazji dowód Czerwińskiego. Udowodnił on, że dowolnie wybrani kolarze losowego peletonu znajdą się w pewnej chwili dowolnie blisko dowolnie wybranych punktów toru.

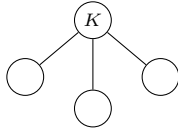
- [1] N. Alon, *The chromatic number of random Cayley graphs*, European J. Combin. 34 (2013), no. 8, 1232–1243.
- [2] J. Barajas, O. Serra, *The lonely runner with seven runners*, Electron. J. Combin. 15 (2008), R48, 18 pp.
- [3] W. Bienia, L. Goddyn, P. Gvozdzjak, A. Sebö, M. Tarsi, *Flows, view obstructions and the lonely runner*, J. Combin. Theory Ser. B 72 (1998), 1–9.
- [4] T. Bohman, R. Holzman, D. Kleitman, *Six lonely runners*, In honor of Aviezri Fraenkel on the occasion of his 70th birthday, Electron. J. Combin. 8 (2001), no. 2, Research Paper 3, 49 pp.
- [5] S. Czerwiński, *Random runners are very lonely*, Journal of Combinatorial Theory, Series A 119 (2012), no. 6, 1194–1199.
- [6] S. Czerwiński, J. Grytczuk, *Invisible runners in finite fields*, Inform. Process. Lett. 108 (2008) 64–67.
- [7] G. Perarnau, O. Serra, *Correlation among runners and some results on the lonely runner conjecture*, Electron. J. Combin. 23 (2016), no. 1, Paper 1.50, 22 pp.
- [8] T. Tao, *Some remarks on the lonely runner conjecture*, arXiv:1701.02048.
- [9] J.M. Wills, *Zwei Sätze über inhomogene diophantische Approximation von Irrationalzahlen*, Monatsch. Math. 71 (1967), 263–269.

Informatyczny kącik olimpijski (122): Zalesianie

Tym razem omówimy zadanie *Zalesianie*, które pojawiło się na finale zawodów drużynowych *XII Olimpiady Informatycznej Gimnazjalistów*.

Zalesianie: Danych jest n wierzchołków ponumerowanych od 1 do n . Ciąg $a = (a_1, a_2, \dots, a_n)$ składa się z wartości przyporządkowanych kolejnym wierzchołkom (a_i to wartość przyporządkowana i -temu wierzchołkowi). Naszym zadaniem jest zbudować drzewo (spójny, acykliczny graf), przez ustalenie $n - 1$ krawędzi między wierzchołkami oraz wybranie wierzchołka, który będzie korzeniem. Chcemy to zrobić w taki sposób, aby zminimalizować współczynnik niezadowolenia. Współczynnik niezadowolenia to maksymalna wartość wyrażenia $a_u \oplus a_v$, dla takich u i v , że u jest przodkiem v (\oplus oznacza operację bitową xor).

Zastanówmy się najpierw nad strukturą drzewa, które budujemy. Zauważmy, że korzeń jest przodkiem każdego innego wierzchołka w tym drzewie. Zatem, licząc współczynnik niezadowolenia, zawsze będziemy rozpatrywali każdą taką parę wierzchołków u i v , że u jest korzeniem drzewa. Okazuje się, że istnieje drzewo, w którym nie ma więcej par wierzchołków pozostających w relacji przodek-potomek. Wystarczy wybrać korzeń oraz połączyć go krawędziami ze wszystkimi pozostałymi wierzchołkami. Poniżej schemat takiego drzewa (K oznacza korzeń).



Ustaliliśmy już strukturę drzewa. Opiszemy teraz, w jaki sposób wybrać taki korzeń, który będzie minimalizował współczynnik niezadowolenia.

Rozwiązanie $O(n^2)$

Pierwszy, najbardziej intuicyjny pomysł, polega na naiwnym sprawdzeniu każdego z n sposobów ustalenia korzenia. Dla każdego wierzchołka $u \in \{1, 2, \dots, n\}$ konstruujemy drzewo, którego korzeniem jest u oraz pozostałe wierzchołki są z nim połączone krawędzią. Następnie, dla każdego z tych drzew obliczamy (z definicji) współczynnik niezadowolenia. Spośród otrzymanych wyników wybieramy najmniejszy. Drzew mamy n (po jednym dla każdego kandydata na korzeń). Obliczenie współczynnika niezadowolenia dla jednego drzewa odbywa się w czasie $O(n)$. Zatem cały algorytm działa w czasie $O(n^2)$.

Rozwiązanie $O(n \cdot \log(\max_i a_i))$

Potraktujmy zapisy binarne elementów ciągu a jako słowa nad alfabetem $\{0, 1\}$. Niech $b' = (b'_1, b'_2, \dots, b'_n)$ oznacza zapisy binarne kolejnych elementów ciągu a (b'_i oznacza zapis binarny a_i , który nie zawiera zer wiodących). Następnie „wyrównajmy” długości słów ciągu b' . Chcemy otrzymać słowa o takiej samej długości, równej długości najdłuższego słowa w ciągu b' . W tym celu wszystkie krótsze słowa należy poprzedzić odpowiednią liczbą zer wiodących. Kolejno otrzymane słowa nazwijmy $b = (b_1, b_2, \dots, b_n)$.

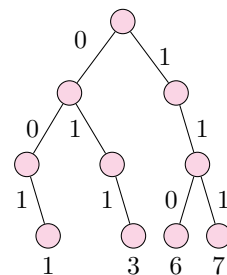
Podobnie jak w rozwiązaniu $O(n^2)$, dla każdego potencjalnego korzenia chcemy obliczyć współczynnik niezadowolenia. W istocie, dla każdego b_i chcemy znaleźć takie b_j , że $b_i \oplus b_j$ jest maksymalne. Na potrzeby tego artykułu zakładamy, że każdemu b_i jest przypisana wartość a_i oraz $b_i \oplus b_j$ ma wartość $a_i \oplus a_j$.

Weźmy $b_i = c_{m-1} \dots c_1 c_0$, dla którego szukamy takiego $b_j = c'_{m-1} \dots c'_1 c'_0$, że $b_i \oplus b_j$ jest maksymalne. Idealnie byłoby, gdyby istniało $b_j = \bar{c}_{m-1} \dots \bar{c}_1 \bar{c}_0$ (\bar{c}_i oznacza negację c_i). Wtedy $b_i \oplus b_j = 2^m - 1$, czyli najlepszy możliwy wynik. Ta obserwacja daje nam pewną intuicję. Będziemy wyszukiwali b_j cyfra po cyfrze, w kolejności od najbardziej znaczących do najmniej znaczących. Załóżmy, że mamy już ustalony prefiks $c'_{m-1} c'_{m-2} \dots c'_{k+1}$ słowa b_j . Zastanawiamy się teraz, jaką wartość może mieć c'_k . Oczywiście, gdyby $c'_k = \bar{c}_k$, wtedy wynik wzrósłby o 2^k . Zatem, jeśli $c'_{m-1} c'_{m-2} \dots c'_{k+1} \bar{c}_k$ jest prefiksem jakiegoś słowa w ciągu b , to $c'_k = \bar{c}_k$, w przeciwnym przypadku $c'_k = c_k$. Prosty dowód pozostawiamy Czytelnikowi.

Pozostało nam jeszcze opisać, w jaki sposób dla danego słowa sprawdzać, czy jest ono prefiksem jakiegoś słowa w ciągu b . W tym celu zbudujemy *drzewo trie* nad słowami ciągu b . Wyszukiwanie b_j cyfra po cyfrze odpowiada wędrowce w drzewie trie od korzenia do liści. Załóżmy, że w danym kroku ustalamy wartość c'_k . Jeśli wierzchołek, w którym jesteśmy, ma dwóch synów, to poruszamy się krawędzią z etykietą \bar{c}_k . W przeciwnym przypadku nie mamy wyboru – idziemy krawędzią z etykietą c_k . Wędrowkę kończymy w liściu. Kolejno wybierane etykiety krawędzi tworzą szukane b_j .

Konstrukcja drzewa trie zajmuje czas $O(n \cdot \log(\max_i a_i))$. Wyznaczenie b_j dla danego b_i zajmuje czas $O(\log(\max_i a_i))$ (długość ścieżki od korzenia do liścia). Współczynnik niezadowolenia obliczamy dla każdego z n potencjalnych drzew, co w sumie daje $O(n \cdot \log(\max_i a_i))$ operacji. Zatem cały algorytm działa w czasie $O(n \cdot \log(\max_i a_i))$.

Rozważmy przykład. Niech $a = (1, 3, 6, 7)$. Wówczas $b' = (1, 11, 110, 111)$, $b = (001, 011, 110, 111)$, a drzewo trie wygląda następująco:



Bartosz ŁUKASIEWICZ

Klub 44

Liga zadaniowa Wydziału Matematyki, Informatyki i Mechaniki, Wydziału Fizyki Uniwersytetu Warszawskiego i Redakcji *Delty*

Skrót regulaminu

Każdy może nadsyłać rozwiązania zadań z numeru n w terminie do końca miesiąca $n + 2$. Szkice rozwiązań zamieszczamy w numerze $n + 4$. Można nadsyłać rozwiązania czterech, trzech, dwóch lub jednego zadania (każde na oddzielnej kartce), można to robić co miesiąc lub z dowolnymi przerwami. Rozwiązania zadań z matematyki i z fizyki należy przysyłać w oddzielnych kopertach, umieszczając na kopercie dopisek: **Klub 44 M** lub **Klub 44 F**. Można je przysyłać również pocztą elektroniczną pod adresem delta@mimuw.edu.pl (preferujemy pliki pdf). Oceniamy zadania w skali od 0 do 1 z dokładnością do 0,1. Ocenę mnożymy przez współczynnik trudności danego zadania: $WT = 4 - 3S/N$, gdzie S oznacza sumę ocen za rozwiązania tego zadania, a N – liczbę osób, które nadesłały rozwiązanie choćby jednego zadania z danego numeru w danej konkurencji (**M** lub **F**) – i tyle punktów otrzymuje nadsyłający. Po zgromadzeniu **44** punktów, w dowolnym czasie i w którejkolwiek z dwóch konkurencji (**M** lub **F**), zostaje on członkiem **Klubu 44**, a nadwyżka punktów jest zaliczana do ponownego udziału. Trzykrotne członkostwo – to tytuł **Weterana**. Szczegółowy regulamin został wydrukowany w numerze 2/2002 oraz znajduje się na stronie deltami.edu.pl

Zadania z matematyki nr 771, 772

Redaguje Marcin E. KUCZMA

771. Wyznaczyć wszystkie funkcje różniczkowalne $f: \mathbb{R} \rightarrow \mathbb{R}$, spełniające równanie

$$f'\left(\frac{a+b}{2}\right) = \frac{f(b) - f(a)}{b-a}$$

dla każdej pary różnych liczb rzeczywistych a, b , których różnica jest liczbą całkowitą.

772. Niech $M_n = 2^n - 1$ dla $n = 1, 2, 3, \dots$. Udowodnić, że następujące dwa warunki są równoważne:

- (1) $2^n \equiv 2 \pmod{n}$;
- (2) $2^{M_n} \equiv 2 \pmod{M_n}$.

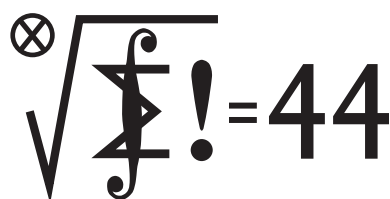
Zadanie 772 zaproponował pan Tomasz Ordowski.

Zadania z fizyki nr 668, 669

Redaguje Elżbieta ZAWISTOWSKA

668. Nauczyciel, zwrócony twarzą do tablicy, obserwuje klasę dzięki odbiciu światła od powierzchni szkieł jego okularów. Nauczyciel widzi dwa obrazy ucznia, który siedzi w odległości 5 m od niego. Jeden obraz znajduje się w odległości 5 m, drugi w odległości $\frac{5}{7}$ m od nauczyciela. Po odwróceniu do klasy nauczyciel widzi przez okulary obraz tego samego ucznia w odległości 2,5 m. Wyznaczyć współczynnik załamania szkła, z którego wykonane są soczewki okularów.

669. Do naczynia w kształcie cylindra o polu przekroju poprzecznego S wlano wodę, w której pływa kawałek lodu z kulką ołowianą wewnątrz. Objętość lodu razem z kulką jest równa V . Nad wodę wystaje $\frac{1}{n}$ część tej objętości. Jak zmieni się poziom wody w naczyniu po stopieniu lodu? Gęstości wody, lodu i ołowiu wynoszą odpowiednio ρ_W, ρ_L, ρ_O .

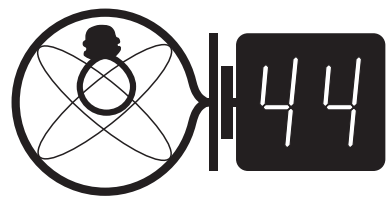


Termin nadsyłania rozwiązań: 28 II 2019

Czołówka ligi zadaniowej **Klub 44 M** po uwzględnieniu ocen rozwiązań zadań 761 ($WT = 1,87$) i 762 ($WT = 2,08$) z numeru 5/2018

Janusz Olszewski	Warszawa	45,72
Tomasz Choczewski	Szczecin	44,36
Tomasz Wietecha	Tarnów	44,19
Michał Miodek	Warszawa	41,65
Franciszek S. Sikorski	Warszawa	39,86
Piotr Kumor	Olsztyn	38,63
Krzysztof Kamiński	Pabianice	35,75
Paweł Kubit	Kraków	35,69
Marcin Małogrosz	Warszawa	35,37

Przez kilka miesięcy nikt nie przekraczał bariery 44 p.; teraz – jednocześnie trzech uczestników, o bardzo zróżnicowanym stażu: Janusz Olszewski po raz dziewiętnasty; Tomasz Choczewski po raz pierwszy (witamy w K44!); Tomasz Wietecha po raz dwunasty (pamiętajmy wszak, że p. T.W. już 13 razy w fizyce...)



Skąd się wzięło siedem?

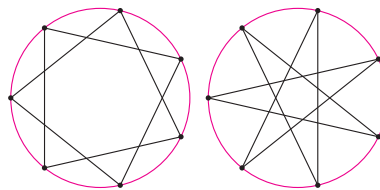
Począwszy od Pitagorasa wierzymy, że przyroda działa zgodnie z regułami matematyki. Wobec tego odszukajmy reguły, którymi kierował się siódmaczek (*Trientalis*) z naszych zagajników, wybierając siedmiokrotną symetrię swoich kwiatów.



Parkietaż płaszczyzny n -kąta foremnymi są możliwe tylko dla 3, 4 i 6. Krystalografia dopuszcza tylko krotność 2, 3 i 6. Siedmiokąta foremnego nie da się skonstruować cyrklem i linijką. Skąd więc 7?

Jedyne, co przychodzi do głowy, to n -kąty foremne gwiazdziste. Ale dla $n = 7$ są takie dwa. Pojawia się więc pytanie, który z nich wybrało DNA siódmaczka.

Zagadka, zupełnie jak ze wzorami Ramanujana.



M. K.

n -kąta foremny gwiazdzisty to wpisana w okrąg łamana dłuższa od okręgu, złożona z cięciw jednakowej długości. Jest ich $\varphi(n)/2 - 1$, gdzie φ to funkcja Eulera, której wartości to $n(1 - \frac{1}{p_1}) \cdot \dots \cdot (1 - \frac{1}{p_k})$, gdzie p_i to różne dzielniki pierwsze n .

Prosto z nieba: Klimat z Kosmosu

Dobrze wiadomo, że klimat naszej planety ulega czasami poważnym zmianom. W ciągu ostatnich 200 milionów lat Ziemia doświadczyła czterech okresów geologicznych (trias, jura, kreda i kenozoik) i jednej wielkiej epoki oziębienia (złodowacenie w czwartorzędzie). Niektóre zmiany klimatyczne, np. obserwowane w ciągu ostatnich 100 lat globalne ocieplenie, mają związek z lokalnymi ziemskimi zmianami (ingerencją cywilizacji człowieka). Inne długotrwałe trendy są niezależne od tego, co dzieje się na Ziemi, można je za to korelować z procesami zachodzącymi w Układzie Słonecznym. Hipotezę wiążącą niewielkie, okresowe zmiany orbity ziemskiej z klimatem postawił blisko 100 lat temu Milutin Milankowić, serbski astronom i geofizyk. *Cykle Milankowicia* są związane z precesją osi obrotu Ziemi i ruchem peryhelium orbity (cykl o okresie około 21 tys. lat), zmianami nachylenia osi Ziemi w stosunku do jego płaszczyzny orbitalnej (okres około 41 tys. lat) oraz ekscentryczności orbity Ziemi (100 tys. lat).

To, oczywiście, nie wszystko. Ziemski klimat jest podatny na periodyczne zmiany orbity Ziemi wywołane przez grawitacyjne przyciąganie innych planet, w szczególności Wenus i Jowisza, w cyklu powtarzającym się regularnie co 405 tys. lat. W sumie cyklicznie zmieniające się nachylenie orbity oraz odległość od Słońca powodują zmiany ilości energii słonecznej docierającej do powierzchni planety, a to z kolei może mieć kluczowy wpływ na m.in. temperaturę, a więc i ewolucję gatunków.

Empirical evidence for stability of the 405-kilo-year Jupiter–Venus eccentricity cycle over hundreds of millions of years.
D.V. Kent, PNAS 201800891 (2018)

Niedawno zademonstrowano namacalne dowody wpływu mechaniki nieba na zmiany w historii Ziemi. Zebrane z ponad półkilometrowej głębokości próbki osadów i odwiertów w okolicy prehistorycznego jeziora w niecce Newark oraz z parku narodowego Petrified Forest w Arizonie potwierdzają ponad wszelką wątpliwość obecność i niezwykle stabilność cyklu Wenus-Jowisz na przestrzeni ostatnich 215 milionów lat. Oprócz tego zaobserwowano „zapisaną” w przekrojach geologicznych ewolucję ziemskiego pola magnetycznego (zamiany biegunów) z czasów, gdy po powierzchni super-kontynentu Pangei przechadzały się dinozaury i pierwsze ssaki.

Badania geologiczne to jeden z lepszych sposobów pokazania, że kosmiczne wydarzenia odgrywają historyczną rolę w naturalnych zmianach klimatu Ziemi. Dodatkowo, obserwowana w skałach historia stabilności Układu Słonecznego jest nieocenioną wskazówką dla astronomów symulujących jego ewolucję w bardzo długich skalach czasowych.

Michał BEJGER

Niebo w grudniu

Przed nami ostatni miesiąc 2018 roku, odznaczający się najkrótszymi dniami i najdłuższymi nocami w ciągu całego roku. Kiedyś grudniowe noce były zimne, lecz pogodne. Ostatnio są cieplejsze, ale za to bardziej pochmurne, stąd mniej okazji do podziwiania nocnego nieba. 21 grudnia, tuż przed północą polskiego czasu, Słońce osiągnie najbardziej na południe wysunięty punkt ekliptyki i tym samym na północnej półkuli Ziemi zacznie się astronomiczna zima. Jednak najwcześniejszy zachód Słońca ma miejsce ponad tydzień wcześniej, około 13 grudnia, a najpóźniejszy wschód – ponad tydzień po przesileniu, 30 grudnia. Dzieje się tak, gdyż Ziemia na przełomie roku jest blisko peryhelium (czyli najbliższego Słońcu punktu swojej orbity, przechodzi przezeń 3 stycznia) i pokonuje w ciągu doby stosunkowo duży odcinek orbity wokółsłonecznej, a tempo obrotu planety wokół własnej osi jest stałe, stąd Słońce niejako ucieka przed daną długością geograficzną.

W grudniu widoczne są prawie wszystkie planety Układu Słonecznego. Saturn na początku stycznia przyszłego roku znajdzie się w koniunkcji ze Słońcem i jest w zasadzie niewidoczny. Od lutego zacznie pokazywać się na niebie porannym.

Merkury i Jowisz wyłonią się z zorzy porannej w drugiej i trzeciej dekadzie grudnia, a pozostałe planety są widoczne całkiem dobrze na ciemnym niebie.

Planeta Mars góruje na początku nocy astronomicznej, wędrując przez gwiazdozbiór Wodnika, gdzie od dłuższego już czasu przebywa planeta Neptun. 7 grudnia obie planety spotkają się. Wieczorem tuż po zmierzchu, a zatem gdy na obserwacje Neptuna jest jeszcze zdecydowanie za wcześnie, obie planety przedzieli dystans $2'$, natomiast dwie godziny później, na początku nocy astronomicznej, gdy Neptun stanie się dobrze widoczny, dystans między nimi urośnie do prawie 4,5 minuty kątowej. Czerwona Planeta cały czas oddala się od nas i jej tarcza oraz jasność nadal szybko się zmniejszają. W dniu przesilenia zimowego Mars przejdzie do gwiazdozbioru Ryb, a do Sylwestra jego blask spadnie do $+0,5^m$, a tarcza skurczy się do $7''$. Planeta Neptun w grudniu porusza się ruchem prostym i pod koniec miesiąca przejdzie niecałe $14'$ na południe od gwiazdy 6. wielkości 81 Aqr, sama świecąc z jasnością $+7,9^m$.

Kolejną planetą jest Uran, który prawie cały miesiąc spędzi w gwiazdozbiorze Ryb, wchodząc do niego na pożegnalne dwa miesiące. Od lutego planeta na dobre wejdzie do gwiazdozbioru Barana, a przez Ryby zacznie wędrować ponownie dopiero w końcu tego stulecia. W grudniu Uran kreśli pętlę niewiele ponad 1° na północ od gwiazdy 4. wielkości α Psc, świecąc z jasnością $+5,7^m$, czyli na granicy widoczności gołym okiem.

Pozostałe trzy planety Układu Słonecznego można obserwować niedługo przed wschodem Słońca. Najlepiej widoczna jest planeta Wenus, która rozgościła się na niebie porannym po październikowej koniunkcji ze Słońcem. Niestety, planeta szybko oddala się od Ziemi, w związku z czym średnica jej tarczy spada, a faza rośnie, co czyni ją coraz mniej atrakcyjnym celem dla posiadaczy teleskopów. Bardzo duża jest jasność Wenus. W trakcie miesiąca zmniejszy się ona z $-4,7$ do $-4,5^m$, jednocześnie jej tarcza skurczy się do z 41 do $27''$, a faza urośnie z 26 do 47% . Grudzień Wenus zacznie 6° na wschód od Spiki, najjaśniejszej gwiazdy Panny, ale 13 grudnia wkroczy na obszar Wagi i 23 grudnia minie gwiazdę Zuben Elgenubi w odległości 3° . Przez cały miesiąc planeta dąży do maksymalnej elongacji zachodniej, przypadającej 6 stycznia 2019 r.

Planety Merkury i Jowisz można obserwować tuż przed wschodem Słońca. Merkury 15 grudnia osiągnie maksymalną elongację zachodnią, wynoszącą ponad 21° i prawie przez cały miesiąc pozostanie widoczny kilkadziesiąt minut przed świtem nisko nad widnokregiem. W miarę upływu czasu blask planety urośnie od $+3$ do $-0,4^m$, jej tarcza zmniejszy się przy tym z 10 do $5''$, a faza zwiększy się z 7 do 90% . Planeta 16 grudnia minie jedną z jaśniejszych gwiazd Skorpiona, gwiazdę Graffias, w odległości niewiele większej od 1° . W drugiej dekadzie grudnia do Merkurego dołączy Jowisz, który 26 listopada przeszedł przez koniunkcję ze Słońcem i zacznie pojawiać się na niebie porannym. Początkowo znajdzie się bardzo nisko, ale systematycznie

wespie się coraz wyżej i 31 grudnia godzinę przed świtem wzniesie się na wysokość ponad 7° . W grudniu jasność Jowisza wyniesie $-1,7^m$, przy średnicy tarczy $31''$. 21 grudnia obie planety miną się w odległości mniejszej niż 1° .

Księżyc, podobnie jak miesiąc temu, początkowo pokaże się na niebie porannym, dążąc do nowiu, przypadającego 7 grudnia. Księżyc spotka się z planetą Wenus 3 i 4 dni wcześniej. Najpierw zbliży się do niej na 8° , prezentując tarczę w fazie 17% , dobę później, przy fazie zaledwie 10% zajmie pozycję 6° na prawo od Wenus. Szkoda, że wtedy jeszcze nie widać pary Merkury-Jowisz. Tworzyłyby widowiskowy układ. Ale 5 i 6 grudnia Księżyc zbliży się do Merkurego na 9 i 5° , mając tarczę oświetloną odpowiednio w 7 i 1% . Srebrny Glob znajdzie się w nowiu 7 grudnia. Niestety, w tych dniach pierwsza planeta od Słońca zdąży pojaśnić tylko do $+0,5^m$ i jeszcze słabo będzie przebijać się przez tło nieba.

8 grudnia Księżyc zacznie pokazywać się na niebie wieczornym, gdzie 14 grudnia, przy fazie 42% , spotka się z parą planet Mars-Neptun, przechodząc ponad 4° na południe od niej. Dobę później przypada I kwadra, 22 grudnia – pełnia. W dniach 26–27 grudnia Srebrny Glob, oświetlony w około 80% , minie Regulusa, 29 grudnia przejdzie przez ostatnią kwadrę, a miesiąc i rok zakończy w fazie 31% będąc 10° od Spiki i 20° od Wenus.

W grudniu promieniują dwa roje meteorów: Geminidy oraz Ursydy. Pierwszy rój pojawia się od 4 do 17 grudnia, z maksimum aktywności 14 grudnia. Wtedy można spodziewać się nawet 120 meteorów na godzinę. Ich radiant znajduje się 2° od Kastora, jasnej gwiazdy Bliźniąt. W tym roku Księżyc zaświetli niebo wieczorem i zostawi prawie 10 godzin na obserwacje Geminidów. Natomiast mające maksimum aktywności 22 grudnia Ursydy przypadają w pełni Księżyca i są niewidoczne.

11 grudnia maksimum blasku osiąga gwiazda Mira Ceti. Jest to zmienna długookresowa, z okresem zmian blasku ponad 330 dni, stąd przez cały miesiąc powinna być widoczna gołym okiem. Zwłaszcza że jest widoczna bardzo dobrze: wschodzi jeszcze za dnia i góruje około 21:30, zachodząc po godzinie 3. Księżyc przejdzie 18 grudnia 12° na północ od Miry.

Ostatnim, lecz wcale nie najmniej atrakcyjnym elementem nocnego grudniowego nieba jest kometa 46P/Wirtanen. 13 grudnia kometa przejdzie przez perihelium, $1,06$ AU od Słońca, zaś 17 grudnia zbliży się do Ziemi na około 11,5 mln km ($0,08$ AU). Dzięki temu może osiągnąć jasność nawet $+3^m$. W związku z bliskością do nas kometa porusza się po niebie bardzo szybko: 1 grudnia zajmie pozycję 12° na wschód od gwiazdy τ Ceti, 10 grudnia przejdzie 5° na wschód od Menkara w Wielorybie, 16 grudnia znajdzie się już 4° na wschód od Plejad, zaś 23 grudnia minie Capellę w Woźnicy, w odległości $0,5^\circ$. Przez miesiąc przemierzy tym samym ponad 90° !

Ariel MAJCHER

Nierogaczna wysokich energii

Nicolas Chauvin był żołnierzem wojsk napoleońskich. Wielokrotnie ranny na polu bitwy, do końca życia pozostał wiernym wyznawcą cesarza Francji, nawet po jego upadku. Od nazwiska tego wojaka wzięło początek pojęcie, które początkowo oznaczało nacjonalistyczne zaślepienie, a z biegiem czasu uległo uogólnieniu, i obecnie jest stosowane do opisywania poczucia wyższości członków jednej grupy ludzi nad inną. Nicolas Chauvin najprawdopodobniej nie istniał bardziej niż Kopciuszek czy Królewna Śnieżka, jednak związana z jego nazwiskiem postawa wciąż ma się nie najgorzej.

W końcu września w CERN-ie odbyły się warsztaty poświęcone różnym aspektom płci w fizyce teoretycznej wielkich energii [1]. Formuła tego spotkania miała połączyć aspekty ściśle naukowe z dyskusją szczegółowych problemów napotykanymi w związku ze swą płcią przez fizyków i fizyczki na różnych poziomach kariery. Naukowy program spotkania wyglądał naprawdę imponująco, miał jednak pewną cechę niespotykaną zwykle na tego typu konferencjach – wszystkie referaty były wygłaszane przez panie. O problemach dyskutowało towarzystwo mieszane.

To właśnie w tej części spotkania miało miejsce wystąpienie, które narobiło mnóstwo szumu medialnego. Jego autorem był Alessandro Strumia, wybitny fizyk teoretyk z Pizy, który w CERN-ie realizuje obecnie prestiżowy grant ERC. O skali talentu tego naukowca można się przekonać, analizując liczbę, wpływ lub popularność jego prac; piszący te słowa miał okazję przekonać się o niej bezpośrednio kilkanaście lat temu, pracując nad wspólnym projektem naukowym [2]. Strumia, wraz ze współpracownikiem Ricardo Torrem, opublikował pół roku temu ciekawą analizę bibliometryczną fizyki wysokich energii i postanowił użyć przygotowanych w tym celu narzędzi, żeby dowiedzieć się czegoś o wadze osiągnięć naukowych w zależności od płci autora osiągnięcia.

W swoim referacie Strumia przedstawił w szczególności rozkład liczby cytowań prac naukowych osobno dla kobiet i mężczyzn. Z analizy tej wynika, że praca napisana przez kobietę ma mniej więcej dziesięciokrotnie mniejsze prawdopodobieństwo trafienia do prac najliczniej cytowanych niż praca napisana przez mężczyznę. Strumia wyciągnął stąd daleko idące wnioski, zasłaniając się wszelako przykładem Marii Skłodowskiej-Curie, który miał pokazywać, że ogólne tendencje nie uniemożliwiają prawdziwym geniuszkom osiągnięcia spektakularnego sukcesu w nauce.

Strumia analizował także – oczywiście z podziałem na płeć – przyrost liczby cytowań prac naukowych w miarę postępu kariery naukowej. Z przedstawionych przez niego danych wynika, że przez pierwsze pięć lat po doktoracie prace kobiet i mężczyzn cytowane są tak samo często, ale po dekadzie pojawia się różnica. Dwadzieścia lat po doktoracie prace mężczyzn cytowane

są półtora raza częściej niż kobiet, różnica staje się zaś dwukrotna po czterdziestu latach od doktoratu.

Inny wątek poruszony przez Strumię miał charakter osobisty. Brał on bowiem udział w konkursie na stanowisko profesora, w którym przegrał z kontrkandydatką. Zirytowany Strumia porównał liczbę cytowań swoich prac z liczbą cytowań zwyciężczyni konkursu i przewodniczącej komisji konkursowej, twierdząc, że w obecnym klimacie poprawności politycznej i poparcia dla akcji afirmacyjnych mężczyźni badacze są po prostu dyskryminowani.

Ta wycieczka osobista wzbudziła zdecydowany sprzeciw środowiska naukowego. Wielu fizyków podpisało się pod listem protestacyjnym, CERN zaś zawiesił Strumię w funkcji pracownika i skasował jego prezentację ze strony internetowej warsztatów. Wśród wyrazów oburzenia pojawiły się liczne kpiny, że jedną trzecią z pięciocyfrowej liczby cytowań Strumii stanowią odniesienia do pracy opisującej odkrycie bozonu Higgsa, której był jednym z tysięcy autorów, i to o mikroskopijnym wkładzie; a dalsze tysiące cytowań przyniosły mu prace na temat sygnału w danych LHC, który po bliższej analizie okazał się fluktuacją statystyczną. Krótko mówiąc, media elektroniczne i portale społecznościowe zawrzały zgrozą i złością – w przeważającej większości bez śladu racjonalnej refleksji.

Co jednak kryje się za analizowanymi przez Strumię danymi? Skąd bierze się zaprezentowana przez niego różnica? Sabine Hossenfelder i Tobiasz Mistele [3], posługując się niezależnie skonstruowanymi narzędziami i używając innych baz danych zawierających prace z fizyki wysokich energii, potwierdzili wolniejszy przyrost liczby cytowań prac pisanych przez kobiety. Zauważyli też jeszcze jeden interesujący fakt – wśród naukowców, którzy napisali co najwyżej cztery prace, jest nieproporcjonalnie wiele pań. Oznacza to najprawdopodobniej, że kobiety częściej niż mężczyźni zdobywają tytuł zawodowy lub stopień naukowy w dziedzinie nauk fizycznych, po czym opuszczają środowisko akademickie. Jedną z konsekwencji tego faktu jest zmniejszenie średniej liczby cytowań przypadających na kobietę. Hossenfelder i Mistele wykazali, że jeśli ograniczyć się do autorów, którzy opublikowali co najmniej pięć prac, opisywana przez Strumię asymetria w przyroście liczby cytowań znika.

Z całej tej historii płynie kilka morałów. Każę się ona zastanawiać, dlaczego kobiety tak często nie widzą siebie w środowisku fizyków. Przypomina, że dyskusje o sprawach trudnych wymagają taktu i przyzwoitości. I wreszcie, pokazuje, że nawet najbardziej inteligentni ludzie są podatni na szowinistyczne stereotypy, które kuszą, by bezkrytycznie traktować dane, o ile potwierdzają one utarte schematy.

[1] <https://indico.cern.ch/event/714346/>

[2] Raidal M., Strumia A., Turzyński K., Phys. Lett. B609 (2005) 351

[3] <http://backreaction.blogspot.com/2018/10/gender-bias-in-academia-case-strumia.html>



Kolorowa płaszczyzna

Joanna JASZUŃSKA

Większości problemów otwartych współczesnej matematyki nie da się zrozumieć bez zaawansowanej wiedzy, ale zdarzają się też takie, których sformułowania są zupełnie elementarne. Poniższa seria zadań prowadzi do jednego z nich.

1. Każdy punkt płaszczyzny pomalowano na czerwono lub żółto. Wykaż, że istnieją dwa punkty odległe o 1 i tego samego koloru.

2. Każdy punkt płaszczyzny pomalowano na czerwono, żółto lub niebiesko. Wykaż, że istnieją dwa punkty odległe o 1 i tego samego koloru.

3. Każdy punkt płaszczyzny pomalowano jednym z siedmiu kolorów. Wykaż, że nie muszą istnieć dwa punkty odległe o 1 i tego samego koloru.

4. Każdy punkt płaszczyzny pomalowano jednym z ośmiu kolorów. Wykaż, że nie muszą istnieć dwa punkty odległe o 1 i tego samego koloru.

Podsumowując, jeśli każdy punkt płaszczyzny pomalowano jednym z n kolorów, to dla $n = 1, 2, 3$ muszą istnieć dwa punkty odległe o 1 i tego samego koloru, dla $n \geq 7$ nie muszą i jeśli dla pewnego n nie muszą, to dla większych n też nie muszą.

Liczba chromatyczna płaszczyzny $\chi(\mathbb{R}^2)$ to najmniejsza wartość n , dla której rozważane punkty nie muszą istnieć; powyżej uzasadniliśmy, że $4 \leq \chi(\mathbb{R}^2) \leq 7$.

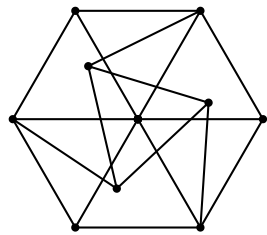
Dokładna wartość $\chi(\mathbb{R}^2)$ nie jest znana, jest to tzw. *problem Hadwiger–Nelsona*.

Sformułowanie i powyższe rezultaty pochodzą z lat 1950–60 i do niedawna nic więcej nie było wiadomo. W kwietniu 2018 roku Aubrey de Grey opublikował w internecie pracę [AdG], w której udowodnił, że $\chi(\mathbb{R}^2) \geq 5$. Skonstruował graf o 1581 wierzchołkach i 7877 krawędziach długości 1 i pokazał (wspomagając się komputerem), że nie da się pomalować jego wierzchołków czterema kolorami bez krawędzi o jednobarwnych końcach. Dowód ten szybko sprawdzono, a następnie w ramach internetowego projektu *Polymath 16* [P16] ruszyły zbiorowe poszukiwania mniejszego grafu o tej własności (najlepiej nie wymagającego komputera do badania go). We wrześniu 2018 roku najmniejszy znany taki graf miał 553 wierzchołki i 2722 krawędzie.

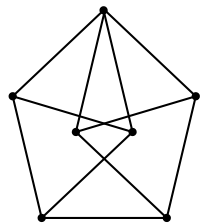
W konstrukcji grafu z pracy [AdG] wykorzystano m.in. następujące obserwacje.

5. Wykaż, że cztery dolne wierzchołki grafu z rysunku 5 leżą na jednej prostej oraz że dwa skrajne z nich wraz z najwyższym tworzą trójkąt równoboczny.

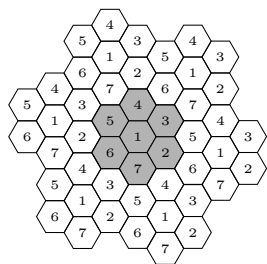
6. Rozważmy wierzchołki i środek sześciokąta foremnego o boku długości 1. Wyznacz liczbę istotnie różnych kolorowań tych siedmiu punktów najwyższej czterema barwami bez punktów odległych o 1 tego samego koloru.



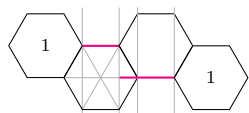
Rys. 1. Graf Golomba: 10 wierzchołków, wszystkie krawędzie długości 1.



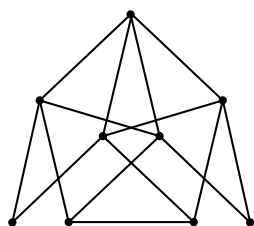
Rys. 2. Wrzeciono Mosera: 7 wierzchołków, wszystkie krawędzie długości 1.



Rys. 3. Liczby oznaczają kolory, szary obszar to powtarzający się fragment. Punkty z linii podziału mają barwę dowolnego z sąsiednich sześciokątów.



Rys. 4



Rys. 5. Wszystkie krawędzie są długości 1.

Rozwiązania niektórych zadań

R1. Trzy wierzchołki dowolnego trójkąta równobocznego o boku długości 1 pomalowano dwoma kolorami, więc pewne dwa są tej samej barwy i odległe o 1. \square

R2. Nie da się pomalować wierzchołków grafu z rysunku 1 trzema kolorami bez krawędzi o końcach jednego koloru. Jeśli bowiem środkowy punkt jest czerwony, to wierzchołki sześciokąta muszą być na przemian żółte i niebieskie. Jeśli punkty połączone z wewnętrznym trójkątem są niebieskie, to jego wierzchołki mogą być tylko czerwone i żółte, a to jak już wiemy daje tezę. \square

Zamiast grafu Golomba można w dowodzie użyć grafu z rysunku 2 lub z *Delty 2/2013* (str. 22).

R3. Podzielmy płaszczyznę na sześciokąty foremne o średnicy 0,99 i pomalujmy jak na rysunku 3. Wówczas wewnątrz żadnego z sześciokątów nie zmieści się odcinek o długości 1, natomiast odcinki o końcach w różnych sześciokątach tego samego koloru mają długość większą niż 1 (co najmniej 1,25 średnicy; rys. 4). \square

R4. Dla ośmiu i więcej kolorów wystarczy wziąć pokolorowanie dla siedmiu i na każdy nowy kolor przemalować inny pojedynczy punkt, który był koloru 1. \square

Literatura:

[AdG] arxiv.org/abs/1804.02385

[P16] michaelnielsen.org/polymath1/index.php?title=Hadwiger-Nelson_problem



41. KONKURS UCZNIOWSKICH PRAC Z MATEMATYKI IM. PAWŁA DOMAŃSKIEGO

W konkursie biorą udział twórcze prace matematyczne napisane przez uczniów szkół ponadpodstawowych oraz podstawowych w klasach 7-8.

Mówiąc krótko: **należy udowodnić coś, czego jeszcze nikt inny nie udowodnił!**



Na stronie www.deltami.edu.pl/kupzm można znaleźć:

- propozycje tematów,
- listę wszystkich dotychczasowych laureatów (czyli od roku 1978),
- wyniki niektórych prac,
- szczegółowy regulamin.

TERMIN ZGŁASZANIA PRAC: 30 KWIETNIA 2019
FINAŁ: WRZESIEŃ 2019



deltami@mimuw.edu.pl

Delta.czasopismo