Teoria złożoności obliczeniowej

Czas, czyli koszt

Henryk Woźniakowski
Wydział Matematyki, Informatyki i Mechaniki
Uniwersytetu Warszawskiego
Department of Computer Science, Columbia University
członek korespondent Polskiej Akademii Nauk
Prof. Henryk Woźniakowski specjalizuje się w teorii złożoności obliczeniowej. Od około 20 lat zajmuje się złożonością problemów wielowymiarowych (*tractability*); bada właściwości metod quasi-Monte Carlo m.in. pod kątem zastosowań w matematyce finansowej

Prof. Henryk Woźniakowski odpowiada na pytania „Academii" o przeszłość, teraźniejszość i przyszłość teorii złożoności obliczeniowej

Academia: Panie Profesorze, czym zajmuje się teoria złożoności?

Prof. Henryk Woźniakowski: *Złożoność obliczeniowa jest stosunkowo nowym działem matematyki lub - dokładniej - informatyki teoretycznej. Pojawiła się wraz z powstaniem komputerów. Dosyć prędko ludzie przekonali się, że trudność niektórych zadań może być tak wielka, że nawet najszybszy komputer ich nie rozwiąże.*

Niektóre algorytmy rozwiązywania zadań są bardzo wolne. A priori nie bardzo wiadomo, czy to algorytm jest zły, czy problem jest za trudny. Dlatego właśnie narodził się dział złożoności obliczeniowej, czyli sztuka poszukiwania algorytmów najtańszych i badania, na ile problem jest złożony.

Kiedyś ludzie mogli długo czekać na rozwiązanie - ważne było, żeby użyta pamięć komputerowa była mała. Wtedy kosztem była pamięć komputera. Teraz na ogół pamięci komputerów są duże, a minimalizuje się czas obliczeń. Złożoność obliczeniowa stara się podać dobre oszacowania tego minimalnego czasu.

Więc kosztem jest dzisiaj tak naprawdę czas?

Tak. Mierzony czas działania algorytmu. Możemy do oceny złożoności zastosować tzw. przypadek najgorszy: oceniamy jakość algorytmu przez najdłuższy czas działania, uwzględniając wszystkie interesujące nas dane. To tak, jakby ostateczną oceną studenta miał być najgorszy wynik, jaki uzyskał na studiach. Studentowi, który ma same piątki, jest wszystko jedno, ale student, który ma same piątki i jedną dwóję, przy takim sposobie oceny miałby dwóję. Wiele zadań przy zastosowaniu tak surowego kryterium okazuje się za trudnych. Można zamiast tego stosować przypadek średni: przyjąć, że czasami noga może się powinąć i uśrednić czas działania algorytmu ze względu na wszystkie dane. Można też przyjąć przypadek probabilistyczny i oceniać algorytm, odrzucając jego zachowanie dla - powiedzmy - 1% danych. Często też rozważamy przypadek zrandomizowany, gdzie czas działania algorytmów szacujemy, uwzględniając średnie zachowanie się dla parametrów losowych. To daje większą szansę znalezienia szybkiego algorytmu. Złożoność obliczeniowa w przypadkach średnim, probabilistycznym czy zrandomizowanym jest zwykle mniejsza, czasem znacznie mniejsza niż w przypadku najgorszym.

Ale nie zawsze?

Istnieją zadania, dla których wyniki zawsze są złe. Niektóre zadania cierpią na tzw. przekleństwo wymiaru. Otóż mamy zadanie zdefiniowane na klasie funkcji d zmiennych. Coraz częściej w praktyce obliczeniowej występują zadania, w których d jest olbrzymie. Na przykład w matematyce finansowej trzeba liczyć całki funkcji, która ma 360 i więcej zmiennych! Często złożoność obliczeniowa jest funkcją wykładniczą w d. Na przykład koszt wynosi co najmniej 2 do potęgi d. Dla d=3, byłby on równy 8 - tyle co nic. Ale gdy zmiennych mamy 360, to 2 podniesione do potęgi 360 daje w praktyce liczbę tak dużą jak prawie nieskończoność. Co wtedy zrobić? Można wprowadzać dodatkowe założenia dotyczące tych funkcji, tak aby rozsądnie zmniejszyć rozpatrywaną klasę funkcji i aby usunąć przekleństwo wymiaru.

Leszek Plaskota

W 2010 roku prof. Henryk Woźniakowski (na zdjęciu w środku w pierwszym rzędzie) współorganizował 9. Międzynarodową Konferencję Metod Monte Carlo i Quasi-Monte Carlo w Obliczeniach Naukowych (9th International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing)

A jak teorię złożoności obliczeniowej można wykorzystać do uproszczenia jakiegoś praktycznego problemu?

Tutaj kłania się matematyka finansowa. Na początek powiem, dlaczego finansiści chcą liczyć całki 360-wymiarowe. Chodzi o pożyczki, ale takie poważniejsze, przynajmniej na dom. Udziela się ich na ogół na 30 lat. Ponieważ rynek szalenie szybko się zmienia, banki zastrzegają sobie, że co miesiąc mogą trochę zmienić warunki umowy pożyczkowej. A ponieważ na 30 lat wypada 360 rat – mamy 360 parametrów. Banki chcą być fair *wobec klienta, a przede wszystkim wobec siebie i zapewnić sobie zysk, liczą więc wartość oczekiwaną pożyczki, której udzielają klientowi. Matematycznie ta wartość oczekiwana to całka.*

Do lat 90. liczono całki tzw. metodami (zrandomizowanymi) Monte Carlo. Istnieją też zupełnie inne metody – tzw. quasi-Monte Carlo. W latach 90. nagle odkryto, że te metody są dużo lepsze. Okazało się, że na ogół dają bardzo podobne wyniki jak metody Monte Carlo, ale po znacznie mniejszej liczbie kroków. Do dziś zagadka ich wydajności nie jest do końca wyjaśniona, chociaż myślę, że główne elementy są już wiadome. Otóż mamy, owszem, 360 zmiennych, ale te zmienne są różnej ważności. Algorytmy quasi-Monte Carlo dla takich zadań potrafią jak gdyby redukować nieważne zmienne. I wtedy zostaje ich nie 360, tylko dwie albo trzy. Nikt oczywiście nie chce liczyć dokładnie tych całek. Jeden procent to już i tak bardzo duża dokładność. Wiem, że w Australii liczy się dziś z powodzeniem całki o ponad 9000 zmiennych!

Obecnie prowadzone są również badania nad komputerem kwantowym. To, co było trudne dla komputerów klasycznych, nie zawsze jest trudne dla komputera kwantowego. Zainteresowanie obliczeniami kwantowymi wywołał algorytm Shora. Chodzi o kryptografię, a mówiąc prościej – o bezpieczeństwo korzystania z usług bankowych. Otóż wiadomo, że dla bardzo dużej liczby naturalnej trudno jest znaleźć jej dzielniki. Ale mając te dzielniki, można już łatwo zrekonstruować tę liczbę. Tę zasadę wykorzystuje się do szyfrowania danych. Shor pokazał, że za pomocą komputera kwantowego możemy zadanie szukania dzielników liczby N rozwiązać kosztem proporcjonalnym do logarytmu z N do potęgi co najwyżej 3, podczas gdy dla komputera standardowego nie znamy algorytmu, którego koszt byłby potęgą logarytmu z N.

Czyli bardzo tanio?

Bardzo tanio. Myślę, że dlatego wiele rządów na świecie zaniepokoiło się, że pierwszy posiadacz komputera kwantowego będzie mógł „otwierać" wszystkie kody bankowe. Nie chcąc popełnić grzechu zaniedbania, zdecydowano się na wydanie miliardów dolarów na badania. Niestety, do dziś nie ma postępu technologicznego w budowie komputerów kwantowych. Ale jeśli kiedyś taki komputer powstanie, to będziemy mieli nowy model obliczeniowy i nowy przypadek złożoności obliczeniowej. Ze wszystkimi konsekwencjami.

A zatem widziałby Pan przyszłość teorii złożoności w komputerach kwantowych?

Jako człowiek już stary nie wierzę, że to będzie tak szybko. Jutro – ale w sensie biblijnym – może takie komputery powstaną. Badanie nowych technologii, nowych sposobów zbudowania komputera podoba mi się, choć nie wiem, czy się kiedyś uda. Model matematyczny obliczeń kwantowych jest już dziś bardzo ciekawy. Ale czy będzie kiedyś przystawał do rzeczywistości? Nie wiem. Pewnie trochę będzie przystawał, a trochę nie.

Rozmawiała Agnieszka Pollo