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 wiedzie 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.

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.

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"*.

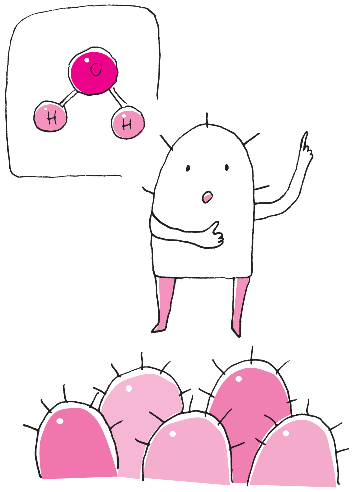
Rozróżnianie słów

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 $Q = \{0, \ldots, 4\}$, stan



początkowy to 0, a stan akceptujący jest tylko jeden, mianowicie 2. Automat, niezależnie od litery w słowie, przechodzi ze stanu q do stanu $(q+1) \mod 5$. Inny automat akceptuje słowa nad $\{a, b\}$, które na pozycjach przystających do 3 modulo 7 mają w sumie parzyście 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 $Q = \{0, \ldots, 7\} \times \{0, 1\}$. 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 $(4, (c+1) \mod 2)$. W przeciwnym przypadku automat, niezależnie od tego, co widzi, przechodzi ze stanu (q, c) do $((q+1) \mod 7, c)$. 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 $1, 2, \ldots, k$, to liczba $|u| - |v|$ musi dzielić się przez $\mathrm{NWW}(1, 2, \ldots, k)$, 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 parzyście 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.