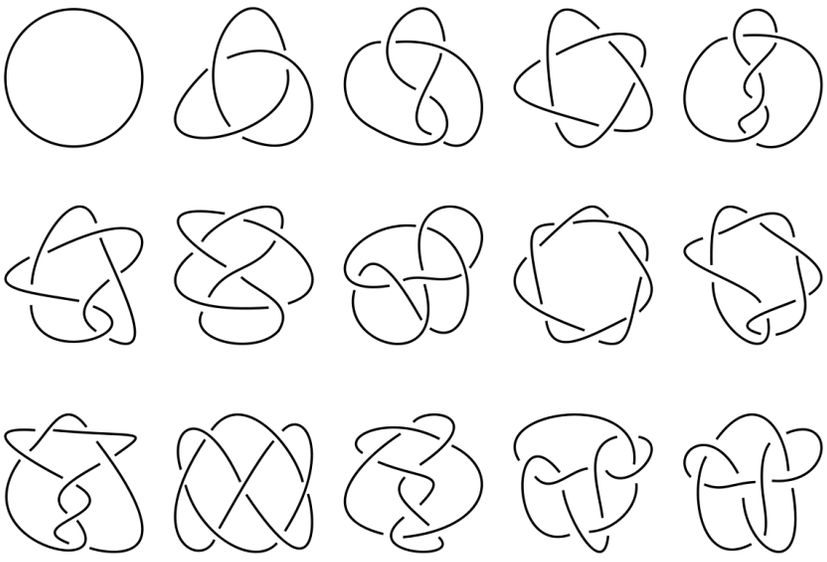
SPIS TREŚCI
NUMERU 12 (523)

Warsaw Center of Mathematics and Computer Science
wcmcs.edu.pl

W następnym numerze plączemy:



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.

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

Okładki i ilustracje: Anna Ludwicka Graphic Design & Serigrafia; rysunki techniczne: Stanisław Walczak.

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`

RUCH S.A.: `www.ruch.com.pl`, infolinia 804-200-600
Prenumerata realizowana przez RUCH S.A.:
Cena prenumeraty w 2018 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 7^{00}–17^{00}. 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`

Wydawca: Uniwersytet Warszawski

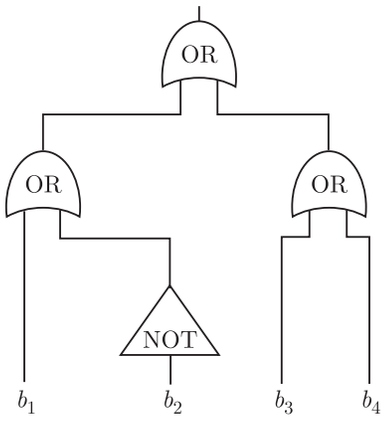
O modelach obliczeń komputerowych

Tomasz KAZANA

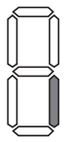
Zastanówmy się nad następującym pytaniem: czym jest komputer? Sądzę, że odpowiedź na tak zadane pytanie może zależeć w znacznej mierze od tego, kogo o to pytamy. Taka sytuacja nie jest, oczywiście, czymś wyjątkowym. Jeśli zamiast informatyką zajmiemy się cukiernictwem i zapytamy: czym jest tort, to też różne osoby będą różnie odpowiadać. Cukiernik opisujący tort widzi go jako kolejne poziome warstwy, które musi odpowiednio przygotować i w dobrej kolejności ułożyć. Łakomczuch – raczej widzi jego przekrój pionowy, stanowiący brzeg konkretnego kawałka. Jeśli zostaniemy przy gastronomii, ale przeskoczymy tym razem do piecyków kuchennych, znowu zaobserwujemy postulowaną dwoistość. Inżynier projektujący piecyk myśli o jego wydajności, o precyzji nastawienia temperatury, o tym, jak sprawić, żeby piecyk odpowiednio szybko się nagrzał itp., itd. Z kolei kucharz zakłada, że piecyk spełnia założenia podane w jego instrukcji i skupia się przede wszystkim na myśleniu, jak za jego pomocą wyczarować coś pysznego.

Spojrzenie na komputery jest w jakimś stopniu podobne do tego opisywanego wyżej. To znaczy mamy konstruktorów (fizyków, inżynierów), którzy chcą zbudować odpowiednio szybką i sprawną maszynę. Z drugiej strony, mamy użytkowników (informatyków, matematyków), którzy chcieliby z tego urządzenia po prostu korzystać. Te dwa spojrzenia mogą być bardzo różne, dlatego potrzebujemy *czegoś*, co jest odpowiednikiem instrukcji obsługi piecyka. To znaczy czegoś na tyle konkretnego, żeby konstruktorzy wiedzieli, co mają stworzyć, a z drugiej strony – na tyle abstrakcyjnego, żeby użytkownicy mogli z komputera korzystać, wcale nie znając szczegółów jego budowy. Tym *czymś* jest właśnie tytułowy formalny model obliczeń.

Zanim przejdziemy do opisów konkretnych modeli obliczeń – mała dygresja. Otóż przykład przejścia od świata fizyków i inżynierów do świata informatyków to szczególny przykład ogólniejszego zjawiska – tak zwanego *abstrahowania*. Pojęcie to ma, pozwolę sobie tutaj na arbitralne stwierdzenie, fundamentalne znaczenie w całej informatyce. Więcej – często występuje szeregowo, jako zbiór tak zwanych *kolejnych warstw abstrakcji*. Jest to z pewnością temat na cały oddzielny szczegółowy artykuł. Tym razem podam tylko ogólnikowy przykład: sieć Internet składa się z warstw abstrakcji: fizycznej, łącz danych, sieciowej, transportowej, sesji, prezentacji i aplikacji. Zawsze polega to na tym, że projektując pewną warstwę, *zapominamy* o szczegółach warstwy niższej, pozostawiając w naszej głowie tylko ogólną instrukcję jej obsługi. I dalej: efektem naszej pracy ma być nie tylko jakiś bardziej złożony produkt, ale również uproszczona instrukcja obsługi do niego. Czyli jak w życiu: równie ważne (a może i ważniejsze) od tego, z kim warto się znać i z kim się spotykać, jest to, kogo nie warto znać i gdzie nie bywać.



Obwód obliczający, czy liczba $(b_4b_3b_2b_1)_2$ zapala zaznaczony segment na wyświetlaczu kalkulatora



Po tym (przyznaję, przydługim) wstępie czas już przejść do konkretów. Zacznijmy więc od modelu obliczeń klasycznego komputera.

Dla programisty komputer to coś, co:
- ma *pamięć*, do której potrafimy *wpisać* jakieś dane;
- potrafi uruchomić zaprojektowany (w specjalnym *języku*) przez użytkownika *program* i jego wynik zapisać do pamięci;
- pozwala na odczytanie zawartości pamięci.

Oczywiście, modele takie jak wyżej mogą się istotnie różnić, zależnie od tego, jaki charakter ma pamięć (zwykle ciąg bitów ustalonej długości) oraz – przede wszystkim – jaki język opisu programu dopuszczamy. Przykładowe modele w tym duchu to: model maszyny Turinga, model maszyny RAM (*random-access machine*), interpreter języka Java czy model oparty o obwody logiczne złożone z bramek. Skupmy się na chwilę na tym ostatnim.

Model obwodów logicznych moglibyśmy opisać, na przykład, tak (modele tego typu są bardzo często stosowane do opisu układów scalonych):
- pamięć stanowią dwa wektory: $v_{\text{in}} \in \{0,1\}^n$ oraz $v_{\text{out}} \in \{0,1\}^m$. Użytkownik potrafi dowolnie ustalić wartość wektora v_{in} (czyli, żargonowo, „mamy n bitów wejściowych”).
- Użytkownik może opisać dowolną sieć co najwyżej T bramek OR, AND oraz NOT łączących wektor v_{in} z wektorem v_{out}. Wówczas komputer jest w stanie przypisać do wektora v_{out} wynik obliczeń opisanej sieci na wektorze v_{in}.
- Użytkownik po skończonym obliczeniu potrafi poznać wartość wektora v_{out}.

Przykład *programu* w tym modelu pokazuje rysunek obok.

Układ programowalny Altera Stratix IV GX FPGA realizujący model obliczeń oparty o obwody logiczne

Poziom abstrakcji w tym przykładzie jest chyba dość jasny. Inżynier projektujący tak zdefiniowany komputer (Czytelnik Lubiący Konkrety może zapoznać się z technologią FPGA) ma na celu zastanowienie się, w jaki sposób stworzyć urządzenie, które:
- zawiera i potrafi (na żądanie użytkownika) ustawić dowolnie T bramek logicznych;
- potrafi przyjąć podane przez użytkownika dane wejściowe (opis wektora v_{in});
- potrafi dokonać obliczenia i *zwrócić* użytkownikowi wynik obliczeń, czyli v_{out}.

Powyższe zadanie zapewne jest bardzo trudne, wymaga znajomości fachowej wiedzy z elektroniki, wiedzy o działaniu tranzystorów itp., itd.

Z drugiej strony: informatyk, który z takiego urządzenia chce korzystać, może zupełnie nie znać fizyki i już myśleć tylko o algorytmice, czyli – w tym przypadku

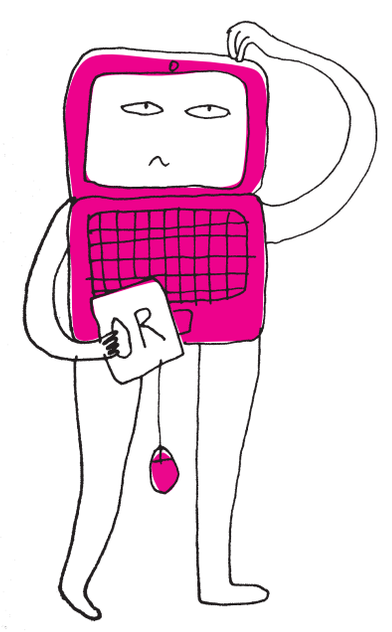
– nauce o takim przestawianiu klocków (bramek), żeby obliczało się dokładnie to, co chcemy i to możliwie szybko (a więc przy użyciu możliwie małej liczby bramek).

Przejdźmy teraz do tego, co stanowi esencję całego tego numeru *Delty*, czyli do komputerów kwantowych. Za chwilę przedstawimy formalny model obliczeń dla komputera kwantowego (czyli jego „instrukcję obsługi"). To, jakie problemy natury fizycznej napotykają projektanci takich potencjalnych komputerów, opisuje Rafał Demkowicz-Dobrzański (str. 6–9). Z drugiej strony – jakie cuda potrafiłby zdziałać informatyk mający dostęp do takiego (hipotetycznego) urządzenia opisuje Wojciech Czerwiński na stronach 10–12, przybliżając szczegóły algorytmu Shora na rozkład dużych liczb na czynniki pierwsze. Prezentowany model korzysta z języka abstrakcyjnej algebry liniowej. Podstawy tej dziedziny prezentuje Maciej Zdanowicz na stronie 5 (oraz Marek Kordos na stronie 4), przy okazji dowodząc, że programiści za kilkadziesiąt lat będą musieli znać chyba trochę więcej matematyki niż ci obecni. Na ile blisko (a na ile daleko) od stworzenia Prawdziwego Komputera Kwantowego jesteśmy w tej chwili pisze Piotr Zalewski na stronie 24. Dodatkowo w artykułach na stronach 12–15 i 16–17, kwartet Gardas, Jałowiecki, Dajka, Mierzejewski oraz (solo) Łukasz Rajkowski próbują przybliżyć Czytelnikowi, co już dziś jest komercyjnie dostępne. Po pierwsze omawiamy komputer D-Wave, który jednak realizuje (na 2048 kubitach) inny niż tu opisany model obliczeń kwantowych. Po drugie: omawiamy praktyczny protokół BB84, zakładający istnienie oraz możliwość szybkiego i taniego tworzenia „komputerów jednokubitowych" na żądanie. Gorąco zachęcam do lektury tych i innych artykułów z tego numeru i bezzwłocznie przystępuję do prezentacji modelu obliczeń kwantowych.

Istnieje więcej niż jeden model obliczeń kwantowych. Ten opisywany tutaj uznaje się za standardowy. Inne modele to np.: kwantowe automaty komórkowe, jednokierunkowe komputery kwantowe, topologiczne komputery kwantowe czy adiabatyczne komputery kwantowe. W tym numerze *Delty* odnosimy się niemal wyłącznie do modelu standardowego, z wyjątkiem artykułu ze stron 12–15, który skupia się na modelu adiabatycznym.

- Do opisu stanu pamięci komputera kwantowego potrzebne są liczby zespolone, których zbiór oznaczamy symbolem $\mathbb{C}$ (więcej o nich pisze Marek Kordos na stronie 4). Zazwyczaj operować będziemy ciągami m liczb zespolonych (tak zwanymi zespolonymi wektorami wymiaru m), których zbiór oznaczamy $\mathbb{C}^m$. (Przykładowo: $\phi = (2+i, 6, 10-3i, i) \in \mathbb{C}^4$.) Dla wektorów określamy ich długość jako pierwiastek z sumy kwadratów modułów jego kolejnych współrzędnych. W naszym przykładzie długość ϕ wynosi więc:
$$\sqrt{|2+i|^2 + |6|^2 + |10-3i|^2 + |i|^2} = \sqrt{5+36+109+1} = \sqrt{151}.$$
Opisem stanu pamięci komputera kwantowego jest jeden wektor o długości 1 z przestrzeni $\mathbb{C}^{2^n}$, np. $\psi = (0, 0, 0, \frac{1}{2}, 0, \frac{i\sqrt{2}}{2}, 0, \frac{-i}{2}) \in \mathbb{C}^{2^3}$. W świecie kwantowym często zapisujemy to samo w nieco innym (równoważnym) języku, mianowicie:
$$\psi = \frac{1}{2}|011\rangle + \frac{i\sqrt{2}}{2}|101\rangle + \frac{-i}{2}|111\rangle,$$
gdzie (jak łatwo się domyślić) $|\mathrm{bin}(k)\rangle$ oznacza wektor złożony z $(2^n - 1)$ zer i jedynki na $(k+1)$-szej współrzędnej, np. $|011\rangle = (0,0,0,1,0,0,0,0)$. Wektory $|\mathrm{bin}(k)\rangle$ nazywamy wektorami bazy standardowej. Stany pamięci, które nie są takimi wektorami, a więc są sumą co najmniej dwóch różnych wektorów bazowych, fizycy lubią nazywać *superpozycją*.
Jeśli stan pamięci jest opisany wektorem z $\mathbb{C}^{2^n}$, to mówimy, że nasz komputer operuje n kubitami. Warto zwrócić uwagę, że stan pamięci klasycznego komputera operującego n bitami opisujemy po prostu jednym ciągiem zer i jedynek długości n (np. $b_1 b_2 \dots b_n$), co możemy interpretować jako ustalenie *jednego* wektora bazy standardowej $|b_1 b_2 \dots b_n\rangle \in \mathbb{C}^{2^n}$. Przewaga komputera kwantowego polega zaś na tym, że w pamięci możemy trzymać bardziej wyrafinowane obiekty, a więc kombinacje liniowe takich wektorów (superpozycje), jak chociażby opisany wyżej wektor ψ, będący przykładem stanu pamięci komputera trójkubitowego.

$\mathrm{bin}(k)$ oznacza binarny zapis liczby k.



- Stan początkowy komputera użytkownik może ustalić zupełnie dowolnie, przy czym może używać iloczynu tensorowego do opisu (ta uwaga jest o tyle istotna, że cała przestrzeń ma wymiar wykładniczy, więc sam opis może czasem być ogromny; iloczyn tensorowy jest tu więc potencjalnym ułatwieniem). Iloczyn tensorowy $\otimes$ wektorów to bardzo prosta operacja, o której więcej piszemy na stronie 5. Na razie wystarczy nam tylko własność $|b_1 \dots b_n\rangle \otimes |b'_1 \dots b'_m\rangle = |b_1 \dots b_n b'_1 \dots b'_m\rangle$, by zrozumieć, że ten sam wektor można opisać długo bądź zwięźle:
$$\alpha = \frac{1}{4}(|0000\rangle + |0001\rangle + |0010\rangle + |0011\rangle - |0100\rangle - |0101\rangle - |0110\rangle - |0111\rangle$$
$$+|1000\rangle + |1001\rangle + |1010\rangle + |1011\rangle - |1100\rangle - |1101\rangle - |1110\rangle - |1111\rangle)$$
lub
$$\alpha = \frac{1}{4}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle).$$

$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

$$\mathrm{T} = \begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$$

$$\mathrm{CNOT} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

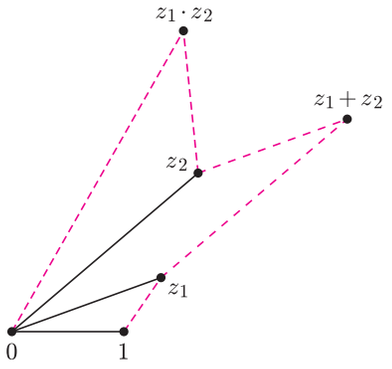
Tak naprawdę opisem obliczenia, na pewnym poziomie abstrakcji, może być dowolna macierz unitarna M z przestrzeni $\mathbb{C}^{2^n\times 2^n}$. W wyniku obliczenia stan pamięci ϕ zmienia się na $M\phi$. Użytkownik może podać dowolną macierz, co więcej, ma prawo używać iloczynu tensorowego do opisu (bezpośredni opis miałby rozmiar wykładniczy). Okazuje się, że (twierdzenie o uniwersalności) każdą macierz unitarną da się (z dowolnym przybliżeniem) uzyskać (korzystając z mnożenia i iloczynu tensorowego), mając do dyspozycji wyłącznie macierze H, T, CNOT i identyczność. Oczywiście, aby takie obliczenie było efektywne, ilość użytych macierzy podstawowych nie może być ogromna.

- Pojedyncze obliczenie na komputerze kwantowym odpowiada przemnożeniu stanu pamięci przez podaną przez użytkownika (nie byle jaką) *macierz*. W tym miejscu Czytelnik Algebraicznie Kulejący bardzo proszony jest o nieprzerażanie się tym pojęciem. Okazuje się, że nawet nie musimy dokładnie wiedzieć, jak się mnoży dowolną macierz przez wektor, bo wystarczą nam tylko trzy przykłady (dla macierzy H, T i CNOT z marginesu oraz macierz identyczności I):
$$\mathrm{H}(a|0\rangle + b|1\rangle) = \frac{1}{\sqrt{2}}\left((a+b)|0\rangle + (a-b)|1\rangle\right),$$
$$\mathrm{T}(a|0\rangle + b|1\rangle) = a|0\rangle + be^{i\pi/4}|1\rangle,$$
$$\mathrm{CNOT}(a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle) = a|00\rangle + b|01\rangle + d|10\rangle + c|11\rangle.$$
Jak widzimy macierze H i T dotyczą tylko wektorów jednokubitowych, a macierz CNOT – dwukubitowych. Aby opisać operację w wyższych wymiarach znów wolno nam się posłużyć iloczynem tensorowym, tym razem zastosowanym do macierzy. Ponownie jest to dość naturalna operacja (opisana szerzej później), a nam na razie wystarczy tylko własność $(M_1 \otimes M_2)(\phi_1 \otimes \phi_2) = M_1(\phi_1) \otimes M_2(\phi_2)$, która jest prawdziwa, gdy *wymiary się zgadzają*. Intuicyjnie oznacza ona, że rozpatrywane macierze można przykładać *lokalnie* do dowolnie wybranych współrzędnych wielowymiarowego wektora stanu pamięci. Podajmy przykład, który powinien rozjaśnić tę operację:
$$\begin{aligned}
&(\mathrm{H}\otimes\mathrm{H}\otimes\mathrm{CNOT}\otimes\mathrm{I})\left(\frac{1}{\sqrt{2}}(|01101\rangle + |10011\rangle)\right) =\\
&\quad= \frac{1}{\sqrt{2}}\big((\mathrm{H}\otimes\mathrm{H}\otimes\mathrm{CNOT}\otimes\mathrm{I})(|0\rangle\otimes|1\rangle\otimes|10\rangle\otimes|1\rangle) +\\
&\qquad + (\mathrm{H}\otimes\mathrm{H}\otimes\mathrm{CNOT}\otimes\mathrm{I})(|1\rangle\otimes|0\rangle\otimes|01\rangle\otimes|1\rangle)\big) =\\
&\quad= \frac{1}{\sqrt{2}}\big(\mathrm{H}(|0\rangle)\otimes\mathrm{H}(|1\rangle)\otimes\mathrm{CNOT}(|10\rangle\otimes\mathrm{I}(|1\rangle)) +\\
&\qquad + \mathrm{H}(|1\rangle)\otimes\mathrm{H}(|0\rangle)\otimes\mathrm{CNOT}(|01\rangle\otimes\mathrm{I}(|1\rangle))\big) =\\
&\quad= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\otimes|11\rangle\otimes|1\rangle +\right.\\
&\qquad \left. + \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|01\rangle\otimes|1\rangle\right) =\\
&\quad= \frac{1}{2\sqrt{2}}\big(|00111\rangle - |01111\rangle + |10111\rangle - |11111\rangle +\\
&\qquad + |00011\rangle + |01011\rangle - |10011\rangle - |11011\rangle\big).
\end{aligned}$$
Użytkownik może wybrać do opisu obliczenia dowolnie wybrany iloczyn tensorowy opisanych wyżej macierzy.
- Odczyt z pamięci jest w tym modelu bardzo nietrywialny. Przede wszystkim pomiar (zwykle) nie jest deterministyczny i może zwrócić różne wyniki dla tego samego stanu pamięci. Spróbujemy zaprezentować tutaj pewien uproszczony (ale wystarczający, by śledzić chociażby artykuł ze stron 10–12 o faktoryzacji Shora) opis odczytu z komputera kwantowego. Użytkownik, chcąc dokonać pomiaru pamięci w pewnym n-kubitowym komputerze, musi podać pewien podzbiór indeksów $(i_1, \ldots, i_k) \subset (1, \ldots, n)$. Jeśli teraz stan komputera to po prostu $|b_1 \ldots b_n\rangle$ (czyli pewien wektor bazowy), to uzyskamy wynik $(b_{i_1}, \ldots, b_{i_k})$. Jeśli natomiast stan komputera jest superpozycją $\sum_{v\in\{0,1\}^n}\alpha_v|v\rangle$, gdzie $\alpha_v \in \mathbb{C}$ są współczynnikami przy wektorach bazowych $|v\rangle$, to pomiar jest istotnie niedeterministyczny. Uzyskamy wynik $u = (b_{i_1}, \ldots, b_{i_k})$ z prawdopodobieństwem $P_u = \sum_{v\in S_u}|\alpha_v|^2$, gdzie S_u to zbiór tych wektorów $v \in \{0,1\}$, które na współrzędnych $i_1, \ldots, i_k$ mają dokładnie wartości $b_{i_1}, \ldots, b_{i_k}$.
W komputerze kwantowym stan pamięci po pomiarze *zmienia się* (w świecie kwantowym pomiar musi zmienić stan pamięci!) na superpozycję tych składowych starego stanu, które są *zgodne* z pomiarem. Oczywiście niektóre stare składowe nie są zgodne z pomiarem, w związku z tym te, które są zgodne, muszą mieć zmienione współczynniki, aby długość całego wektora pamięci pozostała równa 1. Konkretnie rzecz biorąc, nowy stan pamięci po pomiarze to:
$$\frac{1}{\sqrt{P_u}}\sum_{v\in S_u}\alpha_v|v\rangle.$$
Zauważmy, że po pomiarze współrzędne $i_1, \ldots, i_k$ nie będą już nigdy istotne, bo są i tak zawsze takie same dla każdej składowej.
- Użytkownik może wykonać dowolną sekwencję wielu obliczeń i odczytów (może je przeplatać).

W ogólności, przy odczycie z pamięci ϕ, użytkownik może wybrać dowolną macierz hermitowską, która – jak wiadomo z algebry liniowej – rozkłada się na sumę $\sum_i h_i P_i$ przeskalowanych rzutów na swoje podprzestrzenie własne (macierze P_i). Wynikiem pomiaru jest pewien indeks i (nic więcej nie poznajemy!), który otrzymujemy z prawdopodobieństwem $\phi^T P_i \phi$ oraz stan pamięci po pomiarze zmienia się na
$$\frac{P_i\phi}{\sqrt{\phi^T P_i \phi}}$$

Liczby zespolone czterema sposobami

Marek KORDOS



Suma to taki punkt, że $0z_1(z_1+z_2)z_2$ jest równoległobokiem; iloczyn to taki punkt, że trójkąty $01z_1$ i $0z_2(z_1\cdot z_2)$ są podobne i mają tę samą orientację.

Jeżeli określimy dodawanie i mnożenie punktów płaszczyzny, z wyróżnionymi punktami 0 i 1, w sposób przedstawiony na rysunku, to otrzymamy **liczby zespolone**. Ten szybki, jasny sposób wprowadzenia liczb zespolonych – zwany *geometrycznym* – okazał się jednak mało praktyczny. Spójrzmy teraz na te liczby inaczej, jak na wektory o początku w 0. Ponieważ wszystkie mają ten sam początek, więc będziemy je nazywać tak jak ich końce. Każdy z nich może być uzyskany z wektora 1 za pomocą podobieństwa spiralnego o środku 0 (podobieństwo spiralne to złożenie jednokładności i obrotu o tym samym środku; jedynie wtedy obojętna jest kolejność wykonywania tych przekształceń). Dodawanie liczb zespolonych w tej postaci – nazwijmy ją *wektorową* – to składanie przesunięć odpowiadających składnikom, natomiast mnożenie to składanie podobieństw spiralnych (proszę na rysunku sprawdzić, że wektor 1 przy wykonaniu podobieństw spiralnych, odpowiadających z_1 i z_2, stanie się wektorem $(z_1\cdot z_2)$).

Takie ujęcie liczb zespolonych pozwala zauważyć, że każda z nich jest określona przez liczbę r mówiącą, ile razy musiał się przedłużyć wektor 1, aby ją otrzymać i liczbę φ mówiącą, o jaki kąt wektor 1 musiał się obrócić. Pierwszą z tych liczb nazywamy modułem liczby zespolonej, a drugą argumentem. Jeżeli przedstawimy liczbę zespoloną w postaci (r,φ), to – wobec powyższych uwag – wzór na mnożenie będzie wyglądał tak:

$$(r_1,\varphi_1)\cdot(r_2,\varphi_2)=(r_1\cdot r_2,\varphi_1+\varphi_2).$$

Liczba (r,φ) ma, jak łatwo zauważyć, współrzędne kartezjańskie $(r\cos\varphi, r\sin\varphi)$, czyli $r(\cos\varphi,\sin\varphi)$.

Przetłumaczenie tego na zwykłe współrzędne kartezjańskie daje (bez rachunków!) wzór zwany nazwiskiem de Moivre'a

$$r_1(\cos\varphi_1,\sin\varphi_1)\cdot r_2(\cos\varphi_2,\sin\varphi_2)=(r_1\cdot r_2)\big(\cos(\varphi_1+\varphi_2),\sin(\varphi_1+\varphi_2)\big),$$

co łatwo się uogólnia na wzory mówiące o potęgowaniu i pierwiastkowaniu liczb zespolonych.

Trzecia postać liczb zespolonych to przedstawienie ich bezpośrednio za pomocą współrzędnych kartezjańskich. Dodawanie ma wówczas bardzo prostą postać

$$(a,b)+(c,d)=(a+c,b+d),$$

bo tak się przecież dodaje wektory. Natomiast wzór de Moivre'a pozwala zobaczyć, że i wzór na mnożenie nie jest wiele bardziej skomplikowany:

$$(a,b)\cdot(c,d)=(ac-bd,ad+bc).$$

Oto uzasadniający to rachunek:

jeśli $(a,b)=(r_1\cos\varphi_1, r_1\sin\varphi_1)$, a $(c,d)=(r_2\cos\varphi_2, r_2\sin\varphi_2)$, to

$$\begin{aligned}(a,b)\cdot(c,d)&=(r_1\cos\varphi_1,r_1\sin\varphi_1)\cdot(r_2\cos\varphi_2,r_2\sin\varphi_2)=\\&=\big((r_1\cdot r_2)\cos(\varphi_1+\varphi_2),\,(r_1\cdot r_2)\sin(\varphi_1+\varphi_2)\big)=\\&=(r_1\cdot r_2)\big(\cos\varphi_1\cos\varphi_2-\sin\varphi_1\sin\varphi_2,\cos\varphi_1\sin\varphi_2+\sin\varphi_1\cos\varphi_2\big)=\\&=\big(r_1\cos\varphi_1\cdot r_2\cos\varphi_2-r_1\sin\varphi_1\cdot r_2\sin\varphi_2,\\&\qquad\qquad r_1\cos\varphi_1\cdot r_2\sin\varphi_2+r_1\sin\varphi_1\cdot r_2\cos\varphi_2\big)=\\&=(ac-bd,ad+bc).\end{aligned}$$

Można uczynić teraz dwie obserwacje. Pierwsza to ta, że każda liczba zespolona da się przedstawić jako

$$(a,b)=a(1,0)+b(0,1).$$

Gdy $z=(a,b)$, używane są też oznaczenia $\operatorname{Re} z=a$, $\operatorname{Im} z=b$.

Zauważmy, że $(1,0)$ to po prostu 1 – każdy może sprawdzić, jak się przez $(1,0)$ mnoży. Natomiast

$$(0,1)^2=(0\cdot0-1\cdot1,0\cdot1+1\cdot0)=(-1,0),$$

co jest zwykłą minus jedynką, i to też można sprawdzić mnożąc. Liczba $(0,1)$ jest oznaczana przez i (od *imaginarius*), nazywana *jednostką urojoną* i stanowi wielką tajemnicę dla różnego rodzaju filozofów (bo jak to możliwe, aby kwadrat był ujemny...). Tak *algebraicznie* ujęte liczby zespolone to sumy $a+ib$, gdzie a i b to liczby rzeczywiste. Rachunki na nich przeprowadza się tak jak na wielomianach, pamiętając zawsze, że $i^2=-1$. Na przykład wzór na mnożenie wyprowadza się przy tej interpretacji tak:

$$(a+ib)\cdot(c+id)=ac+aid+ibc+i^2bd=(ac-bd)+i(ad+bc).$$

Jest to najstarszy i najczęściej stosowany sposób używania liczb zespolonych.

Oczywiście, można te sposoby mieszać. Często zapisuje się np. liczby w postaci algebraicznej za pomocą modułu i argumentu

$$r(\cos\varphi+i\sin\varphi).$$

Jest to szczególnie wygodne, ponieważ

$$e^{i\varphi}=\cos\varphi+i\sin\varphi,$$

ale to już inna sprawa.

Jeszcze o algebrze obliczeń kwantowych,

czyli artykuł dla Koneserów Macierzy

*Maciej ZDANOWICZ**

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

W poniższym artykule postaramy się przybliżyć Czytelnikowi niektóre podstawowe pojęcia algebry wieloliniowej nad liczbami zespolonymi, która jest podstawą rozważań w kwantowej teorii obliczeń. Bez zbędnej zwłoki przystąpimy od razu do konkretów.

Stany i bramki kwantowe. Stanem komputera kwantowego obsługującego n tak zwanych kubitów jest jakiś wektor długości 1 z $\mathbb{C}^{2^n}$. Wykorzystując bardzo sugestywną notację Paula Diraca stan s w takim komputerze może być zapisany w postaci

$$s = \sum_{(b_1 \dots b_n) \in \{0,1\}^n} s_{b_1,\dots,b_n} \cdot |b_1 \dots b_n\rangle, \qquad \text{dla} \quad s_{b_1,\dots,b_n} \in \mathbb{C}.$$

Zespolona ściągawka:
$|a+bi| = \sqrt{a^2+b^2}$,
długość $\|c\|$ wektora $c = (c_1, \dots, c_n)$ wynosi $\sqrt{|c_1|^2 + \dots |c_n|^2}$,
$\overline{a+bi} = a - bi$.

Intuicyjnie, możemy sobie więc wyobrażać, że pamięć komputera jest niedeterministyczna i znajduje się w stanie $(b_1 \dots b_n)$ z prawdopodobieństwem $|s_{b_1,\dots,b_n}|^2$. Warto zwrócić uwagę, że przy tej uproszczonej interpretacji pomijamy istotną informację pochodzącą od zespolonego *skierowania* współrzędnych stanu s.

Przystąpimy teraz do krótkiej analizy dostępnych operacji na komputerze kwantowym, które odpowiadają odwracalnym operatorom M zachowującym długości wektorów (czyli dla każdego ϕ ma być $\|M\phi\| = \|\phi\|$). Operacje te nazywamy *operatorami unitarnymi*. Dla liczby naturalnej N przez $U(N)$ oznaczać będziemy grupę przekształceń unitarnych przestrzeni $\mathbb{C}^N$. Jak łatwo się przekonać (zachęcamy do próby udowodnienia tego faktu) grupa ta może być utożsamiona ze zbiorem macierzy U rozmiaru $N \times N$ spełniających równość $U \cdot U^\dagger = I_N$, gdzie I_N jest macierzą przekształcenia identycznościowego, a operacja $U \mapsto U^\dagger$ przyporządkowuje macierzy $[u_{ij}]$ macierz $[\overline{u_{ji}}]$, np:

$$\frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}^\dagger = \frac{1}{2}\begin{bmatrix} 1-i & 1+i \\ 1+i & 1-i \end{bmatrix} \text{ oraz } \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} \cdot \frac{1}{2}\begin{bmatrix} 1-i & 1+i \\ 1+i & 1-i \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Iloczyn tensorowy. W celu zwięzłego zapisu bramek kwantowych dużych rozmiarów wykorzystuje się operację tak zwanego iloczynu tensorowego. *Iloczynem tensorowym* przestrzeni wektorowych V i W, oznaczanym $V \otimes W$, nazwiemy przestrzeń generowaną przez elementy $v \otimes w$, dla $v \in V$ i $w \in W$, spełniające liniowe zależności

$$(av + bv') \otimes w = av \otimes w + bv' \otimes w$$
$$v \otimes (aw + bw') = av \otimes w + bv \otimes w'$$

dla $v' \in V$, $w' \in W$ i $a, b \in \mathbb{C}$. Można wykazać, że dla ustalonych baz $v_1, \dots, v_n$ i $w_1, \dots, w_m$ bazą przestrzeni $V \otimes W$ są elementy $v_i \otimes w_j$.

Powyższe zależności oznaczają, że $\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^m}$ może być utożsamione z przestrzenią $\mathbb{C}^{2^{n+m}}$ za pomocą przyporządkowania określonego w bazach Diraca przy użyciu formuły $|b_1 \dots b_n\rangle \otimes |b'_1 \dots b'_n\rangle \mapsto |b_1 \dots b_n b'_1 \dots b'_m\rangle$.

Operacja iloczynu tensorowego może być również wykonana na operatorach $\phi\colon V \to V$ i $\xi\colon W \to W$. Jest ona oznaczana przez $\phi \otimes \xi$ i zdefiniowana za pomocą formuły

$$(\phi \otimes \xi)(v \otimes w) = \phi(v) \otimes \xi(w).$$

Intuicyjnie, każdy z operatorów w iloczynie tensorowym działa „niezależnie” na mniejszym podzbiorze współrzędnych.

Okazuje się (ponownie zachęcamy do próby samodzielnego udowodnienia tego faktu), że jeżeli ϕ i ξ zadane są odpowiednio przez macierze $A = [a_{ij}]$ oraz $B = [b_{km}]$ to $\phi \otimes \xi$ zadane jest przez macierz $A \otimes B$ zdefiniowaną następująco:

$$A \otimes B = \begin{bmatrix} a_{11}\begin{bmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \dots & b_{nn} \end{bmatrix} & \dots & a_{1n}\begin{bmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \dots & b_{nn} \end{bmatrix} \\ \vdots & \ddots & \vdots \\ a_{n1}\begin{bmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \dots & b_{nn} \end{bmatrix} & \dots & a_{nn}\begin{bmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \dots & b_{nn} \end{bmatrix} \end{bmatrix}.$$

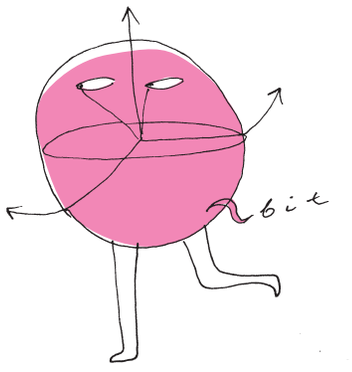
Na przykład:

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Komputery kwantowe – od Feynmana do Google'a

*Rafał DEMKOWICZ-DOBRZAŃSKI**

*Instytut Fizyki Teoretycznej, Wydział Fizyki, Uniwersytet Warszawski



„Informacja jest fizyczna" powiedział Rolf Landauer, fizyk, któremu zawdzięczamy zrozumienie faktu, że usunięcie 1 bitu informacji z pamięci komputera wiąże się z nieuniknionym wytworzeniem ciepła o wartości $kT\ln 2$, gdzie T jest temperaturą otoczenia, a k stałą Boltzmanna. Był to wynik, który pokazał, że warto myśleć o fizycznych podstawach przetwarzanej przez nas informacji, aby zrozumieć ograniczenia i perspektywy dalszego rozwoju komputerów. Dziś wiemy, że materia na poziomie mikroskopowym opisywana jest przez prawa fizyki kwantowej. Pojawia się więc naturalne pytanie, jak fakt ten odbija się na naszych możliwościach przetwarzania informacji. Czy jest to bardziej przeszkoda, związana z rozmytą naturą stanów kwantowych, powodująca, że np. elektrony nie będą chciały pozostawać dobrze zlokalizowane w sytuacji zbyt daleko idącej miniaturyzacji obwodów elektrycznych, czy może daje to nadzieję na wykorzystanie potencjału układów kwantowych mogących być „w wielu stanach jednocześnie", aby uzyskać niewyobrażalne w podejściu klasycznym zrównoleglenie obliczeń?

Warto podkreślić, że działanie dzisiejszych komputerów, które w żargonie informatyków kwantowych nazywa się klasycznymi, również oparte jest na prawach fizyki kwantowej. Pasmowa struktura półprzewodników wykorzystywana do produkcji układów scalonych jest makroskopową emanacją kwantowej natury atomów. Własności magnetyczne materii wykorzystywane do zapisu danych są ściśle związane z jedną z najbardziej kwantowych cech elementarnych składników materii, jaką jest spin. Niemniej, nawet przy obecnym postępie miniaturyzacji, na każdą elementarną bramkę logiczną w układach scalonych czy pojedynczy bit informacji zapisany w pamięci komputera przypada wciąż bardzo duża liczba atomów, rzędu miliona. Ten fakt powoduje, że tak naprawdę subtelne własności kwantowe materii nie są w pełni dostępne i kontrolowalne, więc z bardzo dobrym przybliżeniem przetwarzanie informacji w takim układzie można traktować w czysto klasyczny sposób.

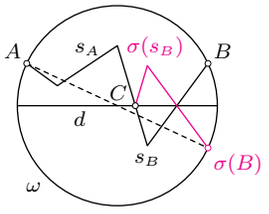
Richard Feynman w swoich wizjach rozwoju komputerów mówił: „jest bardzo dużo miejsca tam na dole", mając na myśli, że rozwijając nasze technologie wciąż pozostajemy na poziomie makroskopowym, nie wykorzystując w pełni potencjału oferowanego przez świat mikroskopowy. Stwierdzenie to, jak widać z powyższych rozważań, jest aktualne do dziś. Chciałoby się zbudować komputer operujący nie na układach milionów atomów, ale na pojedynczych atomach, wykorzystując do maksimum ich własności kwantowe – stworzyć komputer kwantowy.

Bawiąc się w futurologię, można w zasadzie przewidzieć datę powstania komputera kwantowego. Od lat 70. obserwuje się stale postępującą miniaturyzację układów scalonych, powodującą, że gęstość upakowania elementarnych komponentów elektronicznych rośnie dwukrotnie w czasie mniej więcej 18 miesięcy. Obserwacja ta znana jest pod nazwą prawa Moore'a. Mimo pewnych obaw co do utrzymania tego trendu, obserwujemy go do dzisiaj. Jeśli wierzyć, że trend ten się utrzyma, można oszacować moment, kiedy miniaturyzacja układów doprowadzi do sytuacji, że pojedynczy tranzystor będzie rozmiarów pojedynczego atomu. Powinno to nastąpić około roku 2040.

W idei komputera kwantowego nie chodzi jednak tylko o zbudowanie urządzenia wykonującego klasyczne obliczenia na układach logicznych zbudowanych z pojedynczych atomów. W przypadku obliczeń klasycznych wartości bitów mogą przyjmować wartości 0 lub 1. Myśląc o kwantowym odpowiedniku bitu, czyli np. o atomie, w którym wartość 0 lub 1 będziemy zapisywać poprzez przygotowanie atomu w jeden z dwóch różnych stanów energetycznych $|0\rangle$, $|1\rangle$, musimy pamiętać, że zgodnie z kwantową zasadą superpozycji możemy również przygotować atom w dowolnej superpozycji tych dwóch stanów $|\psi\rangle = a|0\rangle + b|1\rangle$, gdzie a, b są liczbami zespolonymi spełniającymi warunek $|a|^2 + |b|^2 = 1$, tak aby $|\psi\rangle$ był wektorem o długości 1. Taki kwantowy bit mogący znajdować się w stanie będącym dowolną superpozycją $|0\rangle$ i $|1\rangle$ nazywamy *kubitem*. Dzięki

Rozwiązanie zadania M 1549.
Oznaczmy przez A, B końce łamanej s. Niech d będzie średnicą okręgu ω równoległą do AB. Udowodnimy, że d spełnia warunki zadania.

Przypuśćmy przeciwnie, czyli że łamana s ma ze średnicą d co najmniej jeden punkt wspólny C i oznaczmy fragmenty łamanej s od punktu A do punktu C oraz od punktu C do punktu B odpowiednio przez s_A oraz s_B.



Rozważmy symetrię σ względem prostej zawierającej d. Wówczas, skoro $AB \parallel d$, to odcinek $A\sigma(B)$ jest średnicą ω, wobec czego

$$1 = |A\sigma(B)| \leqslant |s_A| + |\sigma(s(B))| = \\ = |s_A| + |s_B| = |s| < 1,$$

gdzie $|s|$, $|s_A|$, $|s_B|$ oznaczają długości odpowiednich łamanych. Uzyskana sprzeczność kończy rozwiązanie zadania.

Rozwiązanie zadania M 1550.
Udowodnimy najpierw, że dla dowolnych dodatnich liczb rzeczywistych x, y oraz dodatniej liczby całkowitej k zachodzi nierówność

$$x^2 + ky^2 \geqslant \frac{k}{k+1}(x+y)^2.$$

Rzeczywiście, przekształcając tę nierówność równoważnie, otrzymujemy

$$x^2 + kx^2 + ky^2 + (ky)^2 \geqslant kx^2 + 2kxy + ky^2,$$

$$(x-ky)^2 \geqslant 0.$$

Przyjmując w powyższej nierówności $(x, y) = (a_{k-1}, a_k)$ dla $k = 1, 2, \ldots, n$, mnożąc otrzymane związki stronami i korzystając z założenia zadania, uzyskujemy

$$\prod_{k=1}^{n}(a_{k-1}^2 + ka_k^2) \geqslant$$

$$\geqslant \prod_{k=1}^{n}\frac{k}{k+1} \cdot \prod_{k=1}^{n}(a_{k-1}+a_k)^2 =$$

$$= \frac{1}{n+1}.$$

Uwaga. Można sprawdzić, że równość w dowodzonej nierówności zachodzi wtedy i tylko wtedy, gdy

$$a_k = \frac{1}{k!}\sqrt[n]{\frac{\prod_{i=1}^{n} i!}{(n+1)!}}.$$

zasadzie superpozycji, mając np. N kubitów, możemy przygotować stan będący równoczesną superpozycją stanów, które reprezentują wszystkie liczby N bitowe. (W modelu obliczeń reprezentujemy taką superpozycję przez wektor długości 1 z przestrzeni $\mathbb{C}^{2^N}$.) Dzięki temu możliwe jest wykonanie obliczeń równolegle na wszystkich składnikach superpozycji (poprzez przemnożenie wektora zawartości pamięci przez macierz unitarną) i uzyskanie przyspieszenia obliczeń niedostępnego w ramach klasycznego modelu obliczeń. Jest to fundamentalna idea leżąca u podłoża wszystkich algorytmów kwantowych, których działanie opisane jest bardziej szczegółowo w artykule o modelu obliczeń kwantowych na stronach 1–3.

Jak więc zbudować komputer kwantowy? Pierwszą decyzją, jaką należy podjąć, jest wybór architektury obliczeń kwantowych. Najpopularniejszą, choć nie jedyną (popatrzmy chociażby na artykuł ze stron 12–15) architekturą, jest ta oparta o bramki kwantowe, które podobnie jak w podejściu klasycznym tworzą obwody logiczne realizujące obliczenia. W przypadku obliczeń klasycznych każdy obwód logiczny można zbudować z bramek typu NAND, których działanie polega na zamianie dwóch bitów wejściowych x_1, x_2 na jeden bit wyjściowy y w taki sposób, że $y = 0$, gdy $x_1 = x_2 = 1$, i $y = 1$ w pozostałych trzech przypadkach. Bramka NAND jest bramką nieodwracalną. Znając jedynie wartość bitu na wyjściu, w ogólności nie można odtworzyć wartości bitów wejściowych. Zwróćmy uwagę, że utrata jednego bitu informacji, która następuje podczas każdego użycia bramki NAND, zgodnie ze wspomnianą wcześniej zasadą Landauera musi wiązać się z wytworzeniem ciepła o wartości $kT\ln 2$. W przypadku obliczeń klasycznych możliwa jest modyfikacja bramek logicznych tak, by stały się odwracalne, poprzez przekazanie dodatkowych informacji do wyjścia bramki, unikając tym samym wytworzenia ciepła. Odbywa się to jednak kosztem komplikacji układu logicznego. Nie jest to obecnie stosowane w praktyce, gdyż energia $kT\ln 2$ jest wciąż o wiele rzędów wielkości niższa niż ciepło wydzielane w obecnie wykorzystywanych bramkach logicznych. W przypadku obliczeń kwantowych odwracalność obliczeń ma jednak kluczowe znaczenie. Nie chodzi tu jedynie o kwestię ciepła, ale o fakt, że utrata informacji o części układów kwantowych prowadzi w ogólności do tak zwanego zjawiska dekoherencji i niszczenia superpozycji stanów pozostałych kubitów. Dlatego też wszystkie algorytmy kwantowe formułowane są w języku obliczeń odwracalnych (a konkretnie za pomocą macierzy unitarnych), a ewentualne efekty nieodwracalne to efekty wynikające z niedoskonałej implementacji, przed którą należy chronić obliczenia za pomocą tzw. protokołów kwantowej korekcji błędów.

Okazuje się, że podobnie jak w obliczeniach klasycznych, dowolną operację kwantową na N kubitach można wykonać, składając ją z względnie prostych operacji elementarnych. Wystarczą do tego operacje jednokubitowe, czyli działające na pojedynczy kubit, za pomocą których można przekształcić dowolną superpozycję stanu kubitu w dowolną inną (wystarczą macierze H i T ze strony 3) oraz jeden typ bramki dwukubitowej, którą najczęściej jest tzw. bramka CNOT (controlled-NOT). Oznaczmy przez $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ stany dwóch kubitów, z których każdy ma dobrze określoną wartość logiczną 0 lub 1. Ogólny stan dwóch kubitów będzie dowolną superpozycją tych stanów. Bramka CNOT zmienia stan drugiego kubitu na przeciwny w sytuacji, gdy pierwszy kubit jest w stanie $|1\rangle$, a pozostawia go bez zmian, jeśli pierwszy kubit znajduje się w stanie $|0\rangle$:

$$\begin{array}{ll} |00\rangle & |00\rangle \\ |01\rangle \xrightarrow{\text{CNOT}} & |01\rangle \\ |10\rangle & |11\rangle \\ |11\rangle & |10\rangle \end{array}$$

Aby działanie tej bramki było rzeczywiście w pełni kwantowe, musi ona działać w sposób liniowy na dowolne superpozycje stanów wejściowych, dając na wyjściu odpowiednią superpozycję stanów wyjściowych.

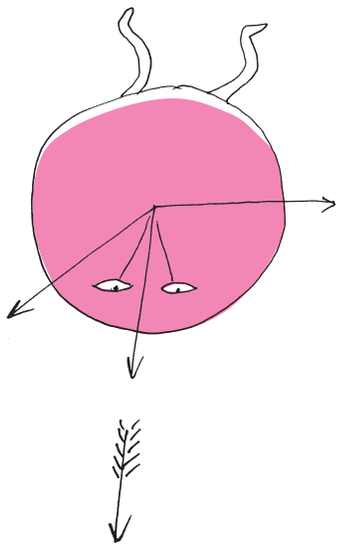
Mając już wybraną architekturę obliczeń kwantowych, możemy się skupić na jej fizycznej implementacji. Fizycy próbują budować bramki kwantowe, wykorzystując różne układy fizyczne: jony w pułapkach elektromagnetycznych, fotony poruszające się w wieloramiennych interferometrach optycznych, układy nadprzewodzące, neutralne atomy w sieciach optycznych, kropki kwantowe i wiele

Rozwiązanie zadania M 1551.
Jeżeli n jest liczbą parzystą, to żądanym przedstawieniem jest $2n - n$.

Przypuśćmy, że n jest liczbą nieparzystą i niech p będzie najmniejszą nieparzystą liczbą pierwszą, która nie jest dzielnikiem liczby n. Wówczas przedstawienie liczby n w postaci różnicy

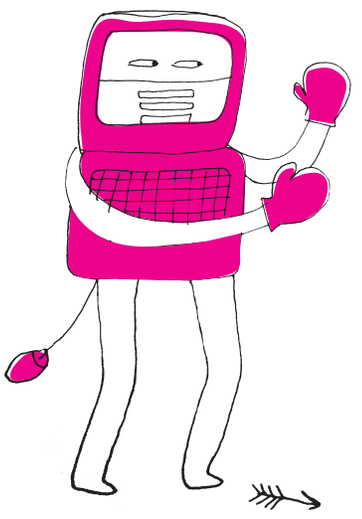
$$pn - (p-1)n$$

spełnia warunki zadania. Rzeczywiście, każda z liczb pn oraz $(p-1)n$ ma dokładnie te dzielniki pierwsze co liczba n, a ponadto po jednym dodatkowym — odpowiednio p oraz 2.



Polak potrafi

W dniach 30–31 sierpnia 2017 roku odbył się (tradycyjnie w Paryżu) międzynarodowy finał 31. Mistrzostw Świata w Grach Matematycznych i Logicznych. W finale biorą udział reprezentacje poszczególnych krajów, wyłonione w drodze krajowych eliminacji. W roku akademickim 2016/17 polskich eliminacji nie zorganizowano, jednak do organizatorów (Francuskiej Federacji Gier Matematycznych) zgłosiły się dwie osoby z Polski z prośbą o indywidualne dopuszczenie do eliminacji. Prośbę spełniono i obie dotarły do finałów w swoich kategoriach wiekowych, kontynuując w ten sposób ciąg wcześniejszych sukcesów polskich uczestników Mistrzostw: Mirosław Zajdel został mistrzem świata w kategorii GP (dorośli niezawodowcy), Robert Ciężabka zajął 7. miejsce w kategorii L2 (studenci). Zadania można znaleźć na naszej stronie.



innych. My skupimy się tutaj na eksperymentach jonowych, gdyż są one z jednej strony najłatwiejsze do zrozumienia, a z drugiej dzięki nim osiąga się największe sukcesy w realizacji bramek kwantowych.

W standardowym eksperymencie tego typu N jonów umieszczonych zostaje w tzw. liniowej elektromagnetycznej pułapce Paula, w której ruch jonów jest praktycznie jednowymiarowy. Siła odpychania kulombowskiego pomiędzy jonami powoduje, że jony znajdują się w odległościach rzędu kilku-kilkudziesięciu μm, co pozwala świecić widzialnym światłem laserowym selektywnie na każdy z jonów osobno. Podstawowym warunkiem użycia danego jonu do obliczeń kwantowych jest istnienie w nim dwóch poziomów energetycznych o długim czasie życia, które mogą pełnić rolę logicznych stanów kubitu $|0\rangle$, $|1\rangle$, a które w dalszym ciągu oznaczymy jako $|g\rangle$, $|e\rangle$, od angielskiego *ground* (podstawowy) i *excited* (wzbudzony). Przykładowo, dla jonu wapnia $^{40}Ca^{+}$ będą to stan podstawowy $^2S_{1/2}$ oraz metastabilny stan wzbudzony $^2D_{5/2}$ o czasie życia rzędu 1 s. Wszystkie jony są początkowo przygotowywane w stanie podstawowym. Następnie, świecąc przez odpowiednio dobrany czas światłem laserowym o częstotliwości ω równej częstotliwości przejścia atomowego, można doprowadzić do pochłonięcia przez jon fotonu i tym samym przeprowadzić go do stanu wzbudzonego. Jeśli operację tę zastosujemy z kolei do jonu, który początkowo był już w stanie wzbudzonym, przeprowadzimy go z powrotem do stanu podstawowego (emisja wymuszona). W ten sposób realizujemy operację, która zamienia stany $|g\rangle$ i $|e\rangle$, a tym samym otrzymujemy kwantową wersję bramki NOT. Jeśli natomiast, na jon w stanie $|g\rangle$ będziemy świecić tym samym światłem przez krótszy czas, nie doprowadzimy do pełnego wzbudzenia jonu i znajdzie się on w superpozycji stanów $|g\rangle$, $|e\rangle$. W ten sposób możemy przygotować dowolną superpozycję stanów $|g\rangle$ i $|e\rangle$, a tym samym zrealizować dowolne operacje jednokubitowe. Wiemy, że dla realizacji obliczeń kwantowych potrzebujemy jeszcze bramki dwukubitowej, np. CNOT. To jest już znacznie większe wyzwanie, gdyż musimy wykonać operację, w której ewolucja stanu danego jonu będzie zależała od stanu innego.

Z pomocą przychodzi tu fakt, że jony bardzo silnie oddziałują elektrostatycznie i w związku z tym można je wzbudzić do wspólnych drgań w pułapce. Pułapkę możemy z dobrym przybliżeniem traktować jako potencjał oscylatora harmonicznego o częstotliwości Ω, która jest rzędu setek kHz (dla porównania częstotliwość światła widzialnego jest rzędu 10^{15}Hz). Drganie jonów w pułapce jest, oczywiście, skwantowane i mogą one być wzbudzone do energii będącej całkowitą wielokrotnością $\hbar\Omega$. Rozważmy teraz dwa jony. Wprowadzimy następujące oznaczenie opisujące jednocześnie stany wewnętrzne jonów, jak i ich ruch drgający w pułapce. Przykładowo niech stan $|g\rangle \otimes |g\rangle \otimes |n\rangle$ (dalej będziemy pisać skrótowo $|g\rangle|g\rangle|n\rangle$), odpowiada sytuacji, gdy oba jony są w stanie podstawowym oraz są wzbudzone do ruchu drgającego o energii $n\hbar\Omega$. Rozważmy teraz sytuację, gdy $n = 0$, czyli stan opisujący ruch drgający jonów jest również stanem podstawowym. Jeśli teraz poświecimy na pierwszy z jonów będący w stanie podstawowym $|g\rangle$ impulsem laserowym o częstotliwości $\omega + \Omega$, wzbudzimy go do stanu $|e\rangle$, ale z uwagi na nadwyżkę energii dokonamy jednocześnie wzbudzenia kolektywnego drgań jonów o energii $\hbar\Omega$. Jeśli natomiast atom byłby początkowo w stanie $|e\rangle$, padający impuls światła o tej częstotliwości nie zmieni jego stanu. Tego typu operacja zachowuje kwantową superpozycję stanów – dlatego pod wpływem takiego impulsu stan, w którym pierwszy jon znajdowałby się w dowolnej superpozycji stanów $|g\rangle$ i $|e\rangle$, zostałby przekształcony do

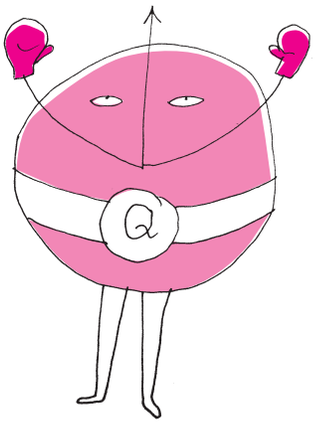
$$(a|g\rangle + b|e\rangle)|g\rangle|0\rangle \to a|e\rangle|g\rangle|1\rangle + b|e\rangle|g\rangle|0\rangle = |e\rangle|g\rangle(a|1\rangle + b|0\rangle).$$

Zwróćmy uwagę, że w ten sposób „przepisaliśmy” stan wewnętrzny jonu na stan drgań jonów w pułapce. Działając teraz z kolei na drugi jon impulsem o częstotliwości $\omega - \Omega$, będziemy mogli wzbudzić ten jon, ale jedynie w przypadku obecności kwantu energii ruchu drgającego, niezbędnego dla zachowania całkowitej energii w procesie. W efekcie przekształcimy stan do

$$|e\rangle|g\rangle(a|1\rangle + b|0\rangle) \to a|e\rangle|e\rangle|0\rangle + b|e\rangle|g\rangle|0\rangle = |e\rangle(a|e\rangle + b|g\rangle)|0\rangle.$$

Następnie świecimy impulsem o częstotliwości ω na drugi jon, wykonując na nim operację NOT, i otrzymujemy ostatecznie stan

$$|e\rangle(a|e\rangle + b|g\rangle)|0\rangle \to |e\rangle(a|g\rangle + b|e\rangle)|0\rangle.$$



W ten sposób przenieśliśmy stan wewnętrzny jonu pierwszego na drugi jon. Pokazuje to, że dzięki pośrednictwu „magistrali" wspólnych drgań jonów możliwe jest wykonywanie operacji wielokubitowych. Nieco bardziej skomplikowany wariant powyższego schematu, którego nie będziemy tu szczegółowo przedstawiać, pozwala w szczególności wykonać operację CNOT, a tym samym dysponować wszystkimi elementami niezbędnymi do zbudowania komputera kwantowego.

Dotychczas w eksperymentach tego typu udało się maksymalnie kontrolować kilkanaście jonów. Dalsze zwiększanie ich liczby prowadzi, niestety, do utraty stabilności układu, jony mogą uciekać z pułapki i pojawiają się dodatkowe efekty psujące kwantową superpozycję. Obecnie trwają prace nad „chipowymi" pułapkami jonowymi, gdzie jony znajdują się w wielu mikropułapkach, pomiędzy którymi mogą być przemieszczane za pomocą sterowania polami elektromagnetycznymi. W ten sposób można przeprowadzić w swoje pobliże jony, na których akurat w danym momencie chcemy wykonać dwukubitową operację, następnie je rozsunąć, zamienić miejscami z innymi jonami znajdującymi się w innej mikropułapce i w ten sposób uniknąć kłopotów związanych z jedną dużą pułapką, która musiałaby kontrolować wszystkie jony równocześnie. Jest to bardzo obiecująca technologia, prace nad nią trwają.

Czy faktycznie komputer kwantowy powstanie w roku 2040? Tego nie wiemy na pewno. Wiemy natomiast, że rozwój technologii związanych z próbami zbudowania komputera kwantowego doprowadził nas do sytuacji, która nie śniła się twórcom teorii kwantowej, a w której jesteśmy w stanie kontrolować i mierzyć pojedyncze układy kwantowe, takie jak atomy i fotony. W eksperymentach z pojedynczymi jonami opisanymi powyżej można w zasadzie zobaczyć pojedynczy jon gołym okiem. Przebyliśmy długą drogę od czasów, gdy eksperymentalnie dostępne nam były jedynie uśrednione wielkości fizyczne zmierzone na bardzo wielu układach kwantowych, a wizje Feynmana wydawały się jedynie spekulacjami geniusza. W ostatnich latach poza ośrodkami akademickimi w rozwijanie technologii związanych z obliczeniami kwantowymi zaczynają angażować się również najwięksi gracze na rynku informatycznym, tacy jak Google, więc może rozwój nabierze tempa ...

Zadania

Redaguje Łukasz BOŻYK

M 1549. Dany jest okrąg ω o średnicy 1 oraz łamana s o końcach należących do tego okręgu, której długość jest mniejsza od 1. Udowodnić, że istnieje średnica okręgu ω, która jest rozłączna z s.
Rozwiązanie na str. 6

M 1550. Dodatnie liczby rzeczywiste a_0, a_1, ..., a_n są takie, że $\prod_{k=1}^{n}(a_{k-1}+a_k)=1$. Udowodnić, że

$$\prod_{k=1}^{n}(a_{k-1}^2+ka_k^2)\geqslant\frac{1}{n+1}.$$

Rozwiązanie na str. 7

M 1551. Wykazać, że każdą dodatnią liczbę całkowitą można zapisać w postaci różnicy dwóch dodatnich liczb całkowitych, które mają tę samą liczbę różnych dzielników pierwszych.
Rozwiązanie na str. 7

Przygotował Michał NAWROCKI

F 941. Gdy czerwone i zielone światło są włączone przez taki sam czas, przed pewnym skrzyżowaniem tworzy się korek. Prędkość samochodów wynosząca normalnie 6 m/s w korku spada do średniej wartości 1,5 m/s (czas włączenia żółtego światła pomijamy). W celu zmniejszenia korka czas włączenia zielonego światła podwojono, nie zmieniając czasu włączenia światła czerwonego. Ile wyniesie średnia prędkość samochodów w korku, jeżeli ich normalna prędkość nie ulegnie zmianie?
Rozwiązanie na str. 10

F 942. Samochód osobowy jedzie równolegle do kolumny ciężarówek poruszających się ze stałą prędkością u w jednakowych odległościach jedna za drugą (odległość przednich zderzaków kolejnych ciężarówek wynosi l). Jeżeli samochód osobowy jedzie z prędkością $v_1 = 36\,\mathrm{km/h}$, to co $t_1 = 10\,\mathrm{s}$ jest wyprzedzany przez ciężarówkę, a jeżeli jedzie z prędkością $v_2 = 90\,\mathrm{km/h}$, to on co $t_2 = 10\,\mathrm{s}$ wyprzedza ciężarówkę. Co ile sekund ciężarówki będą mijać samochód osobowy, jeżeli zatrzyma się on na poboczu?
Rozwiązanie na str. 10

Rozwiązanie zadania F 941.
Po włączeniu zielonego światła samochody nie ruszają jednocześnie. Najpierw rusza pierwszy rząd samochodów, które stoją bezpośrednio przy sygnalizatorze, potem kolejno ruszają następne rzędy – wzdłuż korka rozchodzi się rodzaj „fali". Niech w czasie T_z, gdy włączone jest zielone światło, obok sygnalizatora przejeżdża część korka o długości L. Na czas T_z składa się czas potrzebny na to, aby „fala" przebyła drogę L i czas potrzebny, aby samochód drogę L przejechał. Jeżeli v jest prędkością samochodu (bez uwzględniania jego rozpędzania się), a u prędkością rozchodzenia się „fali", to

$$T_z = \frac{L}{v} + \frac{L}{u} = L\left(\frac{1}{v} + \frac{1}{u}\right).$$

Jeżeli czas, na który jest włączone czerwone światło wynosi T_c, to średnia prędkość poruszania się w korku wynosi $V_S = L/(T_z + T_c)$. Podstawiając, znajdujemy

$$V_S = \frac{T_z}{T_z + T_c} \cdot \left(\frac{1}{v} + \frac{1}{u}\right)^{-1},$$

a stąd dla $T_z = T_c$ otrzymujemy $u = 2vV_S/(v - 2V_S) = 6\,\mathrm{m/s}$. Po podwojeniu czasu T_z prędkość samochodu w korku wyniesie:

$$V_{2S} = \frac{2T_z}{2T_z + T_c} \cdot \left(\frac{1}{v} + \frac{1}{u}\right)^{-1} = \\ = \frac{2(T_z + T_c)}{2T_z + T_c} V_S = \frac{4}{3} V_S = 2\frac{\mathrm{m}}{\mathrm{s}}.$$

Rozwiązanie zadania F 942.
Skoro prędkość kolumny wynosi u, a odległość przednich zderzaków kolejnych ciężarówek wynosi l to $t_1 = l/(u - v_1)$ i $t_2 = l/(v_2 - u)$, gdzie $(u - v_1)$ i $(v_2 - u)$ są względnymi prędkościami samochodu osobowego i kolumny w przypadku (1) i (2). Stąd $(u - v_1)t_1 = l$ oraz $(v_2 - u)t_2 = l$. Rozwiązując ten układ równań dostajemy:

$$u = \frac{v_1 t_1 + v_2 t_2}{t_1 + t_2},$$

$$l = \frac{t_1 t_2 (v_2 - v_1)}{t_1 + t_2}.$$

Kolejne ciężarówki będą mijały stojący samochód co

$$t = \frac{l}{u} = \frac{t_1 t_2 (v_2 - v_1)}{v_1 t_1 + v_2 t_2} = 5\,\mathrm{s}.$$

Odpowiedź na zadanie ze strony 19:

$$p_1 = -3, \qquad p_2 = 5,$$
$$q_1 = -4, \qquad q_2 = 7.$$

Algorytm faktoryzacji Shora

Wojciech CZERWIŃSKI

W 1994 roku Peter Shor, pracujący wówczas w Bell Labs w New Jersey, pokazał, jak przy użyciu hipotetycznego komputera kwantowego rozłożyć w czasie wielomianowym dowolną liczbę naturalną na czynniki pierwsze. W tamtym czasie algorytmy kwantowe dopiero raczkowały. To właśnie odkrycie Shora spowodowało wielki rozwój tej dziedziny. Społeczność informatyków zrozumiała, że gdyby udało się zbudować komputer kwantowy rozsądnej wielkości, to świat stałby się istotnie inny. Nie jest bowiem znany żaden algorytm dla problemu faktoryzacji, czyli rozkładu na dzielniki pierwsze, który działa w czasie wielomianowym na komputerze klasycznym. Co więcej, nawet nie znaleziono algorytmu losowego, który z dużym prawdopodobieństwem w zazwyczaj niedługim czasie faktoryzuje liczbę: nie jest po prostu znana zupełnie żadna rozsądna heurystyka... W 1994, ale też i teraz, w 2017 roku, po prostu nie umiemy rozkładać szybko liczb na czynniki pierwsze. A na trudności faktoryzacji opiera się m.in. kryptologia, najbardziej znany kryptosystem RSA dałby się łatwo łamać, gdybyśmy umieli szybko rozkładać liczby na czynniki pierwsze. Drugim najbardziej popularnym problemem, na którego trudności opiera się wiele w kryptologii, jest problem logarytmu dyskretnego (dla danych $a, b \in \mathbb{N}$ i liczby pierwszej p znajdź k takie, że $a^k \equiv b \bmod p$). Warto wiedzieć, że w tym samym artykule Shor udowodnił również, że komputer kwantowy umie rozwiązywać problem logarytmu dyskretnego w czasie wielomianowym. Algorytm Shora nie tylko zainspirował intensywne badania w tej dziedzinie, ale chyba do tej pory jest najbardziej znanym i celebrowanym algorytmem kwantowym.

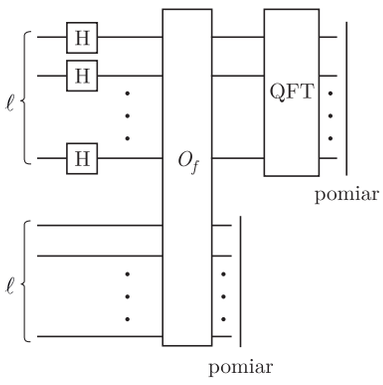
W tym artykule postaramy się zrozumieć najistotniejsze idee w algorytmie Shora. Niektóre szczegóły techniczne pominiemy, gdyż tłumaczenie wszystkiego zajęłoby raczej kilkanaście stron niż kilka.

Sprecyzujmy problem. Dostajemy liczbę $n \in \mathbb{N}$. W naszych rozważaniach skupimy się na przypadku, gdy n jest iloczynem dwóch liczb pierwszych, tj. $n = p_1 p_2$. Ten przypadek jest również trudny (nie ma dla niego żadnych szybko działających heurystyk), a algorytm Shora w ogólności działa prawie identycznie, jak dla tego przypadku. Nasz cel to znaleźć liczby p_1 i p_2. Po pierwsze powiedzmy sobie od razu, że algorytm Shora jest oparty na losowości. Uruchomiony wiele razy z pewnym dużym (bliskim 1) prawdopodobieństwem znajdzie rozkład $n = p_1 p_2$. Myślmy, że zarówno p_1, jak i p_2 mają po 100 cyfr, wtedy będziemy mieli odpowiednie wyobrażenie o tym, co się da, a czego nie da się szybko zrobić.

Pierwszy krok, niemający jeszcze żadnego związku z kwantami, to redukcja faktoryzacji do problemu *rzędu elementu* modulo n. Problem ten, dla danych $x, n \in \mathbb{N}$, pyta o najmniejsze naturalne $r > 0$ takie, że $x^r \equiv 1 \bmod n$ (takie r nazywamy *rzędem* x modulo n). Przy założeniu, że umiemy w czasie wielomianowym znajdować rząd elementu (wszędzie tu używana jest losowość, więc przestaniemy się na niej skupiać, a czasem nawet o niej wspominać), pokażemy, jak rozłożyć n na czynniki w czasie wielomianowym. Rozważmy $n = p_1 p_2$ i wylosujmy liczbę x ze zbioru $\{1, \ldots, n-1\}$. Jeśli $\mathrm{nwd}(x, n) \neq 1$ (co możemy szybko sprawdzić algorytmem Euklidesa), to świetnie, bo wtedy $\mathrm{nwd}(x, n) = p_1$ albo $\mathrm{nwd}(x, n) = p_2$ i znaleźliśmy rozkład. Ale to się zdarza rzadko. Załóżmy więc, że $\mathrm{nwd}(x, n) = 1$. Można wykazać (nie bardzo trudno, szczegóły pominiemy), że dla co najmniej jednej czwartej wylosowanych x zachodzą następujące dwa warunki: 1) r, czyli rząd x, jest parzysty, 2) $x^{\frac{r}{2}} \not\equiv \pm 1 \bmod n$. Dla takiego x mamy $n \mid (x^r - 1) = (x^{\frac{r}{2}} - 1)(x^{\frac{r}{2}} + 1)$. Jednak skoro n nie dzieli żadnego z dwóch nawiasów, to musi być tak, że p_1 dzieli jeden z nich, a p_2 drugi. Zatem $\mathrm{nwd}(n, x^{\frac{r}{2}} - 1)$ jest równe albo p_1, albo p_2. Łatwo je obliczyć algorytmem Euklidesa, a tym samym znaleźć rozkład n. A więc wystarczy skupić się na znajdowaniu rzędu liczby x modulo n, co zrobimy przy użyciu algorytmu kwantowego.

Ustalmy pewne q, które należy do przedziału $(n^2, 2n^2]$ oraz jest potęgą dwójki, niech $q = 2^\ell$. Nasz algorytm na wejściu będzie miał 2ℓ drutów, czyli będzie operował na 2ℓ kubitach (albo jeszcze inaczej: stan pamięci może być opisany

przez wektor długości 1 z $\mathbb{C}^{2^{2\ell}}$). Te 2ℓ drutów podzielimy na dwa segmenty po ℓ drutów. Zaczynamy od stanu pamięci równego 0 na wszystkich kubitach. Czyli, formalnie rzecz biorąc, jest to stan $|0\dots0\rangle$, gdzie ciąg zer ma długość 2ℓ. My jednak na potrzeby naszego algorytmu będziemy o nim myśleli jako o $|0^\ell\rangle \otimes |0^\ell\rangle$, co będziemy zapisywać w skrócie jako $|0^\ell\rangle|0^\ell\rangle$.



Cały obwód kwantowy realizujący algorytm Shora przedstawiony jest na rysunku. Wchodzi do niego 2ℓ drutów po lewej, do których po kolei aplikowane są bramki kwantowe i na końcu wykonywany jest pomiar. Fakt, że algorytm jest wielomianowy, oznacza, że w obwodzie jest wielomianowo wiele podstawowych bramek (czyli bramek Hadamarda H, obrotu T i kontrolowanej negacji CNOT, z których składamy wszystkie macierze unitarne, potrzebne do obliczeń). Teraz szczegółowo opiszemy, co dzieje się po kolei (od lewej).

Najpierw robimy to, co często robią na początek algorytmy kwantowe, czyli zamieniamy stan „same zera" na superpozycję wszystkich możliwych stanów bazowych, każdy z równym prawdopodobieństwem. Tyle, że my teraz zrobimy to tylko na pierwszych ℓ kubitach, tj. w pierwszym segmencie. Aby to zrobić, używamy, jak zawsze w takim przypadku, bramek Hadamarda

$$\mathrm{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Bramka H przekształca $|0\rangle$ na $\mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, czyli na superpozycję $|0\rangle$ i $|1\rangle$ z równym prawdopodobieństwem. Jeśli zastosujemy bramkę H do każdego z pierwszych ℓ kubitów, to stan $|0^\ell\rangle|0^\ell\rangle$ zostanie przekształcony na stan $\sum_{a=0}^{q-1}(\frac{1}{\sqrt{2}})^\ell|a\rangle|0^\ell\rangle = \sum_{a=0}^{q-1}\frac{1}{\sqrt{q}}|a\rangle|0^\ell\rangle$, gdzie przez $|a\rangle$ rozumiemy stan określony przez binarną reprezentację a, np. dla $\ell = 4$ przez $|9\rangle = |1001\rangle$. Formalnie rzecz biorąc, powyżej przyłożyliśmy do aktualnego stanu przekształcenie będące produktem ℓ macierzy Hadamarda H i ℓ macierzy identycznościowych I. Jednak warto patrzeć na to intuicyjnie, jako na przyłożenie bramki Hadamarda do każdego kubitu oddzielnie, bo takie jest właśnie znaczenie produktu tensorowego.

Następnie w algorytmie przykładamy do wszystkich drutów bramkę, która liczy funkcję $f : \mathbb{C}^{2^{2\ell}} \to \mathbb{C}^{2^{2\ell}}$ (czyli z 2ℓ kubitów w 2ℓ kubitów) taką, że

$$f(|a\rangle|0^\ell\rangle) = |a\rangle|x^a \bmod n\rangle.$$

Przypomnijmy, że x to nasza wylosowana liczba ze zbioru $\{1,\dots,n-1\}$. Na rysunku obwód obliczający funkcję f oznaczamy przez O_f. Sprawdzenie, że obliczenie funkcji f jest unitarne oraz że da się je zrealizować obwodem o wielomianowej liczbie małych bramek, nie jest specjalnie trudne. Tutaj jednak pominiemy szczegóły. A więc po przejściu przez bramkę O_f stan jest następującą superpozycją:

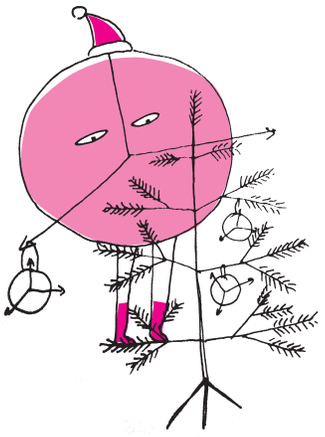
$$\sum_{a=0}^{q-1}\frac{1}{\sqrt{q}}|a\rangle|x^a \bmod n\rangle.$$

Teraz wykonujemy pomiar na drugim segmencie, czyli na drugich ℓ kubitach. W wyniku pomiaru zmierzona zostaje jakaś (nie wiemy z góry jaka!) wartość $|x^s \bmod n\rangle$. Przy czym nie wiadomo wcale, czy na pierwszych ℓ kubitach jest wartość s. Może być również tak, że jest tam wartość $s+r$, gdyż $x^{s+r} = x^s \cdot x^r \equiv x^s \cdot 1 \equiv x^s \bmod n$. Podobnie może być tam wartość $s+2r, s+3r, \dots$ Tak jak po każdym pomiarze, teraz stan układu jest superpozycją tych stanów bazowych sprzed pomiaru, które są zgodne z pomiarem.

W dalszej części rozważa się dwa przypadki. Pierwszy, gdy $r \mid q$, jest łatwiejszy, a drugi, gdy $r \nmid q$ trudniejszy. My przyjrzyjmy się pierwszemu, bo idea jest w obu przypadkach podobna, tylko w drugim jest więcej szczegółów technicznych. W tym przypadku z pomiarem $x^s \bmod n$ (dla $0 \leqslant s < r$) zgodne są wartości $s, s+r, s+2r, \dots, s+(q-r)$ na pierwszych ℓ kubitach. Zatem po pomiarze stan układu na pierwszych ℓ kubitach jest postaci

$$\frac{1}{\sqrt{q/r}}\sum_{j=0}^{(q/r)-1}|s+jr\rangle.$$

Widać teraz, że r jest jakoś związane ze stanem układu. Pytanie tylko, jak je z niego wydobyć. Jeśli zmierzymy po prostu wartość tych kubitów, to otrzymamy



pewną liczbę $s + jr$, która będzie jakąś liczbą ze zbioru $\{0, \ldots, q-1\}$, wiele nam nie powie. Nie znamy przecież s, żeby móc obliczyć jr, a tym bardziej nie znamy j, żeby obliczyć z jr wartość r. Musimy więc postępować inaczej.

Tu w sukurs przychodzi nam dziedzina, która wielu Czytelnikom zapewne wcale nie kojarzy się z faktoryzacją liczb pierwszych. Przyjrzyjmy się jeszcze raz naszemu pytaniu, z nieco innej strony. Możemy pomyśleć o naszej superpozycji jako o ciągu wartości $|a\rangle$, dla których przy większości jest współczynnik 0, ale dla niektórych niezerowy współczynnik $\frac{1}{\sqrt{q/r}}$. Te wartości o niezerowych współczynnikach powtarzają się co r i chcemy odkryć, z jakim okresem to robią. Wróćmy na chwilę do świata niekwantowego i zastanówmy się, co należy robić w takich sytuacjach, jak znaleźć okres pewnego okresowego zjawiska. Zauważmy, że nasze ucho robi to przez cały czas. Dźwięk, który słyszymy, rozkłada się bowiem na wiele składowych o różnych częstotliwościach. Ucho właśnie rozkłada dźwięk na składowe, które wyglądają jak sinusy i kosinusy. To, co robi, nazywa się w matematyce transformatą Fouriera. Okazuje się, że każdą funkcję okresową da się rozłożyć na nieskończoną sumę sinusów i kosinusów. Podobnie robi się, gdy mamy sygnał, który nie jest ciągły, lecz dyskretny. Tylko, że wtedy rozkładamy na skończoną sumę próbkowań kosinusów. Czytelnik Zapoznany Z Algebrą Liniową może sobie wyobrażać oba przekształcenia jako wyrażanie funkcji okresowej (bądź jej próbkowania) po prostu w innej bazie, złożonej z sinusów i kosinusów (bądź ich próbkowań). Ciekawostką może być, że ta sama transformata jest wykorzystywana w innych miejscach informatyki, np. w formatach jpeg lub mpeg.

A więc w świecie kwantowym, jeśli chcemy odnaleźć coś w stylu okresu w naszym stanie, też powinniśmy zastosować transformatę Fouriera, tylko że kwantową. Szczęśliwie rzeczywiście istnieje kwantowa transformata Fouriera (QFT – *quantum Fourier transform*), która okazuje się unitarna i daje się zaimplementować za pomocą wielomianowej liczby podstawowych bramek kwantowych. Przyłożenie jej do naszej konfiguracji $\frac{1}{\sqrt{q/r}} \sum_{j=0}^{(q/r)-1} |s + jr\rangle$ na wyjściu daje współczynniki przy odpowiednich okresach. Dostajemy pewną superpozycję $\sum_{j=0}^{q-1} c_j |j\rangle$. Okazuje się, że dla przypadku gdy $q \mid r$ współczynniki c_j są niezerowe jedynie dla j będących wielokrotnościami q/r. A więc możemy teraz wykonać pomiar i jesteśmy pewni, że otrzymaliśmy jakąś wielokrotność q/r. Gdy wykonamy wiele (ale wielomianowo wiele) takich pomiarów i weźmiemy minimum albo nwd, to obliczymy z dużym prawdopodobieństwem q/r. A zatem poznamy również i rząd r, co kończy naszą opowieść.

Czytelnikom Zainteresowanym Szczegółami polecamy oryginalny artykuł Petera Shora dostępny pod adresem: `arxiv.org/abs/quant-ph/9508027`.

Kwantowe wyżarzanie „klasycznej” optymalizacji

Konrad JAŁOWIECKI, Bartłomiej GARDAS, Jerzy DAJKA, Marcin MIERZEJEWSKI

Wstęp

Komputer D-Wave, opisywany w tym artykule, nie realizuje standardowego modelu obliczeń kwantowych ze stron 1–3. Realizuje tak zwany model adiabatycznych obliczeń kwantowych, który – choć jest koncepcyjnie zupełnie inny – to jest (wielomianowo) równoważny obliczeniowo modelowi standardowemu.

Wydaje się, że moc, szybkość obliczeniowa współczesnych komputerów, bazujących na krzemie, osiąga swoje plateau wynikłe z ograniczeń natury materiałowej. Jednocześnie w wielu dziedzinach życia codziennego, poczynając od prób unikania korków w planowanej podróży, poprzez minimalizację kosztochłonności produkcji aż po liczne zaawansowane zagadnienia badawcze z zakresu teorii sterowania, staramy się optymalizować nasze postępowanie. Wobec wspomnianych ograniczeń sprzętowych pozostaje nam poszukiwanie nowych algorytmów dla optymalizacji lub zupełnie nowych paradygmatów obliczeniowych – być może kwantowych?

Jak się okazuje, istnieje wcale niemała grupa zagadnień, które można wyrazić w języku fizyki poprzez przetłumaczenie ich, odwzorowanie na stary problem poszukiwania minimalizującej energię konfiguracji szkła spinowego w starym i powszechnie szanowanym modelu Isinga. Informatykowi wystarczy wiedzieć, że rzecz tyczy problemu znalezienia globalnego minimum, najmniejszej wartości funkcji wielu zmiennych o argumentach binarnych. Tak naprawdę funkcja ta opisuje energię układu, a zmienne binarne to wartości spinu w węzłach pewnej sieci.

W związku z tym, że problem poszukiwania konfiguracji szkła jest NP-trudny, to poszukiwanie nowych metod jego rozwiązywania jest bardzo ciekawe i pożądane. Jednym z przykładów takich prób jest algorytm *symulowanego wyżarzania*, w ramach którego wcześniej „podgrzany" układ w procesie powolnego „schładzania" relaksuje do szukanej konfiguracji minimalizującej energię. Inna strategia, wiążąca się z intensywnym rozwojem nowego paradygmatu obliczeniowego, nazywanego dziś powszechnie obliczeniami kwantowymi, zaowocowała powstaniem i – co bardzo ważne – komercyjną implementacją algorytmu *wyżarzania kwantowego*.

Klasyczny problem optymalizacyjny: przykład

Załóżmy, że mamy dany prosty graf nieskierowany G o wierzchołkach V i krawędziach E. W jaki sposób wydajnie podzielić V na dwa rozłączne i niepuste podzbiory tak, aby liczba krawędzi łączących wierzchołki nieznajdujące się w jednym zbiorze była możliwie największa? Mimo prostego sformułowania rozwiązanie powyższego problemu nie jest trywialne, nie jest znany ogólny algorytm pozwalający rozwiązać go w wielomianowym czasie na znanych nam z codziennej pracy klasycznych komputerach.

Zanim przedstawimy alternatywny sposób, w jaki współczesna fizyka pozwala nam zaatakować powyższy problem, spróbujmy znaleźć najpierw jego matematyczne sformułowanie, które ma, jak okaże się, wiele wspólnego ze znanym fizykom modelem Isinga. Ponumerujmy zatem wierzchołki naszego grafu kolejnymi liczbami naturalnymi. Wówczas podział zbioru V to przypisanie każdemu z wierzchołków jednej z liczb $\{0, 1\}$. Oznaczmy liczbę przypisaną i-temu wierzchołkowi przez q_i. Wtedy liczba krawędzi, które łączą wierzchołki znajdujące się w różnych podzbiorach, jest dana wzorem:

$$f(q_1, \ldots, q_n) = \sum_{\langle i,j \rangle} (q_i - q_j)^2 = \\ = \sum_{\langle i,j \rangle} q_i + q_j - 2q_iq_j, \tag{1}$$

gdzie sumowanie odbywa się po sąsiadujących ze sobą wierzchołkach, przy czym każdą parę takich wierzchołków zliczamy tylko raz. Rozwiązanie naszego problemu sprowadza się więc do znalezienia takiej konfiguracji $\{q_i\}$, dla której wartość funkcji f jest największa – lub równoważnie – wartość funkcji $H = -f$ jest najmniejsza. Zauważmy, że jeśli funkcję H interpretujemy jako „energię" układu, otrzymujemy model typu Isinga. Funkcja f ma pewną istotną cechę – jest funkcją kwadratową zmiennych zero-jedynkowych. Problemy minimalizacyjne zadane za pomocą takich właśnie funkcji, nazywane w skrócie QUBO, stanowią klasę problemów, które możemy rozwiązać za pomocą kwantowego wyżarzania. Idea jest bardzo prosta i opiera się na przejawianej przez układy kwantowe tendencji do pozostawania w stanie o najniższej energii – stanie podstawowym – o ile ich ewolucja przebiega dostatecznie wolno, czyli adiabatycznie.

Rażąco stronnicza historia informatyki kwantowej napisana w kontekście wyżarzania

Mechanika kwantowa powstała na początku XX stulecia w dość typowy dla nauki sposób: jako teoria próbująca wyjaśnić problemy i zjawiska, z którymi ówczesna fizyka nie mogła sobie poradzić. Jako pierwszy pojęciem kwantyzacji posłużył się Max Planck, który zaproponował rewolucyjny model promieniowania ciała doskonale czarnego, w którym przyjął, że energia fal elektromagnetycznych emitowanych przez ciało doskonale czarne nie jest ciągła, ale może przyjmować jedynie wartości będące wielokrotnościami pewnej elementarnej porcji (kwantu) energii. Analogiczny pomysł został zastosowany w 1905 roku przez Einsteina, który zakładając kwantowanie energii, wyjaśnił zjawisko fotoelektryczne. Dalszy rozwój mechaniki kwantowej to efekt pracy wielu słynnych fizyków.

W mechanice klasycznej opisujemy układ, podając jego położenie i pęd, jakie ma w konkretnej chwili. W mechanice kwantowej jest inaczej: opisywany przez nas układ reprezentujemy przez tzw. wektor stanu, czyli jednostkowy wektor w pewnej, dość abstrakcyjnej, przestrzeni Hilberta. Najprostszym układem kwantowym jest spin, a jako że mówimy tu o obliczeniach kwantowych – kubit. Przestrzeń Hilberta takiego układu jest dwuwymiarowa, a jej bazę tworzą dwa bity $|0\rangle$ oraz $|1\rangle$. Wielkościom obserwowalnym, obserwablom takim jak energia, odpowiadają dwuwymiarowe macierze hermitowskie dane przez kombinacje liniowe macierzy jednostkowej oraz słynnych macierzy Pauliego $\sigma_{x,y,z}$. Wartości własne obserwabli to możliwe do uzyskania w drodze pomiaru wyniki.

Przestrzeń Hilberta jest liniowa, zatem stany układu tworzą *superpozycje* – kombinacje liniowe wektorów bazy (bitów) $a|0\rangle + b|1\rangle$, gdzie skalary a, b są tak dobrane, aby spełniały warunek unormowania $|a|^2 + |b|^2 = 1$ oraz, co istotne, są liczbami zespolonymi, co, jak można się domyślić, nie ułatwia ich narysowania. To właśnie zjawisko superpozycji, niemające swojego klasycznego odpowiednika, leży u podstaw informatyki kwantowej, gdyż superpozycja bitów tworzy kubit, czyli kwantową jednostkę informacji. Wśród pomysłodawców wykorzystania kwantowych zjawisk do wykonywania obliczeń wymienić można takich fizyków jak Paul Benioff, Yuri Manin, Richard Feynman czy David Deutsch. Istnieje dziś kilka modeli obliczeń kwantowych: kwantowe obwody logiczne, kwantowe maszyny Turinga czy adiabatyczne obliczenia kwantowe. Wszystkie je łączy idea wykorzystania do obliczeń kubitów w miejsce bitów klasycznych, co czyni komputer kwantowy fundamentalnie różnym od komputera klasycznego.

Koniec XX i początek XXI wieku to okres intensywnych prac nad teorią obliczeń kwantowych i kwantowych algorytmów, jak również nad próbami fizycznych implementacji tychże teorii. Prawdopodobnie najsłynniejszym algorytmem kwantowym jest służący do faktoryzacji dużych liczb naturalnych algorytm zaproponowany w 1994 roku przez Petera Shora. Algorytm ten doczekał się kilku swoich implementacji, jednak wykorzystujących zbyt małą ilość kubitów, by można je było uznać za praktyczne, a więc zagrażające stosowanym dziś kryptosystemom. Warto wspomnieć, że istnieją inne algorytmy pozwalające na faktoryzację liczb naturalnych przy użyciu nieco innego modelu obliczeń kwantowych, przy czym ich najnowsze implementacje na komercyjnie dostępnych urządzeniach pozwalają na faktoryzację liczb rzędu kilkuset tysięcy.

Adiabatyczne obliczenia kwantowe zostały zaproponowane jako alternatywa dla obliczeń kwantowych opartych na paradygmacie sformułowanym przez Alana Turinga. Dziś wiemy, iż ta niesłychanie prosta koncepcja jest równoważna kwantowym obwodom logicznym. Idea adiabatycznych obliczeń kwantowych sprowadza się do na tyle powolnego zmieniania wybranego parametru układu, aby przez cały czas był on opisywany przez stan o najniższej chwilowej energii. Intencją tego działania jest, lub powinno być, przeprowadzenie układu ze znanego i łatwego do przygotowania stanu początkowego, który jest wektorem własnym Hamiltonianu H_0, do stanu końcowego, który jest wektorem własnym operatora H_1, a który zawiera zakodowane rozwiązanie interesującego nas problemu, takie jak poszukiwana przez nas konfiguracja szkła spinowego. Ewolucję taką można otrzymać, zmieniając w sposób ciągły parametr $s \in [0,1]$ pomiędzy dwiema ustalonymi wartościami $H(s) = (1-s)H_0 + sH_1$.

Jedynym dostępnym dziś na rynku komercyjnym urządzeniem, które realizuje opisaną powyżej procedurę, jest D-Wave 2X. Składa się on z chipa liczącego ponad 10^3 kubitów połączonych w strukturę zwaną chimerą. Fizycznie układ taki realizuje kwantowy model Isinga, a jego ewolucja w czasie to kwantowe wyżarzanie szkła spinowego. Dla $s = 0$ układ startuje ze stanu własnego H_0, gdzie wszystkie kubity ułożone są w jednym kierunku. Konfiguracja taka jest łatwa do przygotowania, wystarczy włączyć dostatecznie silne pole magnetyczne. Następnie stopniowo i wolno zmniejszamy pole. W stanie końcowym pole magnetyczne staje się zaniedbywalne, a układ, opisany przez H_1, osiąga szukaną przez nas konfigurację, którą w drodze pomiaru możemy odczytać. Jeśli wyjściowym problemem byłoby poszukiwanie konfiguracji (klasycznego) szkła spinowego minimalizującej energię $H_1 = \sum_{i,j} w_{i,j} q_i q_j$ (na przykład optymalny podział grafu z poprzedniego rozdziału dla pewnych wartości $w_{i,j}$), wówczas problem kwantowy w komputerze D-Wave otrzymuje się poprzez przypisanie zmiennej binarnej q_i macierzy Pauliego σ_z^i, czyli $q_i \to \sigma_z^i$, otrzymując $H_1 = \sum_{i,j} w_{i,j} \sigma_z^i \sigma_z^j$. Naturalnym wyborem jest wtedy $H_0 = \delta \sum_i \sigma_x^i$, przy czym δ to pole magnetyczne, za pomocą którego „wyżarzamy” rozwiązanie.

Takie podejście wiąże się z wieloma problemami. Aby dla $s = 1$ „trafić” w stan o najniższej energii, którego przecież szukamy, musimy w chwili $s = 0$ rozpocząć w stanie o najniższej energii (to w zasadzie jest proste), a potem zmieniać pole magnetyczne na tyle wolno, aby nie wzbudzić układu do stanu o wyższej energii – co już jest trudniejsze. Układ kwantowy pozostanie w stanie podstawowym, tylko gdy ewolucja przebiegać będzie adiabatycznie. Kiedy dynamika układu kwantowego jest wystarczająco wolna, aby adiabatyczne obliczenia kwantowe stały się możliwe? Niestety, odpowiedź na to pytanie jest w ogólności bardzo trudna. Pesymistycznie może się okazać, że czas chłodzenia nie jest wcale istotnie krótszy niż rozwiązanie badanego problemu przez komputer klasyczny.

Kolejny przykład: kolorowanie mapy

Pokażemy teraz, w jaki sposób możemy wyżarzyć rozwiązanie problemu kolorowania mapy. Przypomnijmy jego sformułowanie: mapę podzieloną na regiony (na przykład polityczną mapę Europy lub mapę Niemiec podzieloną na landy) chcemy pokolorować tak, aby żadne dwa sąsiednie regiony nie były tej samej barwy. Okaże się zaraz, że problem ten można sprowadzić do poszukiwania optymalnej konfiguracji spinów w modelu Isinga i użyć komputera D-Wave do jego rozwiązania. Nasza mapa to graf, którego wierzchołki to regiony mapy, a krawędź łączy dwa wierzchołki wtedy i tylko wtedy, gdy odpowiadające im regiony sąsiadują na mapie. Otrzymany w ten sposób graf jest, oczywiście, planarny, a nasz problem sprowadza się do problemu kolorowania jego wierzchołków. Klasyczny rezultat z teorii grafów mówi nam, że wystarczą nam do tego cztery kolory.

Kolejnym krokiem jest przeformułowanie naszego problemu do postaci QUBO. Fundamentalną kwestią jest ustalenie kodowania kolorów. Do zakodowania w postaci zero-jedynkowej czterech kolorów wystarczą dwa bity. Okazuje się jednak, że wybranie takiego kodowania prowadziłoby do większego skomplikowania problemu. Zamiast tego kolor i-tego regionu zakodujemy w postaci czterech bitów $q_{i1}, q_{i2}, q_{i3}, q_{i4}$, uznając, że region ten jest pokolorowany na j-ty kolor wtedy i tylko wtedy, gdy bit q_{ij} jest ustawiony na 1. Oczywiście, takie kodowanie niesie ze sobą problemy – co jeśli dwa z czterech bitów będą ustawione na 1 albo wszystkie cztery będą miały wartość 0? Mając to na uwadze, musimy sformułować nasze QUBO tak, aby niepoprawne konfiguracje były „niekorzystne energetycznie”. Innymi słowy, chcemy skonstruować funkcję kwadratową $f(q_{i1}, q_{i2}, q_{i3}, q_{i4})$, która jest zerem dokładnie wtedy, gdy jeden z jej argumentów jest jedynką oraz przyjmuje dodatnią wartość w pozostałych przypadkach. Funkcją taką jest $f(q_{i1}, q_{i2}, q_{i3}, q_{i4}) = (1 - q_{i1} - q_{i2} - q_{i3} - q_{i4})^2$. Podnosząc nawias do kwadratu i zaniedbując stałą (dodawanie stałej do QUBO nie zmienia problemu optymalizacyjnego), możemy przyjąć

$$f(q_{i1}, q_{i2}, q_{i3}, q_{i4}) = \sum_{j \neq k} q_{ij} q_{ik} - \sum_j q_{ij}. \tag{2}$$

Tak skonstruowana funkcja f, dodana z dużą stałą dodatnią do naszej funkcji celu (energii), powinna

zapewnić nam znalezienie optymalnego rozwiązania o dopuszczalnej konfiguracji.

Pozostaje skonstruowanie tego fragmentu funkcji celu, który spenalizuje rozwiązania, w których sąsiednie regiony są pokolorowane w ten sam sposób. Jeżeli i-ty oraz j-ty region sąsiadują, to dla żadnego $k = 1, 2, 3, 4$ nie może spełniona być równość $q_{ij} = q_{ik} = 1$, lub równoważnie $q_{ij}q_{ik} = 1$. Kolejnym składnikiem naszej „energii" jest więc $g(q_{ik}, q_{jk}) = q_{ik}q_{jk}$.

Ostatecznie zatem, poszukujemy konfiguracji szkła spinowego minimalizującego energię

$$H_1(\mathbf{q}) = \alpha \sum_{\langle i,j \rangle} \sum_k q_{ik}q_{jk} + \beta \sum_i f(q_{i1}, q_{i2}, q_{i3}, q_{i4}), \tag{3}$$

przy czym α i β to pewne stałe dodatnie, a notacja $\langle i, j \rangle$ oznacza sąsiadujące regiony o numerach i oraz j. Teraz wystarczy dodać H_0 i wyżarzać rozwiązanie.

Koncepcyjnie mamy już skonstruowany problem optymalizacyjny, ale, niestety, dla większości map nie wystarczy to do rozwiązania go na maszynie D-Wave. Powodem jest topologia grafu tworzonego przez kubity – graf ten, mimo sporej liczby kubitów, jest dość rzadki, ma stosunkowo mało krawędzi, co widać na rysunku na tylnej okładce. Będziemy musieli się więc uciec do tak zwanego *embeddingu*. Idea jest prosta, ale w praktyce często wymagająca w realizacji: łączymy kilka kubitów fizycznych w jeden logiczny. Taki logiczny kubit będzie miał więcej sąsiadów niż każdy ze składowych fizycznych kubitów. Wynik naszych starań widzimy na rysunku.

Łyżka dziegciu

Zaskakująco wiele problemów znanych z klasycznej teorii obliczeń daje się wyrazić w języku spinowego szkła Isinga. W szczególności można to zrobić w przypadku wszystkich 21 problemów Karpa. Czy to oznacza, że ich rozwiązanie można zawsze wyżarzyć, używając do tego maszyn D-Wave? Niestety, jeszcze nie. Jednym z powodów jest wspomniane już ograniczenie narzucane przez topologię chimery ukrytej w maszynie D-Wave: zaskakująco niewiele spośród naprawdę ciekawych problemów daje się zapisać na takim typie grafu. Co więcej, nawet jeśli okazuje się to możliwe, wcale nie jest oczywiste, czy warto to robić (może się okazać, że czas rozwiązania jest wciąż porównywalny z najlepszymi rozwiązaniami dla komputerów klasycznych). Wyniki intensywnych badań prowadzonych przez fizyków przy użyciu maszyn D-Wave oraz nad maszynami D-Wave wskazują, że oczekiwane „kwantowe przyśpieszenie" wyżarzania kwantowego nie jest wcale oczywiste. Uniwersalnym kandydatem na winnego wszelkich niepowodzeń informatyki kwantowej jest wszechobecna dekoherencja, i choć w porównaniu do wnętrza maszyn D-Wave przestrzeń kosmiczna jest całkiem ciepłym miejscem, nie można wykluczyć, że D-Wave pracuje w reżimie nie dość adiabatycznym. Nie można jednak wykluczyć, że problemem znów jest chimera, gdyż pechowym zbiegiem okoliczności, dla tego typu grafów wyżarzanie kwantowe jest nie lepsze niż klasyczne algorytmy, takie jak choćby symulowane wyżarzanie lub dynamika molekularna. Maszyny D-Wave rosną jak na drożdżach, na chimerę w ich trzewiach składa się coraz to więcej kubitów. To dobrze, gdyż daje to użytkownikom możliwość wykorzystania skutecznego embeddingu i tworzenia kubitów logicznych. Z drugiej jednak strony dopiero możliwość implementacji szerszej klasy mniej chimerycznych grafów da nam odpowiedź, czy w przyszłości będziemy wyżarzać kwantowo rozwiązanie naszych problemów optymalizacyjnych.

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

Jury Konkursu Uczniowskich Prac z Matematyki w składzie: Andrzej Komisarski – przewodniczący jury, Adam Dzedzej, Andrzej Grzesik, Kamila Łyczek, Zdzisław Pogoda, Daniel Strzelecki po wysłuchaniu w dniu 20 września 2017 roku w Lublinie prezentacji prac dopuszczonych do finału, biorąc pod uwagę dobór tematów, treść prac i sposób ich przedstawienia, postanowiło, co następuje:

• srebrne medale i nagrody w wysokości 1200 zł otrzymują prace
Podzielność silni a suma cyfr **Wojciecha Kretowicza**
z I LO im. Cypriana Kamila Norwida w Bydgoszczy
oraz
Twierdzenie Sylwestera–Gallai dla okręgów **Radosława Peszkowskiego**, **Andrzeja Szablewskiego**
z Gimnazjum im. Jana Matejki w Zabierzowie
i **Tobiasza Szemberga**
z VII Liceum Ogólnokształcącego im. Zofii Nałkowskiej w Krakowie;

• wyróżnienie i nagrodę w wysokości 300 zł otrzymuje praca *Paradoks pierwszeństwa, czyli gry zaprzeczające intuicjom o prawdopodobieństwie* **Małgorzaty Róg**
z V LO im. Augusta Witkowskiego w Krakowie.

W finale wzięły udział również prace
Słowo o quasi-kwadratach **Pawła Sawickiego**
z III LO w Gdyni
i *Diagramy* **Semena Słobodianiuka**
z Ogólnokształcącej Szkoły Muzycznej im. Zenona Brzewskiego w Warszawie.

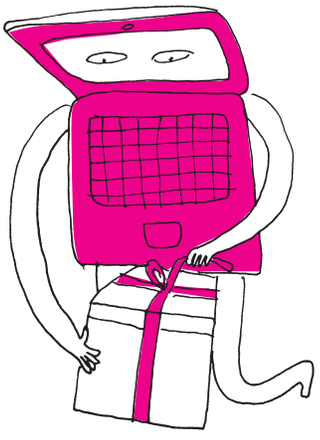
Opiekunowie prac: Mariusz Adamczak, Jacek Dymel, Tomasz Szemberg i Wojciech Tomalczyk otrzymują dyplomy honorowe.

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

Prace nadsyłane na Konkurs powinny być samodzielnie przygotowanym przez ucznia opracowaniem, zawierającym 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 2018 roku**.

BB84 zgłoś się

Łukasz RAJKOWSKI



Jak można dowiedzieć się z rozlicznych filmów akcji, nieodłączną częścią życia każdego szanującego się tajnego agenta jest wymiana tajnych informacji, najlepiej takich z wielką, czerwoną pieczęcią „Top Secret". Jeśli agent ma taką możliwość, najlepiej przekazać teczkę pełną tajemnic osobiście, jednak jest to luksus, na który może on pozwolić sobie w niewielu sytuacjach, gdyż nierzadko odbiorca tych tajemnic znajduje się na drugim końcu globu. W tej sytuacji konieczne staje się odpowiednie zaszyfrowanie naszych sekretów, aby nawet w przypadku przechwycenia ich przez oślizgłe macki szwarccharakterów, pozostały one sekretami.

Najskuteczniejszym (i najprostszym) sposobem szyfrowania jest *one time pad*, w którym tajny agent (nadamy mu kryptonim B) ustala z odbiorcą swoich wiadomości (nazywanym dalej admirałem M) klucz k, będący pewnym zerojedynkowym ciągiem. Kiedy B chce przesłać M uzyskane sekrety, najpierw konwertuje je w ustalony sposób na zerojedynkowy ciąg m (np. „a" = 00000, „b" = 00001, „c" = 00010 itd.), a następnie wysyła ciąg e (zwany *kryptogramem*), który na i-tej współrzędnej ma resztę z dzielenia przez 2 sumy i-tych współrzędnych ciągów m i k (operacja ta w informatycznej nowomowie nazywana jest *xorem* ciągów m i k i oznaczana przez $m \oplus k$). W ten sposób, jeśli tajna informacja to $m = 10110$, a $k = 10101$, to kryptogramem jest $e = 00011$. Aby odcyfrować otrzymany kryptogram, M wykonuje tę samą operację, która posłużyła B do szyfrowania – oblicza $d = e \oplus k$. Nietrudno sprawdzić, że $d = m$, mamy bowiem $d = e \oplus k = (m \oplus k) \oplus k = m \oplus (k \oplus k) = m$. Ponadto, jeśli e zostanie przechwycone przez wrogie siły (reprezentowane przez nikczemnego doktora N), to nie będą one w stanie wywnioskować stąd m, gdyż byłoby to równoważne z ustaleniem wartości klucza ($k = e \oplus m$), o którym zakładamy przecież, że jest znany tylko B i M. Słabym punktem powyższej procedury jest konieczność spotkania się B i M w celu ustalenia klucza, nie mogą go bowiem przesłać na odległość, gdyż mógłby on zostać „podsłuchany" przez doktora $N\ldots$, a może jednak mogą?

W protokole Diffiego–Hellmana agent B i admirał M ustalają najpierw dużą liczbę pierwszą p oraz niezerową resztę g z dzielenia przez p (i nie boją się , że wartości te zostaną podsłuchane). Następnie każdy z nich wymyśla sobie liczbę naturalną (oznaczmy je odpowiednio przez x i y), po czym B wysyła do M wartość $b = (g^x \bmod p)$, a M odsyła B wartość $m = (g^y \bmod p)$. Wspólnie ustalonym kluczem jest wówczas $k \equiv b^y \equiv m^x \equiv g^{xy} \bmod p$, co (jak na razie) jest trudne do obliczenia wyłącznie na podstawie p, g, b i m.

W 1976 roku Whitfield Diffie i Martin Hellman zaproponowali protokół (znany teraz pod nazwiskami twórców), który pozwala na ustalenie klucza w taki sposób, że nawet jeśli komunikacja zostanie podsłuchana, to strona podsłuchująca nie będzie w stanie odcyfrować prawdziwej wartości klucza. Protokół ten wiąże się z trudnością wykonania tzw. *logarytmu dyskretnego*, czyli odpowiedzi na pytanie w rodzaju „do jakiej potęgi należy podnieść 123, aby otrzymać resztę 321 z dzielenia przez 983?". Jak jednak można dowiedzieć się w tym numerze, w „postkwantowym" świecie z dostępem do wydajnych komputerów kwantowych logarytm dyskretny przestaje być zadaniem trudnym. Na szczęście (dla agenta B) komputery kwantowe dostarczają również nowe narzędzia do kodowania wiadomości i to takie, których w „dowodliwy" sposób same nie mogą przełamać. W tym kontekście podstawową własnością komputerów kwantowych jest fakt, że sprawdzenie stanu ich pamięci często powoduje zmianę tego stanu, co pozwala na wykrycie próby podsłuchania informacji i zerwanie połączenia, a potem poszukiwanie bezpieczniejszego kanału komunikacji. Realizacja tej idei została opisana w 1984 roku przez Charlesa Bennetta i Gillesa Brassarda, a przedstawiony przez nich protokół to tytułowy BB84.

Czytelnikowi Obeznanemu z Algebrą Liniową proponujemy upewnić się, że przedstawione wyobrażenie jednokubitowego komputera kwantowego zgadza się z modelem obliczeń kwantowych, przedstawionym przez Tomasza Kazanę na stronie 2.

Aby wytłumaczyć działanie BB84, zanurzymy się w oparach absurdu i będziemy wyobrażać sobie najprostszy, jednokubitowy komputer kwantowy jako czarną skrzynkę, w której zamknięta jest tarcza zegara wraz ze wskazówką godzinową – godzinę przez nią wskazywaną nazwiemy stanem komputera. W jaki sposób można czegoś się o nim dowiedzieć? Można poprosić komputer o porównanie swojego stanu z konkretną „eLką" – pod tym pojęciem rozumieć będziemy układ dwóch „prostopadłych" godzin, np. 1:30 i 4:30, a ogólnie godzinę h wraz z godziną $h+3$. Jeśli poprosimy komputer znajdujący się w stanie x o porównanie z eLką (h_1, h_2), to możemy otrzymać dwie odpowiedzi: h_1 z prawdopodobieństwem $\cos^2 \alpha_1$ oraz h_2 z prawdopodobieństwem $\cos^2 \alpha_2$, gdzie α_1, α_2 to kąty, jakie tworzy godzina x odpowiednio z godzinami h_1 i h_2 (prawdopodobieństwa te sumują się do 1, dlaczego?). Ponadto po przedstawieniu odpowiedzi komputer nagina do niej rzeczywistość, to znaczy zmienia swój stan na zgodny z odpowiedzią.

Dla przykładu, jeśli komputer był w stanie 4:30 i poprosiliśmy go o porównanie z eLką (2:30, 5:30), to z prawdopodobieństwem $\cos^2 60^\circ = \frac{1}{4}$

otrzymamy odpowiedź 2:30 (i wówczas stan komputera zmieni się na 2:30), a z prawdopodobieństwem $\cos^2 30^\circ = \frac{3}{4}$ usłyszymy 5:30 i taką godzinę zacznie wskazywać wskazówka wewnątrz czarnej skrzynki. Zwróćmy ponadto uwagę, że jeśli stan komputera pokrywa się z jedną z godzin z wybranej przez nas eLki, to na pewno uzyskamy tę godzinę w odpowiedzi, a stan komputera nie ulegnie zmianie. Przejdźmy do opisu protokołu. Wyróżnijmy na początku dwa rodzaje eLek: $L_0 = (0{:}00, 3{:}00)$ i $L_1 = (1{:}30, 4{:}30)$. Agent B zaopatruje się w n jednokubitowych komputerów kwantowych (gdzie n jest raczej duże) i wybiera losowo dwa ciągi zerojedynkowe: $w = (w_1, \ldots, w_n)$ oraz $l = (l_1, \ldots, l_n)$, a następnie stan i-tego komputera ustawia na godzinę s_i będącą $(w_i + 1)$-szą współrzędną eLki L_{l_i}. W ten sposób, jeśli $w_5 = 1$, $l_5 = 0$, to stan piątego komputera zostanie ustawiony na drugą współrzędną L_0, czyli na 3:00. Następnie agent B przesyła pocztą wszystkie komputery do M. Ten ostatni również ustala zerojedynkowy ciąg $l' = (l'_1, \ldots, l'_n)$ i odczytuje stan i-tego komputera przy użyciu eLki $L_{l'_i}$. Później na swojej stronie internetowej (lub innym ogólnodostępnym medium, które tylko on może edytować) udostępnia użyty ciąg l', w odpowiedzi na co agent B publikuje na swojej stronie ciąg l. Zauważmy, że wszędzie tam, gdzie $l_i = l'_i$, admirał M odczytał godzinę zakodowaną przez agenta B, a skoro wie również, jaka eLka posłużyła do jej zakodowania, pozna w_i. Zwróćmy ponadto uwagę, że szansa na to, by $l_i = l'_i$ wynosi 50%, dlatego M powinien poznać około połowy wyrazów ciągu w. Na koniec B upublicznia połowę z tych wyrazów w, które powinien był poznać M. Dlaczego?

w_i	l_i	s_i	l'_i	s'_i
1	1	↘	0	→
0	0	↑	0	↑
0	1	↗	1	↗
0	1	↗	0	→
1	0	→	1	↘
1	1	↘	1	↘
0	0	↑	0	↑
1	0	→	0	→
0	0	↑	1	↘
0	1	↗	1	↗

Przykładowy przebieg protokołu BB84. Szara czcionka występuje w wierszach, w których B i M użyli różnych eLek. Kolorem zaznaczone zostały wiersze zawierające wyrazy ciągu w upublicznione przez B. Jeśli nie pojawiły się żadne rozbieżności, wspólnym kluczem jest 001.

w_i	l_i	s_i	l_i^N	s_i^N	l'_i	s'_i
1	1	↘	0	↑	0	↑
0	0	↑	1	↘	0	↑
0	1	↗	0	→	1	↗
0	1	↗	1	↗	0	→
1	0	→	0	→	1	↗
1	1	↘	1	↘	1	↘
0	0	↑	1	↘	0	→
1	0	→	0	→	0	→
0	0	↑	1	↗	1	↗
0	**1**	↗	**0**	↑	**1**	↘

Przykładowy przebieg podsłuchiwanego protokołu BB84. W czwartej i piątej kolumnie znajdują się eLki wykorzystywane przez podsłuchującego doktora N oraz stany, w jakich odpowiednie komputery kwantowe znalazły się po niepożądanym odczycie. W ostatnim wierszu wystąpiła rozbieżność między B i M, co dowodzi zaistnienia podsłuchu.

Przypomnijmy, że cały ten ambaras miał na celu popsucie szyków nikczemnemu doktorowi N, który przechwycił paczkę z komputerami i postanowił odczytać ich stany. Poprzez odczyt stanu i-tego komputera stwarza on szansę na zmianę tego stanu i tylko w tej sytuacji możliwe jest, aby M, pomimo równości $l_i = l'_i$, odczytał złą wartość w_i. Rozpatrzmy sytuację, w której doktor N użył L_0 do odczytania stanu i-tego komputera, przy czym B i M użyli na tej współrzędnej identyczne eLki (a zatem, gdyby nie podsłuch, M na pewno poznałby wartość w_i). Jeśli B również zakodował wiadomość przy użyciu eLki L_0, to N odczytał pierwotny stan i-tego komputera (w związku z czym również w_i) i go nie zmienił, w związku z czym szpiegostwo pozostanie niewykryte. Jeśli jednak B użył L_1, to N zmienił stan komputera na którąś z godzin 0:00, 3:00 i w każdym z tych przypadków M będzie miał szansę 50% na błędny odczyt w_i. Podsumowując, jeśli doktor N wybrał eLkę L_0 do odczytu stanu i-tego komputera, to z prawdopodobieństwem 25% admirał M odczyta złą wartość w_i.

Okazuje się, że jest tak niezależnie od eLki wybranej przez doktora N (uzasadnienie jest wdzięcznym ćwiczeniem z trygonometrii). Fakt ten tłumaczy ostatnią, „kontrolną” fazę naszego protokołu: jeśli po ujawnieniu przez agenta B połowy wyrazów ciągu w, dla których $l_i = l'_i$, admirał M stwierdzi jakąkolwiek niezgodność ze swoimi odczytami, oznaczać to będzie, że komunikacja została podsłuchana i w związku z tym należy ją powtórzyć, najlepiej przy użyciu bardziej wiarygodnej poczty. Jeśli natomiast wszystkie wartości ujawnione przez B zgadzały się z odczytami M, to prawdopodobieństwo takiego zdarzenia przy założeniu o podsłuchiwaniu kanału wyniosłoby $75\%^{k/2}$ (gdzie $k \approx n/2$ to liczba indeksów i, dla których $l_i = l'_i$), co dla odpowiednio dużych wartości n jest na tyle małe, że można z czystym sumieniem odrzucić hipotezę o podsłuchu i wykorzystać nieujawnione przez agenta B i poprawnie obliczone przez M wartości w_i jako wspólny klucz.

Warto zauważyć, że doktor N mógłby odczytać stany tylko kilku komputerów kwantowych w nadziei, że pozna pewne współrzędne w, a jego podsłuch nie zostanie wykryty. W obronie przed takim zagrożeniem poznane przez M i nieopublikowane przez B wartości w poddawane są *ekstraktorom losowości* – są to specjalne funkcje, dla których znajomość niewielkiej części argumentów nie niesie ze sobą żadnej istotnej informacji o wyniku. Dopiero tak uzyskana wartość jest wykorzystywana przez B i M jako klucz.

Najwyższy czas opuścić opary absurdu i stawić czoła brutalnej, szpiegowskiej rzeczywistości – przecież żaden tajny agent nie będzie wysyłał pocztą tysiąca jednokubitowych komputerów kwantowych. Pocztą pewnie nie, ale już światłowodem bez problemu! Okazuje się bowiem (za czym stoi fizyczna magia, o której trochę piszemy w tym numerze), że jednokubitowy komputer kwantowy, ta czarna skrzynka z zamkniętym w środku zegarem, to (w rozsądnym uproszczeniu) po prostu foton, a tych przecież nie brakuje i przesyłać przy użyciu światłowodu też je można. Nie jest to jednak tanie – agenci chcący zaopatrzyć się w parę odbiorników oraz odpowiedni światłowód muszą liczyć się z wydatkiem rzędu 100 tysięcy dolarów; czego jednak się nie robi w tajnej służbie Jej Królewskiej Mości...

Kryptologia postkwantowa

Tomasz KAZANA

Jednym z ważniejszych osiągnięć informatyki opartej o komputer kwantowy, które zresztą eksponujemy w tym numerze *Delty*, jest opracowanie efektywnego (wielomianowego od rozmiaru danych) algorytmu na rozkład dużych liczb na czynniki pierwsze. Wspaniały, budzący zachwyt wynik. Nie dość, że przepiękny, korzystający z bardzo ładnego fragmentu matematyki, to jeszcze pozwalający wierzyć, że komputer kwantowy złożony z n kubitów jest *istotnie lepszy* od komputera klasycznego, zawierającego pamięć o n bitach. Albo inaczej: że (też prezentowany w tym numerze) model obliczeń komputera kwantowego ma istotnie większą siłę wyrazu (przy założeniu wielomianowego czasu działania) niż klasyczny model Turinga czy inne równoważne.

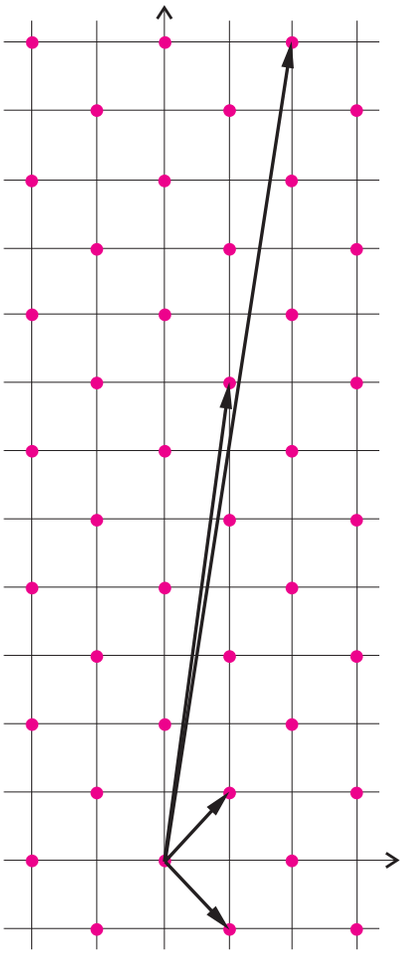
Co to znaczy w praktyce?

To znaczy, że wierzymy, iż istnieją problemy, które komputer kwantowy, mający n kubitów i wielomianowy od n czas na działanie, rozwiąże, ale już komputer klasyczny, obdarzony analogicznymi zasobami (n bitów pamięci i wielomianowy czas), im nie podoła. Hipotetycznym przykładem takiego problemu jest właśnie rozkład liczb na czynniki pierwsze. Dzięki Peterowi Shorowi wiemy, że komputer kwantowy radzi sobie z tym zadaniem. Z drugiej strony: nikt jeszcze nie potrafił pokazać, jak to zadanie rozwiązać (efektywnie) na komputerze klasycznym.

Wszystko, co powyżej, wydaje się tylko i wyłącznie zestawem dobrych wiadomości. Jednak nie do końca! W dziedzinie kryptologii istnienie lepszych niż klasyczne komputerów może powodować problemy. No bo przecież bezpieczeństwo większości protokołów kryptologicznych opiera się na założeniu, że jakiś problem jest bardzo trudny. Gdy nagle dostajemy nowe potężne narzędzie, może się przecież okazać, że pewne problemy nagle stają się już łatwe! Nie jest to wcale czcze gadanie, co od razu pokazuje algorytm Shora: przecież szyfrowanie RSA opiera się na trudności faktoryzacji, więc nie będzie ono miało sensu w świecie postkwantowym.

Kryptolodzy stoją więc przed konkretnym wyzwaniem. Chcąc przygotować świat na nadejście komputerów kwantowych, muszą projektować protokoły oparte na trudności problemów innych niż rozkład na czynniki pierwsze. Takie inne założenia w świecie kryptologów oczywiście istnieją: często zakładamy chociażby trudność problemu logarytmu dyskretnego (np. w protokole Diffiego–Hellmana), czy problemu logarytmu w grupie krzywych eliptycznych (np. w podpisie cyfrowym ECDSA). Niestety! Oba te założenia również potrafimy rozwiązywać efektywnie za pomocą (hipotetycznego) komputera kwantowego...

Dziedzina kryptologii postkwantowej rozwija się naprawdę prężnie. Na wszystkich czołowych konferencjach kryptologicznych (CRYPTO, EUROCRYPT, TCC) zawsze co najmniej jedna sesja jest ostatnio przeznaczana na ten temat. Co więcej, w roku 2006 po raz pierwszy odbyła się – i odbywa rokrocznie do dziś – konferencja PQCrypto, dedykowana wyłącznie tematyce postkwantowej w kryptologii.



Czytelnik Pełen Obaw zapewne w tym miejscu zastanawia się, czy może nie jest przypadkiem tak, że po prostu komputer kwantowy zaatakuje skutecznie *wszystkie* potencjalne protokoły kryptologiczne, bo, na przykład, będzie potrafił rozwiązać szybko każdy problem z klasy NP. Większość badaczy nie jest jednak aż tak pesymistyczna w tym temacie. To znaczy, o ile wierzy się, że komputer kwantowy *jest* lepszy od klasycznego, to jednak intuicja informatyków powszechnie skłania ich ku hipotezie, że nie jest on w stanie szybko rozwiązywać problemów NP-zupełnych.

Powyższy pogląd daje nadzieję na bezpieczną kryptologię postkwantową. Co więcej, mamy już kandydatów na problemy, które *wydają* się trudne dla komputera kwantowego. Mamy także gotowy dość szeroki wachlarz konkretnych protokołów opartych na tych założeniach. Przykładów takich protokołów tutaj podawać tym razem nie będziemy, ale chcemy przynajmniej zaprezentować problem, który przyjmujemy jako trudny w świecie postkwantowym. (Co oznacza, że badacze tej dziedziny starają się redukować do niego inne protokoły.) Opowiemy o problemie najmniejszego wektora w kracie (*shortest vector problem*, w skrócie SVP).

Załóżmy, że mamy dane n wektorów $v_i \in \mathbb{Z}^k$. Kratą całkowitoliczbową rozpiętą przez te wektory nazywamy zbiór

$$B = \left\{ u \in \mathbb{Z}^k : u = \sum_{i=1}^{n} x_i v_i \text{ dla pewnych } x_i \in \mathbb{Z} \right\}.$$

Pytamy teraz o najkrótszy (w sensie zwykłej metryki euklidesowej) niezerowy wektor w zbiorze B.

Powyższy problem (oczywiście dla odpowiednio dobranych parametrów n i k oraz umiejętnie wylosowanych wektorów v_i) uchodzi za bardzo trudny nawet dla komputera kwantowego.

Popatrzmy jeszcze przez chwilę na bardzo małe instancje problemu SVP. Proponuję dwie zagadki. Najpierw zerknijmy na zestaw: $v_1' = (1, 1)$, $v_2' = (1, -1)$, a następnie na: $v_1'' = (1, 7)$, $v_2'' = (2, 12)$.

Pytamy, oczywiście, o najmniejszy niezerowy wektor w kratach rozpiętych przez te zestawy wektorów.

W pierwszym przypadku dość łatwo zauważyć (i udowodnić), że najmniejszymi wektorami (poza dwoma innymi, symetrycznymi względem zera) są właśnie wejściowe v'_1 i v'_2. Co ciekawe, w drugiej zagadce, mimo że wejściowe wektory wyglądają groźniej, to rozpinana przez nie krata jest dokładnie tą samą kratą (czemu?), więc najmniejsze wektory to ponownie $(1,1), (1,-1), (-1,-1)$ oraz $(-1,1)$.

Podane przykłady mają na celu ilustrację jeszcze jednej własności problemu SVP. Otóż dla ustalonej kraty istnieją różne zestawy wektorów ją definiujące (tzw. bazy), co więcej: problem SVP dla różnych baz tej samej kraty może być istotnie trudniejszy. Czytelnik Domyślny, któremu kojarzy się to z kryptografią opartą o klucze prywatne i publiczne, nie myli się.

PS. Czytelnik-Profan może być z kolei zaniepokojony nadużywaniem w tym tekście zwrotów takich jak *wydaje się*, *pozwalający wierzyć* itp. Nie jest to jednak przypadek, a o tym, że kryptologia to nauka dla ludzi dużej wiary, próbowałem przekonać Czytelników już w numerze 10/2017 *Delty*.

Czytelnikowi Sumiennemu proponujemy znalezienie takich liczb całkowitych p_1 i p_2 oraz q_1 i q_2, aby było

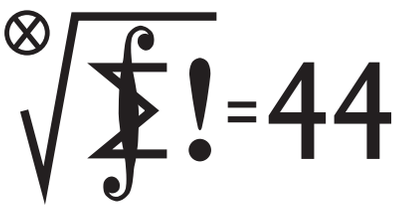
$$p_1 v''_1 + p_2 v''_2 = v'_1$$

i

$$q_1 v''_1 + q_2 v''_2 = v'_2.$$

Odpowiedź zamieściliśmy w numerze.

Klub 44

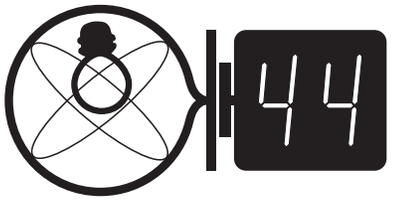


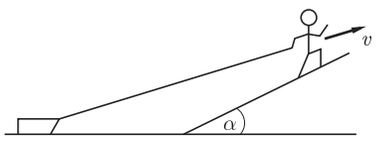
Termin nadsyłania rozwiązań: 28 II 2018

Czołówka ligi zadaniowej **Klub 44 M** po uwzględnieniu ocen rozwiązań zadań 741 ($WT = 1{,}82$) i 742 ($WT = 1{,}55$) z numeru 5/2017

Jerzy Cisło	Wrocław	47,31
Janusz Olszewski	Warszawa	46,79
Marcin Małogrosz	Warszawa	44,23
Adam Dzedzej	Gdańsk	43,22
Marcin Kasperski	Warszawa	42,59
Patryk Jaśniewski	Gdańsk	42,49
Roksana Słowik	Knurów	41,91
Franciszek S. Sikorski	Warszawa	39,71
Krzysztof Maziarz	Kraków	37,45

Widywaliśmy już te nazwiska – prawda?
Jerzy Cisło – po raz trzynasty.
Janusz Olszewski – po raz osiemnasty.
Marcin Małogrosz – po raz drugi.





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 przesyłać w oddzielnych kopertach, umieszczając na kopercie dopisek: **Klub 44 M** lub **Klub 44 F**. 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 751, 752

Redaguje Marcin E. KUCZMA

751. Trójkąt równoboczny o boku długości n został podzielony (prostymi równoległymi do boków) na n^2 trójkątów o boku 1 (trójkątów jednostkowych). Wierzchołkom powstałej siatki zostały przyporządkowane różne liczby rzeczywiste ($(n+1)(n+2)/2$ różnych liczb). Trójkąt jednostkowy nazwiemy zorientowanym dodatnio, jeśli – idąc wzdłuż jego brzegu, w kierunku wzrastania liczb przy wierzchołkach (tj. startując od najmniejszej i idąc przez średnią do największej) – mamy jego wnętrze po lewej stronie. Dla ustalonej liczby naturalnej n wyznaczyć najmniejszą i największą możliwą wartość liczby trójkątów jednostkowych zorientowanych dodatnio.

752. Znaleźć wszystkie pary liczb całkowitych dodatnich, których średnia arytmetyczna i średnia geometryczna różnią się o 1.

Zadanie 752 zaproponował pan Witold Bednarek z Łodzi.

Zadania z fizyki nr 648, 649

Redaguje Elżbieta ZAWISTOWSKA

648. Człowiek wchodzi ze stałą prędkością v na zbocze nachylone pod kątem α do poziomu (rysunek) i ciągnie sanki o masie m za pomocą nierozciągliwej, lekkiej linki o długości l. Sanki ślizgają się bez tarcia po powierzchni poziomej. Jakie jest naprężenie linki, gdy tworzy ona z poziomem kąt α?

649. Na bardzo cienką przezroczystą płytkę naniesiono nieprzezroczyste, koncentryczne pierścienie. Położenia i rozmiary pierścieni są tak dobrane, że równoległa wiązka światła o długości fali $\lambda = 500$ nm, padająca prostopadle na płytkę, ogniskuje się w odległości $f = 25$ cm od płytki. Rozmiary płytki są małe w porównaniu z odległością f.
a) Wyznaczyć promienie wewnętrzne i zewnętrzne dwóch najbliższych centrum nieprzezroczystych pierścieni.
b) W jakiej odległości od płytki powstanie obraz punktowego źródła światła monochromatycznego o tej samej długości fali co wiązka równoległa, umieszczonego w odległości a od płytki na jej osi przechodzącej przez środki pierścieni?

Informatyczny kącik olimpijski (110): Liczby

W tym miesiącu omówimy zadanie *Liczby*, które pojawiło się podczas rundy 72. na portalu `codeforces.com`.

W zadaniu należy, mając dane liczby naturalne $a, b, k \leqslant 2 \cdot 10^9$, wyznaczyć liczbę liczb naturalnych w przedziale $[a, b]$, których najmniejszym dzielnikiem, większym od 1, jest k. Zauważmy najpierw, że wystarczy umieć obliczać wyniki dla przedziałów postaci $[1, n]$, ponieważ wynik dla przedziału $[a, b]$ jest różnicą wyników dla przedziałów $[1, b]$ i $[1, a-1]$. Ponadto, jeśli k nie jest liczbą pierwszą, to wynik jest równy 0, ponieważ jeśli liczba jest podzielna przez k, to jest też podzielna przez każdy dzielnik k, a skoro k nie jest pierwsza, to ma dzielnik większy od 1 i mniejszy od k. Załóżmy teraz, że k jest pierwsza. Zadanie można rozwiązać w czasie $O(n \log\log n)$, wyznaczając dla każdej liczby z przedziału $[1, n]$ jej najmniejszy dzielnik, większy od 1, za pomocą sita Eratostenesa. Rozwiązanie to dla $n \leqslant 2 \cdot 10^9$ jest dalece niewystarczające. Zauważmy, że można je łatwo usprawnić. Każda liczba, której najmniejszy dzielnik jest równy k, jest postaci $k \cdot m$, gdzie m nie ma dzielników większych od 1 i mniejszych od k. Wystarczy zatem zliczyć takie m-y z przedziału $\left[1, \left\lfloor \frac{n}{k} \right\rfloor\right]$, które nie mają dzielników pierwszych mniejszych od k. Można to zrobić, iterując kolejne liczby pierwsze mniejsze od k i zaznaczając w tablicy liczby podzielne przez którąś z nich.

Rozwiązanie to wykona dla każdej liczby pierwszej p, mniejszej od k, $\frac{n}{kp}$ operacji, czyli łącznie

$$\frac{n}{k} \sum_{p \in \mathbb{P},\, p<k} \frac{1}{p} = \Theta\left(\frac{n}{k} \log\log k\right).$$

Dla $k \geqslant 100$ rozwiązanie takie jest wystarczające. Jeśli natomiast k jest mniejsze od 100, to liczb pierwszych mniejszych od k jest nie więcej niż 25. Niech teraz A_p oznacza zbiór liczb podzielnych przez k oraz p leżących w przedziale $[1, n]$. Naszym zadaniem jest obliczenie

$$\left| \{x \in [1, n] : k \mid x\} \setminus \left(\bigcup_{p \in \mathbb{P},\, p<k} A_p \right) \right|.$$

Możemy to zrobić, korzystając z zasady włączeń i wyłączeń. W tym celu musimy umieć obliczyć $|A_{p_1} \cap A_{p_2} \cap \ldots \cap A_{p_i}|$. Jest to zbiór liczb podzielnych przez $kp_1p_2 \ldots p_i$, leżących w przedziale $[1, n]$, czyli ma $\left\lfloor \frac{n}{kp_1p_2 \ldots p_i} \right\rfloor$ elementów.

Całe rozwiązanie działa w czasie

$$O\left(\min\left(2^{\pi(k)}, \frac{n}{k} \log\log k\right)\right).$$

Na to zadanie można też spojrzeć inaczej. Niech $F(n, p)$ będzie liczbą liczb w przedziale $[1, n]$, które nie mają dzielników większych od 1 i mniejszych od p. Wykażemy, że

$$F(n, p) = n - \sum_{q \in \mathbb{P},\, q<p} F\left(\left\lfloor \frac{n}{q} \right\rfloor, q\right)$$

Istotnie, liczb nie większych od n, których najmniejszym dzielnikiem jest q, jest $F\left(\left\lfloor \frac{n}{q} \right\rfloor, q\right)$, ponieważ każda taka liczba jest postaci $q \cdot m$, gdzie m nie ma dzielników większych od 1 i mniejszych od q, a $q \cdot m \leqslant n$, czyli $m \leqslant \left\lfloor \frac{n}{q} \right\rfloor$. Wszystkich liczb w przedziale $[1, n]$ jest n, a każda z nich albo ma dzielnik pierwszy mniejszy od p, wówczas zostanie odjęta dokładnie raz, dla q będącego jej najmniejszym dzielnikiem pierwszym, albo nie ma i wtedy nie zostanie odjęta. Liczba liczb w przedziale $[1, n]$, których najmniejszym dzielnikiem jest k, jest równa $F(\left\lfloor \frac{n}{k} \right\rfloor, k)$. Zadanie można rozwiązać, obliczając wartość funkcji F, rekurencyjnie korzystając z tego wzoru. Niech $p_1, p_2, \ldots$ będą kolejnymi liczbami pierwszymi, a $T(n)$ liczbą operacji wykonanych przez algorytm dla liczby pierwszej p_n. Wówczas $T(n) = 1 + \sum_{i=1}^{n-1} T(i)$. Rozwiązaniem tego równania jest $T(n) = \Theta(2^n)$, czyli całe rozwiązanie będzie działało w czasie $O(2^{\pi(k)})$, co jest zdecydowanie za wolne.

Rozwiązanie to można łatwo przyspieszyć. Wystarczy zauważyć, że jeśli $n < p$, to jedyną liczbą w przedziale $[1, n]$ niemającą dzielników większych od 1 i mniejszych od p jest 1, więc $F(n, p) = 1$ i w każdym wywołaniu rekurencyjnym obliczającym wynik dla $n < p$ zwracać $\min(1, n)$ bez dalszych wywołań rekurencyjnych. Wykażemy, że rozwiązanie z tą optymalizacją obliczające $F(n, p)$ wykona co najwyżej $O(n)$ wywołań rekurencyjnych. Rozważmy gałąź w drzewie rekursji, w której algorytm wykonał kolejno dzielenia przez $p_1, p_2, \ldots, p_i$. Oznacza to, że w przedostatnim wywołaniu obliczał $F\left(\left\lfloor \frac{n}{p_1p_2 \ldots p_{i-1}} \right\rfloor, p_{i-1}\right)$. Skoro nie zwrócił wyniku od razu, tylko wykonał następne wykonanie rekurencyjne, to $\left\lfloor \frac{n}{p_1p_2 \ldots p_{i-1}} \right\rfloor \geqslant p_{i-1}$, skąd wynika, że $\frac{n}{p_1p_2 \ldots p_{i-1}} \geqslant p_{i-1}$, czyli $n > p_1p_2 \ldots p_{i-2}p_{i-1}^2$. Algorytm w danym wywołaniu przegląda jedynie liczby pierwsze, mniejsze od poprzedniej, zatem $p_{i-1} > p_i$, skąd otrzymujemy $n > p_1p_2 \ldots p_i$. Liczby p_i są pierwsze, więc dla różnych wywołań rekurencyjnych iloczyny $p_1p_2 \ldots p_i$ będą parami różne, więc liczba tych wywołań nie przekroczy n.

Prezentowane rozwiązanie potrzebuje listy liczb pierwszych mniejszych od $\min(n, p)$. Można ją, oczywiście, wyznaczyć, używając sita Eratostenesa, w czasie $O(\min(n, p) \log(\min(n, p)))$. Ostatecznie, całe rozwiązanie obliczające $F\left(\left\lfloor \frac{n}{p} \right\rfloor, p\right)$ działa w czasie

$$O\left(\min\left(2^{\pi(k)}, \frac{n}{k}\right)\right).$$

Konrad PALUSZEK

Wyplatanie komputera kwantowego

Wyplatanie było ważnym osiągnięciem technologicznym, dzięki któremu tworzono powrozy, koszyki, łapcie, płoty, tkaniny itp. Z drugiej strony czynność ta nie zawsze była poważana, o czym świadczy powiedzenie „pleść trzy po trzy".

Komputery kwantowe (KK) okazują się łączyć oba aspekty plecenia. Patrząc z tej drugiej strony, specjaliści obiecują wiele, albo i więcej, ale dopiero (albo „i to już") jutro [1]. Nie wiadomo jednak, z czego KK miałby być ostatecznie wyrzeźbiony.

Podejścia są w zasadzie trzy, choć kryteria tego podziału nie są jednolite. Parafrazując, można powiedzieć, że KK może być np. zielony, kwadratowy lub konopny.

Jeden odłam to podejście „analogowo-kwantowe", które już jest wykorzystywane praktycznie np. przez D-Wave (patrz str. 12). Drugie to dążenie do wykazania tzw. przewagi kwantowej [2] za pomocą relatywnie małych macierzy kubitów (np. 7×7). Układy te mają, w zasadzie, działać według standardowego modelu obliczeń kwantowych (patrz str. 1–3). To, czego im będzie brakować, to korekcja błędów, która wymaga nadmiarowej liczby kubitów. Google twierdzi, że to już znajdzie zastosowanie praktyczne czy wręcz komercyjne, a usługę chce świadczyć poprzez chmurę [3]. W tym podejściu sprawą nadal otwartą jest technologia tworzenia kubitów (Google ma konkurentów).

O ostatnim podejściu jeszcze w tym numerze *Delty* nie pisaliśmy. Chodzi o tytułowe wyplatanie, czyli topologiczny komputer kwantowy. Jest to coś, co ma szansę rozwiązać wszystkie problemy, tylko na razie nie wiadomo, czy to, z czego ma zostać wypleciony, w ogóle istnieje, albo czy to, co wygląda na istniejące, jest tym, czym się być wydaje.

Za ojca chrzestnego tego nurtu można uznać Kitajewa [4], który właśnie za to został pięć lat temu jednym z pierwszych laureatów *Fundamental Physics Prize* (Δ^2_{13}). Chodzi o jeden ze sposobów wykorzystania *topologicznych stanów materii* (TSM), za odkrycie których przyznano zeszłoroczną *Nagrodę Nobla z Fizyki* (Δ^1_{17}).

Nibymateriałem potrzebnym do tej plecionki mają być anyony i to koniecznie w postaci nieabelowego TSM, a najlepszym kandydatem na te nibycząstki (pseudocząstki, kwazicząstki) wydają się być fermiony Majorany.

O co dokładnie chodzi, nie napiszę. Mógłbym zasugerować, że nie ma tu wystarczająco dużo miejsca, ale powód jest dużo prostszy – nie czuję się kompetentny. Polecam natomiast opracowanie [5], przynajmniej jeżeli chodzi o sam anyonowy TSM. Można też zapoznać się z amerykańskim patentem [6].

Anyony to kolektywne ekscytacje w materii o obniżonej liczbie wymiarów. W trójwymiarze identyczne (niby)cząstki mogą być albo fermi-onami, albo bos-onami, dla których podwójna zamiana cząstek jest operacją albo antysymetryczną (faza $e^{i\pi}$), albo symetryczną (e^{i0}), bo linie świata cząstek nie zapętlają się – w przeciwieństwie do sytuacji w dwóch wymiarach. Dlatego faza może być tam dowolna ($e^{i\theta}$) i stąd nazwa: any-on. Zaplatanie anyonów jest opisywane za pomocą (nieabelowej) grupy warkoczowej zamiast uboższej grupy permutacji.

Fermiony Majorany, o które w kontekście KK budowanego z TSM chodzi, to nibycząstki będące połączeniem połowy elektronu z połową dziury. Nie mają ładunku, nie mają masy, są swoimi własnymi antycząstkami i występują parami. Powinny się pojawiać w jednowymiarowych nadprzewodnikach z polem magnetycznym skierowanym wzdłuż nich. Przewidziało to prawie jednocześnie kilka grup teoretycznych w 2010 roku, a pierwsze potwierdzenie uzyskano dwa lata później [7]. Niedawno (innymi metodami) otrzymano wyniki [8–10] na tyle wyraźne, że idea budowy KK z fermionów Majorany wydaje się być w zasięgu ręki (optymistom, którzy przy okazji obiecują międzymordzie w Visual Studio [11]). Wymyślenie, dlaczego nibycząstki pojawiające się w jednowymiarowych materiałach też mogą być anyonami, warte było części zeszłorocznej Nagrody Nobla z Fizyki.

Ich fantastyczną cechą (z punktu widzenia budowy KK) jest to, że żyją na dwóch końcach nanodrutu z nadprzewodnika. Ta ich „topologiczność" powoduje, że są niewrażliwe na zakłócenia, które nieuchronnie prowadziłyby do dekoherencji zbudowanego z nich kubitu. W ten sposób podstawowe ograniczenie związane z rzeźbieniem kubitów znika przy ich pleceniu (według optymistów).

Sytuacja jednak jest taka, że na razie mamy coś, co być może jest włóczką, a już sprzedają nam arras. Głównym sponsorem rozproszonego warsztatu tkackiego jest Microsoft. Środków raczej nie zabraknie, ale czy międzymordzie będzie działać, to ja nie wiem.

Piotr ZALEWSKI

[1] D. Castelvecchi; *Quantum computers ready to leap out of the lab*; *News in Focus, Nature*, **541**, 9, 5 stycznia 2017

[2] S. Boixo *i inni*; *Characterizing Quantum Supremacy in Near-Term Devices*, `arXiv:1608.00263v3 [quant-ph]`; 6 kwietnia 2017

[3] M. Mohseni, P. Read oraz H. Neven; *Commercialize early quantum technologies*; *Comment, Nature* **543**, 171, 9 marca 2017

[4] A. Yu. Kitaev; *Fault tolerant quantum computation by anyons*; `quant-ph/9707021`, *Annals Phys.* **303**(1998)2-30

[5] Ch. Nayak, S. H. Simon, A. Stern M. Freedman oraz S. Das Sarma; *Non-Abelian Anyons and Topological Quantum Computation*; `arXiv:0707.1889v2 [cond-mat.str-el]`, 28 marca 2008

[6] M. Freedman, Ch. Nayak oraz S. Das Sarma; Microsoft Corporation; *Quasi-Particle Interferometry for Logical Gates*; Patent: US 7,394,092 B2; 1 lipca 2008

[7] V. Mourik *i inni*; *Signatures of Majorana Fermions in Hybrid Superconductor-Semiconductor Nanowire Devices*; *Science* **336** 1003, 25 maja 2012

[8] J. Kammhuber *i inni*; *Conductance through a helical state in an indium antimonide nanowire*; *Nature Communications* **8**; 7 września 2017; `doi:10.1038/s41467-017-00315-y`

[9] F. Nichele *i inni*; *Scaling of Majorana Zero-Bias Conductance Peaks*; *Phys. Rev. Lett,* **119**, 136803; 27 września 2017; `doi:10.1103/PhysRevLett.119.136803`

[10] S. Jeon *i inni*; *Distinguishing a Majorana zero mode using spin-resolved measurements*; *Science*, eaan3670; 12 października 2017; `doi:10.1126/science.aan3670`;

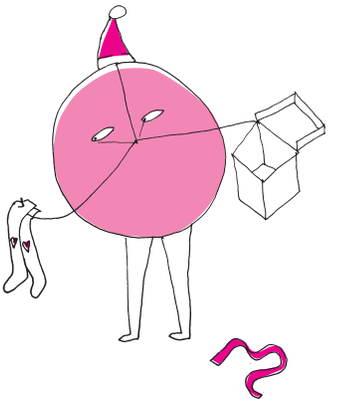
[11] A. Linn; *With new Microsoft breakthroughs, general purpose quantum computing moves closer to reality*; `news.microsoft.com/features/new-microsoft-breakthroughs-general-purpose-quantum-computing-moves-closer-reality`; 25 września 2017

Prosto z nieba: Czy da się żyć na Plutonie?

Wśród nazw proponowanych dla obiektu odkrytego przez Clyde'a Tombaugha w 1930 roku wymieniano imiona różnych greckich i rzymskich bóstw, jednak ostatecznie został on ochrzczony Plutonem, zawierającym inicjały Percivala Lowella (amerykańskiego przedsiębiorcy i astronoma), który wyznaczył jedno z możliwych położeń Plutona na podstawie zaburzeń ruchu Neptuna.

Do czasu misji New Horizons planetę karłowatą Pluton wyobrażaliśmy sobie, poniekąd słusznie, jako glob pogrążony w ciemnościach, zimny i praktycznie martwy. Średnia odległość Plutona do Słońca wynosi prawie 40 jednostek astronomicznych, co oznacza, że światła słonecznego dociera na jednostkę powierzchni 1600 razy mniej niż na Ziemi. W związku z tym średnia temperatura powierzchni planety wynosi jedynie około 50 K. W porównaniu do Ziemi Pluton jest niewielki: promień 0,19 $R_\oplus$ i masa 0,002 $M_\oplus$. Największy z jego pięciu obecnie znanych księżyców, Charon (pozostałe to Hydra i Nix obserwowane po raz pierwszy przez teleskop Hubble'a w 2005 roku, oraz Kerberos i Styx odkryte w 2011 i 2012 roku) o promieniu 600 km, jest tylko o połowę mniejszy od Plutona.

Mimo ciemności i zimna Pluton w obiektywach misji New Horizons zaskakuje w wielu aspektach związanych z obecnością molekuł organicznych. Planeta ma rzadką, przypominającą mgiełkę atmosferę złożoną z metanu (CH_4), azotu (N_2) i węglowodorów (C_2H_x), która rozciąga się aż 200 km ponad powierzchnię (ponad 10 razy dalej, niż oczekiwano). Ciśnienie na powierzchni planety wynosi zaledwie 10 milibarów! Molekuły organiczne wynoszone są na duże wysokości przez naładowane elektrycznie cząstki (elektrony i jony) powstające w jonosferze. Obecność prostych związków organicznych sugeruje istnienie cząsteczek bardziej skomplikowanych, być może nawet takich, które mogą prowadzić do powstania materii ożywionej.



Przykładem „podstawowej cegiełki" jest cyjanowodór (HCN), który uważa się za prekursora aminokwasów i kwasów nukleinowych, a także tholiny, które powstają z prostych molekuł atmosfery Plutona pod wpływem promieniowania ultrafioletowego. Ich nazwa pochodzi od greckiego *tholos* (muł), ponieważ tholiny mają charakterystyczny czerwono-brązowy kolor; zostały tak nazwane przez Carla Sagana w celu scharakteryzowania cech atmosfery Tytana, księżyca Jowisza. Tholiny zostały wykryte na Plutonie w pobliżu lodowych wulkanów (powierzchnia Plutona pokryta jest w wielu miejscach wzgórzami lodu H_2O!). Jest możliwe, że niepozorny Pluton ukrywa pod swoją powierzchnią wodny ocean; podobnie przypuszcza się w przypadku Tytana, Europy i księżyca Saturna, Enceladusa. W odróżnieniu od księżyców dużych planet wnętrze Plutona nie jest rozgrzewane oddziaływaniami pływowymi, ale, najprawdopodobniej, resztkową radioaktywnością. Dostęp do źródeł energii oraz dostatek prostych związków materii organicznej jest silną przesłanką do twierdzenia, że nawet na Plutonie mogą wystąpić warunki sprzyjające powstaniu życia.

Michał BEJGER

Niebo w grudniu

Grudzień odznacza się najdłuższymi nocami w ciągu roku, stąd mogłoby się wydawać, że właśnie w grudniu miłośnicy astronomii mają najwięcej okazji do przyglądania się ciałom niebieskim. Niestety, grudniowe noce bardzo często są zachmurzone lub zamglone i w rezultacie liczba godzin, którą można poświęcić na obserwacje, nie jest taka duża. 21 grudnia Słońce osiągnie najbardziej na południe wysunięty punkt ekliptyki. Ten dzień będzie najkrótszym dniem w roku, na północnych krańcach Polski od wschodu do zachodu Słońca minie 7 godzin i 12 minut, podczas gdy na południowych – godzinę więcej. Może się wydawać, że tego dnia również zdarzy się najpóźniejszy wschód i najwcześniejszy zachód Słońca. Lecz tak nie jest. Najwcześniejszy zmierzch ma miejsce około 12 grudnia, natomiast najpóźniejszy świt – około 1 stycznia, ale coraz późniejszy zachód nie kompensuje coraz późniejszych wschodów, przez co dzień się skraca aż do przesilenia zimowego.

W grudniu promieniują dwa znane roje meteorów. Pierwszym są Geminidy, które można obserwować od 4 do 17 grudnia, z maksimum w okolicach 14 grudnia. Jest to jeden z obfitszych rojów meteorów w ciągu roku.

W maksimum można spodziewać się nawet 120 meteorów na godzinę. Radiant roju znajduje się niecałe 2° na północny zachód od Kastora z Bliźniąt i góruje przed godziną 3 na wysokości ponad 70°. Drugim rojem są Ursydy, mające swój radiant w gwiazdozbiorze Małej Niedźwiedzicy, prawie 2,5 stopnia od gwiazdy Kochab, czyli zachodniego koła Małego Wozu. Ursydy promieniują od 17 do 26 grudnia, z maksimum 22 grudnia, kiedy to można spodziewać się około 10 meteorów na godzinę. Meteory z obu rojów mają podobne prędkości, odpowiednio 35 i 33 km/s. Oba również są widoczne całą noc. Obserwacji obu rojów Księżyc zbytnio nie popsuje, gdyż podczas obu maksimów Srebrny Glob będzie 4 dni przed lub po nowiu, w fazie około 15%. Zatem jeśli tylko pogoda pozwoli, to warto się wybrać na ich obserwacje, oczywiście pamiętając o odpowiednim ubraniu się.

Księżyc mocno rozświetli noce na początku i na końcu miesiąca, gdyż 3 grudnia przejdzie on przez pełnię, 10 grudnia – przez ostatnią kwadrę, 18 grudnia – przez nów, 26 grudnia – przez I kwadrę i ponownie przez pełnię 2 stycznia. Podczas grudniowej pełni Księżyc zakryje Aldebarana, jedną z jaśniejszych gwiazd na niebie, lecz tym razem zjawisko widoczne będzie w północno-zachodniej części Ameryki Północnej i zachodniej części Azji. W Polsce w chwili zachodu 3 grudnia rano Księżycowi zabraknie 1,5 stopnia do gwiazdy γ Tauri, najbardziej na zachód wysuniętej gwiazdy Hiad i jednocześnie ponad 5° do Aldebarana. Wieczorem, około godziny 18 tego samego dnia, Srebrny Glob znajdzie się już ponad 2° na wschód od Aldebarana. Więcej szczęścia będziemy mieli w nocy z 30 na 31 grudnia, gdy Księżyc przejdzie przez Hiady drugi raz w tym miesiącu. Z Polski da się obserwować całe przejście Księżyca przez tę gromadę gwiazd. Jak zawsze naturalny satelita Ziemi zakryje najpierw gwiazdę γ Tauri (około godz. 18:20, odkrycie niecałe 50 minut później). Aldebaran zniknie za księżycową tarczą 8 godzin później. Oczywiście, między γ Tau a Aldebaranem jest kilka słabszych gwiazd, które również zostaną zakryte.

5 dni po zakryciu Aldebarana Księżyc dotrze do gwiazdozbioru Lwa. Tym razem za tarczą Srebrnego Globu, oświetloną w 65%, zniknie Regulus – najjaśniejsza gwiazda tej konstelacji. Zakrycie zacznie się około godziny 22:25, tuż po wschodzie Księżyca i potrwa do mniej więcej 23:15. Będzie to jedyne dobrze widoczne w Polsce zakrycie Regulusa z całej serii, trwającej od listopada 2016 do kwietnia 2018 r. Kolejne zakrycie nastąpi co prawda za miesiąc, 5 stycznia, lecz w Polsce będzie widoczny tylko początek i to już po wschodzie Słońca. Południowa granica kolejnego zakrycia, 1 lutego, przejdzie około 200 km na północ od granic Polski. I to by było na tyle. Przez kilka następnych lat Księżyc będzie mijał Regulusa od północy. Podczas kolejnej serii zakryć Regulusa w latach 2025–26, przy powrocie Srebrnego Globu na południe od ekliptyki, z Polski również da się obserwować tylko jedno zakrycie tej gwiazdy przez Księżyc, 29 marca 2026 roku.

Z planet Układu Słonecznego na niebie wieczornym można obserwować tylko Neptuna w Wodniku i Urana w Rybach. Neptun góruje w godzinach 17–18, kreśląc swoją pętlę po niebie niewiele ponad 0,5 stopnia od gwiazdy λ Aqr, która znakomicie może służyć jako niebowskaz przy szukaniu tej planety. Jasność Neptuna w grudniu osłabnie do $+47{,}9^m$. W Wigilię Bożego Narodzenia z Neptunem spotka się Księżyc w fazie 33%, mijając planetę w odległości 2,5 stopnia. Uran na początku stycznia zmieni kierunek ruchu z wstecznego na prosty, stąd pod koniec miesiąca prawie nie będzie poruszał się względem gwiazd. Planeta zajmie pozycję około 3,5 stopnia na zachód od gwiazdy o Psc i jednocześnie niecałe 3° na północ od gwiazdy μ Psc, górując 2,5 godziny po Neptunie. Jasność Urana w grudniu wyniesie $+5{,}8^m$ i będzie to odpowiednio 1,5 oraz 1^m słabiej od wymienionych przed chwilą gwiazd. Księżyc odwiedzi Urana 27 grudnia, kiedy minie go w odległości ponad 5,5 stopnia, mając fazę 64%.

Na niebie porannym przez cały miesiąc Mars będzie zmniejszał dystans do Jowisza, przy ciągłej poprawie warunków obserwacyjnych obu planet. Mars rozpocznie miesiąc w Pannie, nieco ponad 3° na północny wschód od Spiki i jednocześnie ponad 16° na północny zachód od Jowisza. 31 grudnia również Mars dotrze do gwiazdozbioru Wagi, a jego dystans do Jowisza zmniejszy się do 3°. Towarzystwa planetom dotrzyma gwiazda Zuben Elgenubi, oznaczana na mapach nieba grecką literą α. 23 grudnia Jowisz minie tę gwiazdę $40'$ na północ. Mars uczyni to samo na początku stycznia w prawie tej samej odległości. W trakcie miesiąca Mars pojaśnieje z $+1{,}7$ do $+1{,}5^m$, jednak jego tarcza cały czas będzie miała średnicę $4''$. W tym samym czasie Jowisz zwiększy swoją jasność z $-1{,}7$ do $-1{,}8^m$, a jego tarcza urośnie do $33''$. W dniach 13–15 grudnia obie planety minie zbliżający się do nowiu Księżyc. 13 grudnia Księżyc w fazie 22% przejdzie 6° na północ od Spiki, do Marsa braknie mu ponad 1° więcej. Kolejnej doby jego faza spadnie do 14% i utworzy on trójkąt równoramienny z Marsem i Jowiszem. 15 grudnia Księżyc w fazie 8% znajdzie się prawie 8° na lewo od Jowisza. Natomiast jeszcze kolejnego dnia widoczny będzie bardzo cienki sierp Srebrnego Globu na 2 dni przed nowiem. 3° na południe od niego znajdzie się łuk gwiazd z północno-zachodniej części Skorpiona, z gwiazdami Graffias i Dschubba.

W drugiej połowie grudnia na porannym niebie pokaże się Merkury, który 1 stycznia osiągnie maksymalną elongację zachodnią, ponad 23° od Słońca. Planeta zacznie szybko wznosić się nad widnokrąg w trzeciej dekadzie miesiąca, pokazując się na godzinę przed świtem na wysokości prawie 6° nad punktem SE widnokręgu. Merkury pozostanie widoczny do połowy stycznia. Początkowo znajdzie się on około 8° na północ od Antaresa w Skorpionie, a już w styczniu spotka się z Księżycem i powracającym na nocne niebo Saturnem.

Ariel MAJCHER

Pierwsza jednoczesna detekcja fal grawitacyjnych i fotonów

Grawitacja jest jednym z czterech podstawowych oddziaływań znanych fizykom. Mimo że doświadczamy jej w codziennym życiu, jej natura jest najsłabiej zbadana zwłaszcza w warunkach odbiegających od ziemskich. Obserwacje Kosmosu pozwalają nam na śledzenie procesów zachodzących w ogromnych, nieosiągalnych na Ziemi polach grawitacyjnych, i w ten sposób testować nasze teorie. Jak do tej pory świetnie sprawdza się ogólna teoria względności Einsteina: opis sposobu, w jaki masy zakrzywiają wokół siebie przestrzeń i zmieniają tempo, w jakim płynie czas. Jeśli masy poruszają się w czasoprzestrzeni z przyśpieszeniem, to faluje ona i drga proporcjonalnie do wielkości mas i szybkości ich ruchu. Zmienne w czasie zachowanie się odległości i przepływu czasu w czasoprzestrzeni, wywołane ruchem mas, nazywamy falami grawitacyjnymi.

Detektory fal grawitacyjnych Advanced LIGO (USA) i Advanced Virgo (projekt europejski, do którego należy także polski zespół Polgraw [1]) zostały zbudowane w celu wykrywania fal grawitacyjnych emitowanych przez odległe, kosmiczne katastrofy. Projekty LIGO i Virgo od lat współpracują, dokonując wspólnie detekcji i analizując dane. Do tej pory zarejestrowaliśmy 4 zjawiska, które polegają na zderzeniu się czarnych dziur o masach kilkadziesiąt mas Słońca każda, i ich połączeniu się w jedną, większą, szybko kręcącą się czarną dziurę. Ostatnie nowości w tej dziedzinie to tegoroczna Nagroda Nobla z Fizyki oraz pierwsza w historii detekcja fal przez sieć trzech detektorów; Advanced Virgo zaczął naukowe obserwacje 1 sierpnia 2017 roku. Dzięki temu po raz pierwszy w historii możliwy był pomiar polaryzacji fal grawitacyjnych (fale grawitacyjne, podobnie jak fale elektromagnetyczne, mają dwie niezależne polaryzacje).

Opisywana dziś kolejna obserwacja fal grawitacyjnych pochodzi z nowego typu źródeł: układu podwójnego gwiazd neutronowych. Gwiazdy neutronowe to najbardziej ekstremalne, najgęstsze obiekty znane nauce – jedna łyżeczka materiału gwiazdy neutronowej waży mniej więcej tyle, co cała obecnie znajdująca się na Ziemi populacja ludzka! Powstają podczas eksplozji gwiazd supernowych, podczas których materia jest zgniatana do gęstości wielokrotnie większych od gęstości jąder atomowych. Takiej materii nie da się w żaden sposób wyprodukować i zbadać na Ziemi.

17 sierpnia 2017 roku globalna sieć trzech detektorów Advanced LIGO i Advanced Virgo zarejestrowała trwający ponad 100 sekund bardzo wyraźny sygnał „ćwierku”, oznaczony symbolem GW170817, wyemitowany przez zapadający się układ podwójny. Długość sygnału, jego zakres częstotliwości oraz zmierzona masa ćwierku $\mathcal{M}_c = (m_1 m_2)^{3/5}/(m_1+m_2)^{1/5}$ (gdzie m_1, m_2 to masy składników), równa $1{,}188^{+0{,}004}_{-0{,}002}\ M_\odot$ wskazują na układ gwiazd neutronowych. Tracący energię układ zacieśnia się aż do momentu zderzenia, kiedy to gwiazdy łączą się w jeden gorący, niestabilny obiekt. Około $\Delta t = 1{,}74 \pm 0{,}05$ sekund po momencie zarejestrowania zderzenia obserwatoria satelitarne Fermi oraz INTEGRAL zarejestrowały błysk energetycznego promieniowania: krótki błysk gamma, oznaczony GRB 170817a. Podobne zjawiska są znane astronomom od ponad 50 lat: są najjaśniejszymi elektromagnetycznymi kataklizmami, widocznymi z kosmologicznych odległości. Lokalizacja źródła dostarczona przez satelitę Fermi była, niestety, bardzo przybliżona. Na szczęście dzięki temu, że w obserwacjach fal uczestniczył trzeci detektor – Advanced Virgo – który dodatkowo znajdował się w bardzo dogodnym położeniu względem kierunku na źródło, możliwa była precyzyjna lokalizacja pozycji źródła na podstawie jedynie danych z LIGO i Virgo: pola 28° kwadratowych w gwiazdozbiorze Hydry. Dzięki tej informacji różne rodzaje teleskopów szybko namierzyły nowe źródła światła w galaktyce NGC 4993. Znajduje się ona w odległości w pełni kompatybilnej z wartością 40^{+8}_{-14} Mpc wynikającą z detekcji fal. Prawdopodobieństwo zbiegu okoliczności (czyli odnotowanie niezwiązanych „ćwierku” i błysku gamma) jest mniejsze niż $5 \cdot 10^{-8}$. Szybka lokalizacja pozwoliła na obserwacje fotonów pochodzących z wybuchu oraz jego późniejszej ewolucji w świetle widzialnym, ultrafiolecie, podczerwieni, w zakresie radiowym i X. Pełna lista prac w [2].

Czego nowego nauczymy się z obserwacji GW170817? Po pierwsze, mamy dostęp do zupełnie nowej metody pomiaru odległości we Wszechświecie, niezależnej od tradycyjnych metod polegających na „świecach standardowych”. Układ podwójny będący „syreną standardową” [3] dostarcza odległości d, którą można porównać ze znaną prędkością ucieczki v_H galaktyki NGC 4993, czyli zastosować prawo Hubble'a: $v_H = H_0 d$. Otrzymujemy w ten sposób nowy pomiar stałej Hubble'a, $H_0 = 70{,}0^{+12{,}0}_{-8{,}0}$ km s^{-1} Mpc^{-1} i nowe oszacowanie tempa rozszerzania się Wszechświata. Porównanie przesunięcia czasowego pomiędzy falami grawitacyjnymi i fotonami przydaje się do obliczenia prędkości fal grawitacyjnych v_{GW}: $(v_{GW} - c)/c \approx c\Delta t/d$. Prędkość v_{GW} okazuje się być bardzo bliska c: $v_{GW} = c^{+0{,}000001}_{-0{,}000006}$ m/s. Analiza ostatnich orbit i zderzenia się gwiazd neutronowych pozwala na wykluczenie niektórych teorii opisujących materię gęstą: obserwacje preferują gwiazdy o promieniach mniejszych od 14 km, a pozostałość po zderzeniu ma masę co najmniej $2{,}74^{+0{,}04}_{-0{,}01}\ M_\odot$ – jest albo ciężką gwiazdą neutronową, albo lekką czarną dziurą, co z pewnością da do myślenia astrofizykom od gęstej materii. Obserwacje świecenia pozostałości po zderzeniu wyjaśniają pochodzenie metali cięższych od żelaza. Światło widzialne i podczerwone pochodzi z rozpadu ciężkich radioaktywnych pierwiastków powstałych z materii gwiazd neutronowych rozrzuconych po zderzeniu. Z obserwacji GW170817 wynika, że przeważająca większość m.in. złota i platyny, które znajdujemy obecnie na Ziemi, powstała podczas takich właśnie katastrof.

Michał BEJGER

[1] https://polgraw.camk.edu.pl
[2] http://public.virgo-gw.eu/gw170817_papers
[3] Newtonowskie intuicje dla fal grawitacyjnych, *Delta* 3/17

System dziesiętny używa 10 cyfr (od 0 do 9) w taki sposób:

$$207 = 2 \cdot 10^2 + 0 \cdot 10^1 + 7 \cdot 10^0.$$

Nieujemne liczby mniejsze od 10^n wymagają najwyżej n cyfr.

Podobnie w innych systemach, np. w dwójkowym są 2 cyfry (0 i 1), a liczba 5 wygląda tak:

$$101 = 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0.$$

Nieujemne liczby mniejsze od 2^n wymagają najwyżej n cyfr.

Krąży anegdota o teleturnieju bazującym na grze w 20 pytań, w którym zespół matematyków zastosował opisaną tu strategię. Podobno był to ostatni odcinek tego turnieju... Co więcej, ponieważ wystarczało tam 19 pytań, matematycy ponoć zaczęli od: *Czy wybrane słowo to „żaba”?*

1	10	19
2	11	20
3	12	21
4	13	22
5	14	23
6	15	24
7	16	(25)
8	17	26
9	18	27

(a)

1	2	3
4	5	6
7	8	9
19	20	21
22	23	24
(25)	26	27
10	11	12
13	14	15
16	17	18

(b)

2	5	8
20	23	26
11	14	17
3	6	9
21	24	27
12	15	18
1	4	7
19	22	(25)
10	13	16

(c)

Rys. 1. (a) Stos z wybraną kartą (25) składamy jako środkowy i rozdajemy – 25 trafi do środkowej trójki w swoim nowym stosie.
(b) Stos z kartą 25 składamy jako dolny i rozdajemy – 25 trafi jako środkowa karta ostatniej trójki swojego nowego stosu.
(c) Stos z 25 składamy jako górny – przed 25 jest 0 dziewiątek, 2 trójki i 1 jedynka (czyli 7 kart).

Zadanie 6 pochodzi z XII Olimpiady Matematycznej Juniorów.
Jeszcze jeden przykład zastosowania systemu dwójkowego opisano w *deltoidzie* 10/2017.

Języki obce

Joanna JASZUŃSKA

Czasem warto przetłumaczyć problem na inny język, aby łatwiej go rozwiązać.

1. W grze w 20 pytań gracz A wybiera słowo (ze słownika zawierającego ich najwyżej milion), po czym gracz B zadaje pytanie typu tak/nie. Po usłyszeniu odpowiedzi, B zadaje kolejne pytanie itd. Gracz B wygrywa, jeśli po uzyskaniu 20 odpowiedzi odgadnie słowo wybrane przez A. Wykaż, że B zawsze może wygrać.

2. W grze w 20 pytań wprowadzono nową regułę: gracz B ma zadać wszystkie 20 pytań jednocześnie, zanim usłyszy odpowiedzi. Czy nadal B zawsze może wygrać?

3. Mamy talię 27 kart. Ktoś potajemnie wybiera jedną z nich i mówi, ile kart ma się znaleźć przed nią w talii. Możemy trzykrotnie rozdać karty na trzy stosy po 9, dowiedzieć się, w którym z nich jest wybrana karta i złożyć te trzy stosy znów w jeden. Jak wykryć wybraną kartę i ustawić ją na żądanej pozycji?

4. Oblicz $2^n + 2^{n-1} + \ldots + 2^2 + 2^1 + 2^0$ oraz $7^n + 7^{n-1} + \ldots + 7^2 + 7^1 + 7^0$.

Rozwiązania

R1. Gracz B najpierw pyta, czy wybrane słowo jest w pierwszej połowie słownika. Potem pyta, czy jest ono w pierwszej połowie odpowiednio pierwszej lub drugiej połowy itd.; w każdym kolejnym pytaniu dwukrotnie zawęża obszar poszukiwań. Ponieważ $1\,000\,000 < 2^{20}$, więc 20 pytań wystarczy, by zostało tylko jedno słowo. □

R2. Nic się nie zmienia, gracz B gra jak dotychczas: numeruje słowa w systemie dwójkowym (wystarcza do tego 20 cyfr) i w n-tym pytaniu pyta, czy na n-tym miejscu w numerze wybranego słowa jest cyfra 0. □

R3. Przypuśćmy, że przed wybraną kartą ma być 7 innych; w systemie trójkowym 7 to 021 (i dowolną liczbę od 0 do 26 też można zapisać jako 3-cyfrową). Trzykrotnie rozdajemy karty na 3 stosy i kolejno składamy je tak, by za pierwszym razem wskazany stos był w środku, za drugim na dole, a za trzecim – na górze (cyfry 021 czytamy od końca: 1 oznacza środek, 2 – dół, 0 – górę; rys. 1).

Dlaczego ta metoda działa? Przy ostatnim składaniu stosów kart, wybrana karta trafia do odpowiedniej z trzech dziewiątek (u nas do górnej), gdyż pierwsza cyfra zapisu trójkowego koduje, ile dziewiątek kart ma być przed wybraną (u nas zero).

We wcześniejszym ruchu, w ramach tejże dziewiątki wybrana karta trafiła do odpowiedniej z trzech trójek, gdyż środkowa cyfra zapisu trójkowego właśnie to koduje. Podobnie w pierwszym ruchu karta została ustawiona na odpowiednim z trzech miejsc w ramach swojej trójki, zgodnie z trzecią cyfrą zapisu. □

R4. Łatwo obliczyć $10^n + \ldots + 10^2 + 10^1 + 10^0 = 100\ldots0 + \ldots + 100 + 10 + 1 = 11\ldots1$. Podobnie szukane sumy równe są $11\ldots1$ w odpowiednich systemach pozycyjnych. W dwójkowym liczba $11\ldots1$ jest jak $99\ldots9$ w dziesiętnym, więc pierwsza z sum to $2^{n+1} - 1$. Analogicznie dla drugiej sumy: w systemie siódemkowym $11\ldots1 = \frac{1}{6} \cdot 66\ldots6$ równe jest $\frac{1}{6}(7^{n+1} - 1)$ w dziesiętnym. □

Zadania domowe

5. Jak w 10 ponumerowanych kopertach rozmieścić w sumie równo 1000 zł, aby móc zapłacić dowolną całkowitą kwotę od 0 do 1000 zł bez otwierania kopert?

6. W każde pole tablicy 4×4 należy wpisać pewną liczbę całkowitą w taki sposób, aby sumy liczb w każdej kolumnie i w każdym wierszu były potęgami liczby 2 o wykładniku całkowitym nieujemnym. Czy można to zrobić w taki sposób, aby każde dwie z tych ośmiu sum były różne?

Wskazówka. Warto rozważyć zapis dwójkowy sumy wszystkich liczb w tablicy.

7. Wykaż, że $(1+q)(1+q^2)(1+q^{2^2}) \cdot \ldots \cdot (1+q^{2^n}) = 1 + q + q^2 + q^3 + \ldots + q^{2^{n+1}-1}$.

8. Ciąg liczb całkowitych $(a_n)_{n \geqslant 0}$ definiujemy rekurencyjnie: $a_0 = 0$, $a_{2n} = 3a_n$, $a_{2n+1} = 3a_n + 1$. Scharakteryzuj wszystkie liczby całkowite $s \geqslant 0$, dla których istnieje dokładnie jedna para (k, l) spełniająca warunki $k > l$ oraz $a_k + a_l = s$.

Wskazówka. Dla wyznaczenia a_n należy zapisać liczbę n w systemie dwójkowym i odczytać w trójkowym.