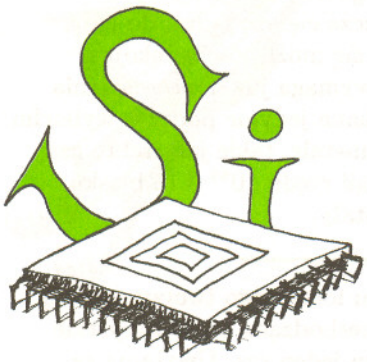
Komputery kwantowe, czyli wyrachowana interferencja

Konrad BANASZEK



Zapewne każdy użytkownik komputera chciałby, żeby jego urządzenie działało *jeszcze* szybciej i miało *jeszcze* większą pamięć. Powody po temu są rozmaite. Jedni pragnęliby dokładniej poznać tajemnice Wszechświata. Innym zależy z kolei na bardziej prozaicznych zastosowaniach, jak np. przewidywanie pogody. Są wreszcie i tacy, którym marzą się jeszcze mocniejsze wrażenia podczas zmagań z wyimaginowanymi przeciwnościami losu na ekranie komputera.

Droga do zwiększenia wydajności komputerów prowadzi obecnie jedna. Jest nią miniaturyzacja, wkraczająca powszechnie wkraczająca powszechnie w nasze codzienne życie. Miniaturyzacja nie może jednak postępować w nieskończoność, przynajmniej na pewno nie zgodnie z dotychczasowymi zasadami działania układów elektronicznych. Trudno jest bowiem wyobrazić sobie ścieżkę w układzie scalonym, której szerokość byłaby porównywalna z rozmiarami atomu, a prąd nią płynący składał się z pojedynczego elektronu. Procesy w takiej skali opisywane są przez mechanikę kwantową. W zjawiskach przez nią opisywanych pojawia się wiele nieoczekiwanych efektów: cząstki zachowywują się czasem jak fale, a fale – jak cząstki.

Można jednak popuścić wodze fantazji i zastanowić się nad działaniem komputera złożonego z pojedynczych układów kwantowych. Przede wszystkim musimy znaleźć sposób na kodowanie bitów, czyli podstawowych zero-jedynkowych cegiełek informacji, którymi posługuje się komputer. Dobrym kandydatem do przechowywania jednego bitu informacji jest pojedynczy atom, gdy z jego struktury energetycznej wybierzemy dwa poziomy i przypiszemy im wartości logiczne 0 i 1. Wprowadzając odpowiednie oddziaływanie między dwoma lub więcej atomami, można otrzymać różne wyniki, w zależności od stanu początkowego układu, czyli – w języku informatyki – wykonywać operacje logiczne na stanach wejściowych. Składając razem wiele takich elementarnych operacji, dałoby się zbudować komputer, który w pełni zasługiwałby na przydomek: kwantowy.

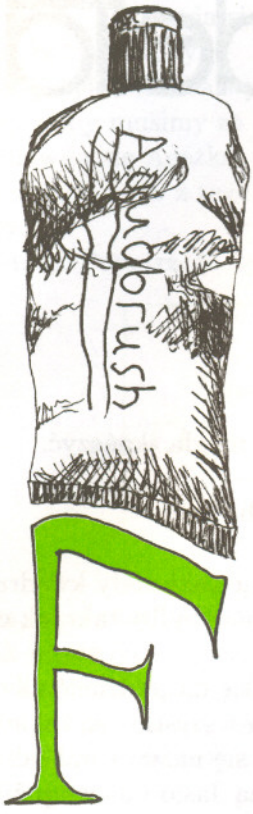
Komputer kwantowy ma istotnie nowe cechy w porównaniu z jego klasycznym odpowiednikiem. W mechanice kwantowej bowiem cząstki wykazują własności falowe. Dzięki temu możemy dodawać różne stany kwantowe – czyli tworzyć ich *superpozycje* – na podobnej zasadzie, jak dodają się drgania w ruchu falowym. Każdy z atomów na wejściu układu logicznego nie musi być więc w ściśle określonym stanie 0 lub 1. Możemy je przygotować w stanie superpozycji będącej kombinacją różnych stanów kwantowych. Nasz układ logiczny przetworzy wtedy *równolegle* każdy ze składników i dostarczy na wyjściu superpozycję wyników odpowiadających poszczególnym stanom wejściowym.

Brzmi to bardzo obiecująco, ale pozostaje jeden podstawowy kłopot – odczytanie wyniku obliczeń. Na końcu musimy dokonać pomiaru i sprawdzić, które z atomów znajdują się w stanie 0, a które w stanie 1. Pomiar taki dostarczyłby jednak informacji tylko o jednym ze składników superpozycji. Pomocną analogią jest tutaj doświadczenie z dyfrakcją elektronów, w którym obserwujemy na ekranie rozkład wiązki elektronów po przejściu przez szczelinę. Pojedynczy elektron może zostać zarejestrowany w różnych punktach ekranu z pewnym prawdopodobieństwem. Zaobserwowanie położenia jednego elektronu mówi nam jednak niewiele o pełnym obrazie dyfrakcyjnym. Dopiero wielokrotne powtórzenie doświadczenia przynosi pełny rozkład prawdopodobieństwa na ekranie. Podobnie, aby otrzymać informację o wszystkich składnikach superpozycji przetworzonych przez komputer kwantowy, musielibyśmy wielokrotnie powtórzyć wszystkie operacje logiczne i końcowy pomiar.

Jest na to jednak rada. Otóż trzeba w pełni wykorzystać dobrodziejstwa mechaniki kwantowej i skłonić poszczególne składniki superpozycji do *interferencji*. Tak jak składając razem drgania falowe, możemy je wzmacniać

Rozwiązanie zadania M 928.
Punkt a) jest szczególnym przypadkiem punktu b) dla $l = m = 2$. Do dowodu b) rozważmy nieskończony poziomy pas szerokości ln, którego brzegiem są dwie proste siatki. Składa się on z nieskończonej liczby słupków szerokości 1 i wysokości ln. Wśród nich znajdziemy m jednakowo pokolorowanych (zasada szufladkowa Dirichleta). Każdy z tych słupków pokolorowany jest n kolorami, wysokość słupków wynosi ln, a więc znajdziemy kolor, którym pokolorowanych jest co najmniej l kratek jednego z wybranych słupków (zasada szufladkowa). Szukane proste to m prostych pionowych przechodzących przez środki wybranych słupków i l prostych poziomych przechodzących przez środki znalezionych l kratek.

Pytanie dodatkowe: A czy kwadrat zawsze istnieje? (Możemy ograniczyć się do dwóch kolorów.)



albo wygaszać (mówimy wtedy o interferencji *konstruktywnej* bądź *destruktywnej*), podobnie interferencja kwantowa pozwala nam manipulować „udziałem" stanów składowych w superpozycji. Przypuśćmy, że naszym zadaniem jest znalezienie rozwiązań spełniających pewien określony warunek. Okazuje się często, że najlepszy algorytm dla zwykłych (klasycznych) komputerów sprowadza się do pracowitego sprawdzenia, które z potencjalnych rozwiązań spełnia wymagane warunki. Komputer kwantowy może przetworzyć równolegle superpozycję potencjalnych rozwiązań, i to w taki sposób, aby te spełniające żądany warunek ulegały interferencji konstruktywnej, czyli wzmocnieniu, natomiast pozostałe interferowały destruktywnie i zostały wygaszone. Pomiar stanu wyjściowego przyniesie nam wtedy tę odpowiedź, której właśnie szukamy.

Przykładem problemu obliczeniowego powyższego typu jest rozkład liczby naturalnej na czynniki pierwsze. Złożoność tego problemu rośnie niesłychanie szybko wraz z liczbą cyfr. Jest to praktycznie wykorzystywane w powszechnie używanych protokołach szyfrujących z tak zwanym kluczem publicznym. Mając dwie liczby pierwsze, nietrudno jest znaleźć ich iloczyn. Co więcej, można go ogłosić wszem i wobec bez szczególnej obawy, że ktoś znajdzie jego rozkład na czynniki pierwsze. Procedura kodująca używa tylko tego iloczynu, natomiast do odkodowania zaszyfrowanej informacji potrzebna jest już znajomość obu czynników. Dzięki temu rozszyfrować wiadomość może tylko autor klucza.

Komputer kwantowy (gdyby ktoś go zbudował, oczywiście) byłby w stanie znaleźć rozkład na czynniki pierwsze, używając znacznie mniejszej liczby operacji. Stanowiłoby to poważne zagrożenie dla bezpieczeństwa protokołów szyfrujących z kluczem publicznym. Mechanika kwantowa oferuje jednak coś w zamian – kwantowe systemy kryptograficzne, których bezpieczeństwo gwarantuje całym swoim autorytetem. Ale to już następna historia...

Tajemnica liczb Fermata

Wielu badaczom świata liczb marzyło się uzyskanie cudownego wzoru, który dawałby wyłącznie liczby pierwsze. Próbowano wykorzystywać różne formuły, z których dwie pozostały przedmiotem rozważań do dziś. Chodzi mianowicie o liczby postaci $2^m - 1$ i $2^m + 1$ ($m \in \mathbb{N}$). Można wykazać, że jeśli $2^m - 1$ jest liczbą pierwszą, to m jest również liczbą pierwszą. Liczby $M_p = 2^p - 1$ (p – liczba pierwsza) nazywamy liczbami Mersenne'a. Liczby M_2, M_3, M_5, M_7 są pierwsze, ale już liczba M_{11} jest złożona. Prawdopodobnie wśród liczb Mersenne'a jest nieskończenie wiele zarówno liczb pierwszych, jak i złożonych. Największą znaną liczbą pierwszą Mersenne'a była w 1999 r. liczba $M_{6972593}$. Jeśli natomiast liczba $2^m + 1$ jest pierwsza, to $m = 2^n$ ($n \in \mathbb{N} \cup \{0\}$). Fermat przypuszczał, że zachodzi twierdzenie odwrotne. Oznaczmy $F_n = 2^{2^n} + 1$. Wprawdzie liczby F_0, F_1, F_2, F_3, F_4 są pierwsze, ale już liczba F_5 jest złożona. Do chwili obecnej wykazano, że liczby $F_5, F_6, \ldots, F_{23}$ są złożone (i niektóre inne).

Liczby Fermata mają nieoczekiwany związek z geometrią. Otóż Gauss udowodnił, że jeśli $s = 2^k F_{n_1} F_{n_2} \ldots F_{n_t}$, $k \geq 0$, gdzie $F_{n_1}, F_{n_2}, \ldots, F_{n_t}$ są różnymi liczbami pierwszymi Fermata, to można skonstruować s-kąt foremny za pomocą cyrkla i linijki. Nieco później Wantzel wykazał twierdzenie odwrotne. Od czasów Fermata (1640 r.) nie znaleziono nowej liczby pierwszej F_n. Obecnie pierwszą podejrzaną jest F_{24} (mająca 5 050 446 cyfr). Gdyby okazała się pierwsza (co raczej jest wątpliwe), to na podstawie twierdzenia Gaussa można by skonstruować za pomocą cyrkla i linijki F_{24}-kąt foremny. Jest to wielokąt o ogromnej liczbie boków (na rysunku wyglądałby praktycznie jak koło). Podanie konstrukcji takiego wielokąta to zadanie karkołomne. Byłoby może zatem lepiej, gdyby okazało się, że poza F_0, F_1, F_2, F_3, F_4 nie ma innych liczb pierwszych Fermata. Czy jednak da się to udowodnić?

Witold BEDNAREK

Rozwiązanie zadania F 531.
Oznaczmy szukany stosunek oporu r_2 dużego boku ramki do oporu r_1 mniejszego przez $x = r_2/r_1$. Po włączeniu ramki do obwodu w punktach A i B mamy

$$\frac{1}{R_1} = \frac{1}{r_1} + \frac{1}{r_1 + 2xr_1} = \frac{2(x+1)}{r_1(2x+1)}.$$

Po włączeniu ramki w punktach B i C otrzymujemy

$$\frac{1}{R_2} = \frac{1}{xr_1} + \frac{1}{2r_1 + xr_1} = \frac{2(x+1)}{xr_1(x+2)}.$$

Stosunek oporów jest równy

$$\frac{R_2}{R_1} = \frac{x(x+2)}{2x+1} = 1{,}6,$$

a stąd równanie na x

$$x^2 - 1{,}2x - 1{,}6 = 0.$$

Odrzucając ujemny pierwiastek równania otrzymujemy $x = 2$.