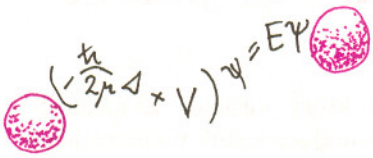


Powyższe rozważania prowadzą do wniosku, że jakikolwiek wybralibyśmy rozkład na prawdopodobieństwa wystąpienia każdego z ośmiu zestawów parametrów ukrytych, to nigdy P nie przekroczy wartości $\frac{2}{3}$, tzn. $P \leq \frac{2}{3}$. Tymczasem z praw mechaniki kwantowej (potwierdzonych doświadczalnie) wynika, że $P = \sin^2(\phi/2)$, gdzie ϕ jest kątem między kierunkami pomiarów spinów. W naszym przypadku $P = \sin^2(120^\circ/2) = \frac{3}{4}$. Otrzymany wynik jest więc sprzeczny z nierównością $P \leq \frac{2}{3}$, co dowodzi, że elektron nie może mieć parametrów ukrytych, określających wynik pomiaru jego spinu.

Komputery kwantowe i obliczenia kwantowe

Arkadiusz ORŁOWSKI

Recenzowanie nieistniejących książek może być zajęciem bardzo pouczającym i twórczym. Dobrym przykładem są utwory Stanisława Lema: „Doskonała próżnia", „Wielkość urojona" i „Biblioteka XX wieku". Wnikliwa recenzja lub posłowie do książki, której (jeszcze) nikt nie napisał, pozwala lepiej zrozumieć, dlaczego książka taka powinna (lub nie powinna) powstać. W niniejszym artykule idziemy w ślady Lema, omawiając urządzenia, które nie istnieją – komputery kwantowe. Chodzi o komputery, których działanie w istotny sposób wykorzystuje niezwykłe własności obiektów kwantowych. Nie mamy wątpliwości, że komputery kwantowe powinny zostać zbudowane. Wiemy, że mogą istnieć (nie przeczy to żadnym znanym prawom przyrody) i że jeżeli powstaną – mogą się bardzo przydać. Wiemy również, jak powinny działać i w jakich zagadnieniach biją na głowę wszelkie istniejące lub dające się pomyśleć komputery klasyczne (nie kwantowe).

W pewnym (trywialnym) sensie każdy komputer jest komputerem kwantowym, ponieważ jest obiektem materialnym, a materia podlega prawom mechaniki kwantowej. Chodzi jednak o to, że komputery współczesne nie wykorzystują (jak dotąd) tych własności obiektów fizycznych, które przeczą naszej klasycznej intuicji. Do zrozumienia, jak działa komputer klasyczny, nie musimy znać mechaniki kwantowej. Wiedza ta nie jest również niezbędna projektantom komputerów i programistom (choć projektanci układów scalonych i chipów muszą się liczyć z prawami fizyki, także kwantowej). Zachowanie się współczesnych komputerów, podobnie jak funkcjonowanie samochodów, można zrozumieć w ramach fizyki klasycznej. Komputer, zwany też elektroniczną maszyną cyfrową i (do lat siedemdziesiątych) mózgiem elektronowym, jest urządzeniem realizującym pewną koncepcję matematyczną. Ale działający komputer jest, oczywiście, obiektem fizycznym. Podobnie jak samochód. Jednak w odróżnieniu od samochodu, który jest urządzeniem przetwarzającym energię, komputer zajmuje się przetwarzaniem informacji. Komputer też pobiera energię i wydziela ciepło, ale jego istotną funkcją jest obróbka informacji. Teoria informacji jest obecnie dobrze ugruntowaną dyscypliną matematyczną. Informację można traktować także jako obiekt fizyczny, bowiem w świecie rzeczywistym musi być zawsze zakodowana w stanach obiektów fizycznych i jest przenoszona przez obiekty fizyczne poprzez fizyczne kanały transmisji (zwykle nieidealne – z szumem). Ponieważ nasz Wszechświat podlega prawom mechaniki kwantowej (nie tylko w skali mikroświata – współczesna kosmologia też jest kosmologią kwantową), również informacja musi mieć swoją „kwantową twarz". Komputer kwantowy możemy więc zdefiniować jako urządzenie przetwarzające informację kwantową.

Jednostką klasycznej informacji jest bit, który może przyjmować jedną z dwu wartości: 0 lub 1. Bit można zrealizować fizycznie za pomocą dowolnego układu, który może znajdować się w dowolnym z dwu wyraźnie rozróżnialnych stanów (kondensator jest naładowany lub nie, prąd płynie lub nie płynie, namagnesowanie domeny jest skierowane w dół lub w górę względem przyłożonego pola magnetycznego). W mechanice kwantowej istnieje wiele układów fizycznych o dwóch stanach bazowych, takich jak spin elektronu lub protonu, polaryzacja fotonu itp. W odróżnieniu od układów klasycznych w tym przypadku układ może być również w dowolnej superpozycji stanów bazowych. Bit kwantowy (qubit) może więc być jednocześnie w dwóch stanach bazowych. Przypomina to trochę logikę wielowartościową z nieprzeliczalną liczbą możliwości (wartości logicznych).

Qubit jest pewną superpozycją $\alpha|0\rangle + \beta|1\rangle$ stanów $|0\rangle$ i $|1\rangle$ – opisujących jakiś obiekt fizyczny. Są to ustalone wektory ortogonalne o jednostkowej długości, na przykład $(1,0)$ i $(0,1)$. Ewolucja tych stanów w czasie jest zakodowana w pewnej macierzy, nazywanej macierzą ewolucji, działającej na wektory stanu. Na pierwszy rzut oka qubit zawiera więc więcej informacji niż bit. Nieskończenie wiele informacji można przecież zakodować w rozwinięciu dwójkowym współczynników α i β stojących przy wektorach bazowych. Współczynniki te, zwane amplitudami prawdopodobieństwa, są liczbami zespolonymi – po uwzględnieniu normalizacji $|\alpha|^2 + |\beta|^2 = 1$ pozostają trzy wolne parametry rzeczywiste. Ale w rzeczywistości pojedynczy, izolowany qubit niesie dokładnie tyle samo informacji co pojedynczy bit. Chcąc odczytać wartość qubitu, musimy bowiem dokonać pomiaru, co powoduje, że qubit może się znaleźć tylko w jednym ze stanów własnych operatora opisującego układ pomiarowy. Co więcej, teoria kwantowa twierdzi, że wynik takiego pomiaru jest zupełnie przypadkowy. Dla powyższej superpozycji prawdopodobieństwa znalezienia qubitu w stanach $|0\rangle$ i $|1\rangle$ wynoszą $|\alpha|^2$ i $|\beta|^2$, odpowiednio. W mechanikę kwantową wbudowany jest doskonały generator liczb losowych.

Komputer klasyczny jaki jest – każdy widział. Na jednym z nich napisałem ten tekst. Namiętnie grający w multimedialne gry komputerowe lub zajmujący

W klasie komputerów osobistych standardem jest już procesor Pentium III z zegarem co najmniej 800 MHz – na powierzchni niewiele większej niż 100 mm^2 mieści się ponad 28 milionów tranzystorów. Odpowiednio skonfigurowane klastry takich PC-tów potrafią wykonywać kilkaset miliardów operacji na sekundę! A jeszcze nie tak dawno z podziwem i niedowierzaniem patrzono na komputer ENIAC, zbudowany z około 20 tysięcy lamp elektronowych. Mógł on wykonywać „aż" 5 tysięcy operacji na sekundę przy wadze rzędu 30 ton i rozmiarach sporego pomieszczenia. Dokonał się więc ogromny postęp w technice komputerowej. Postęp ten wciąż trwa – tak zwane prawo Moore'a stwierdza, że gęstość upakowania tranzystorów w układach scalonych podwaja się co 18 miesięcy.

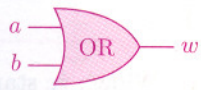
Ewolucja wektora stanu jest odwracalna. Obliczenia kwantowe można zawsze wykonać „wspak", otrzymując stan wejściowy. Klasyczne mikroprocesory projektowane są w oparciu o logikę nieodwracalną. Okazuje się jednak, że można zaprojektować komputer klasyczny, który wykonuje obliczenia w sposób odwracalny. Może to mieć pewne konsekwencje praktyczne – wymazanie jednego bitu informacji powoduje wydzielanie się ciepła. W obliczeniach odwracalnych wydzielane ciepło byłoby więc mniejsze. Jeżeli do obliczeń używamy układów opartych na ruchu elektronów, to nie da się, oczywiście, całkowicie wyeliminować nagrzewania się procesora. Wydaje się, że wkraczamy w erę opłacalności klasycznych obliczeń odwracalnych. Prawdopodobnie dalsza miniaturyzacja mikroprocesorów wymusi wkrótce stosowanie odwracalnej architektury. Jest pocieszające, że chociaż odwracalność powoduje konieczność użycia większej liczby elementów (bramek) logicznych, to liczba ta nie rośnie w zastraszającym tempie – procesor odwracalny jest tylko trochę „większy" niż zwykły.

się wirtualną rzeczywistością mogą protestować, ale tak naprawdę komputer wykonuje jedynie proste dodawanie zer i jedynek. Robi to jednak bardzo szybko. Współczesne komputery (klasyczne) mają bez wątpienia niezwykłe możliwości. Lecz skoro jest tak dobrze, to czemu jest tak źle? Mimo iż komputery klasyczne są bardzo szybkie, są za wolne. Choćbyśmy byli w stanie zaprząc do pracy obliczeniowej cały Wszechświat (swoją drogą to ciekawe pytanie, jaką część Wszechświata da się wykorzystać do prowadzenia obliczeń?), to i tak pewne problemy na zawsze pozostałyby poza zasięgiem naszych klasycznych możliwości.

Jeśli więc uda nam się zbudować komputery kwantowe, to czy będą one mogły zrobić coś, czego zupełnie nie potrafią komputery klasyczne? Tak nie jest. Chociaż te drugie działają na zupełnie innych zasadach, to przecież komputer klasyczny może symulować działanie komputera kwantowego. Stan N qubitów w komputerze kwantowym opisany jest przez wektor w 2^N-wymiarowej przestrzeni Hilberta (na potrzeby tego artykułu możemy ją sobie wyobrażać jako przestrzeń wektorów N-wymiarowych z określonym dodawaniem, mnożeniem przez liczby zespolone i iloczynem skalarnym). Z fizycznego punktu widzenia obliczenia kwantowe to odpowiednio zaprojektowana ewolucja określonego stanu początkowego. Ewolucja wektora stanu polega na jego obracaniu w określony sposób (nie zmieniając jego długości), pomiar zaś na zrzutowaniu tego wektora na pewien układ wzajemnie prostopadłych osi. Wektory, ich obroty i rzuty nie są rzeczą obcą dla klasycznych komputerów. W czym więc problem? W czasie potrzebnym na wykonanie takiej symulacji. Aby w pełni opisać stan kwantowy 100 qubitów, musimy przechować około 10^{30} liczb zespolonych! A to już naprawdę sporo... Klasyczne komputery nie są dobrym narzędziem do symulacji układów kwantowych. Natomiast komputer kwantowy wykonuje wszystkie operacje na wszystkich qubitach naraz, co pozwala na rozwiązywanie w czasie wielomianowym problemów, które wymagają czasu wykładniczego na komputerach klasycznych.

Okazuje się, że istnieją ciekawe i ważne problemy, których nie umiemy rozwiązywać w czasie wielomianowym, a dla których istnieją algorytmy kwantowe upraszczające problem. Jednym z takich problemów jest rozkład dużych liczb na czynniki pierwsze. Dla wszystkich znanych algorytmów klasycznych czas potrzebny na wykonanie tej operacji rośnie wykładniczo z liczbą cyfr rozkładanej liczby. Na fakcie tym (jest to fakt empiryczny, nie istnieje żaden dowód matematyczny, że problemu tego nie da się rozwiązać w czasie wielomianowym, jest to jednak mało prawdopodobne) opiera się bezpieczeństwo naszych (i cudzych) transakcji elektronicznych i poufność korespondencji. W 1994 roku Peter Shor opublikował pracę, w której podał algorytm kwantowy faktoryzacji w czasie wielomianowym. Algorytm wymaga jednak istnienia komputera kwantowego. Nie będzie przesadą stwierdzenie, że od momentu publikacji tej pracy rozpoczął się prawdziwy boom w tej dziedzinie. Znów potwierdziła się stara prawda, że o ile podstawowe problemy fizyki interesują nielicznych, o tyle łatwo o pieniądze, gdy chodzi o pieniądze...

a	b	w
0	0	0
0	1	0
1	0	0
1	1	1



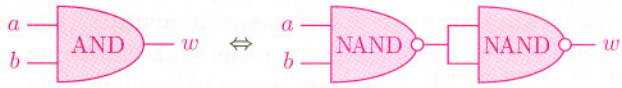
a	b	w
0	0	0
0	1	1
1	0	1
1	1	1

a	w
0	1
1	0

a	b	w
0	0	1
0	1	1
1	0	1
1	1	0

Aby zbudować komputer kwantowy, niezbędne są różne elementy. Pierwszy to qubity – nośniki informacji kwantowej. Drugi to odpowiedni zestaw kwantowych bramek logicznych. Pożądany jest, oczywiście, niewielki zbiór bramek uniwersalnych – a więc takich, z których można zbudować wszystkie operacje. W obliczeniach klasycznych takie zestawy to, na przykład, AND i NOT oraz OR i NOT. Obok są pokazane ich schematyczne oznaczenia i tak zwane „tabelki prawdy". Każdą operację logiczną da się przedstawić za pomocą bramek AND (koniunkcja) i NOT (zaprzeczenie). Z praw de Morgana wynika, że również bramki OR (alternatywa) i NOT wystarczą do zbudowania dowolnie skomplikowanej sieci logicznej. Pary te tworzą więc uniwersalny zestaw bramek. Czy istnieje pojedyncza uniwersalna bramka logiczna? Tak. Popatrzmy na tabelkę prawdy operacji NAND. Uniwersalność tej bramki najłatwiej udowodnić, pokazując, że można

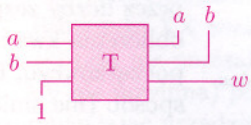
z niej zbudować AND, OR i NOT, na przykład:

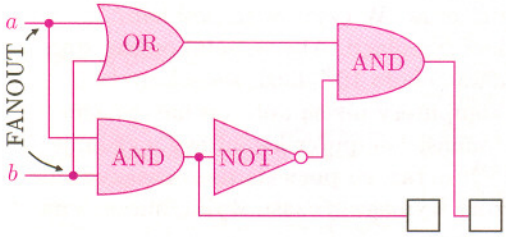


a	b	c	→	a	b	w
0	0	0		0	0	0
0	0	1		0	0	1
0	1	0		0	1	0
1	0	0		1	0	0
0	1	1		0	1	1
1	0	1		1	0	1
1	1	0		1	1	1
1	1	1		1	1	0

Bramka Toffoliego

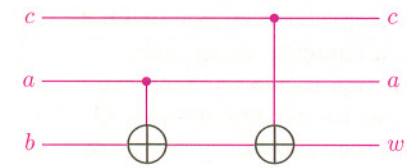
Nie możemy jednak wykorzystać klasycznych sieci logicznych przez prostą zamianę klasycznych bramek przez ich kwantowe odpowiedniki. Jeden z powodów to fakt, że bramki AND i OR są nieodwracalne. W mechanice kwantowej dopuszczalne są operacje unitarne, a więc odwracalne w czasie. Istnieją bramki klasyczne, które są jednocześnie odwracalne i uniwersalne. Ale muszą mieć one co najmniej 3 wejścia i 3 wyjścia (jest prawie oczywiste, że bramki odwracalne muszą mieć tę samą liczbę wejść i wyjść). Na marginesie mamy pokazany przykład takiej bramki, zwanej bramką Toffoliego. Jest to bramka uniwersalna, bowiem możemy z niej zrobić NAND, a więc zbudować z niej wszystkie możliwe operacje logiczne:





Półsumator klasyczny

Drugim powodem jest powszechne występowanie w klasycznych sieciach logicznych operacji FANOUT, czyli tworzenia kopii pewnych wartości logicznych, kierowanych następnie na wejścia innych bramek, na przykład w klasycznym półsumatorze (rysunek obok) albo w przykładzie u góry strony. Okazuje się, że operacji FANOUT nie da się wykonać w komputerze kwantowym. Podstawowe prawa mechaniki kwantowej zabraniają bowiem klonowania nieznanych stanów kwantowych. Należy to dobrze rozumieć – można skonstruować kwantowe ksero, które potrafi kopiować pewne wybrane stany kwantowe. Natomiast nie istnieje uniwersalny kserograf, który potrafiłby dokładnie skopiować dowolny (nieznany) stan kwantowy. Jeśli stan jest znany, to można wyprodukować dowolną liczbę kopii. Słowo *dokładnie* też jest ważne, gdyż możliwe jest kopiowanie przybliżone. Dowód twierdzenia o niemożliwości klonowania jest bardzo prosty i wynika z liniowości mechaniki kwantowej (z faktu, że superpozycja dwóch stanów kwantowych też jest stanem kwantowym). Odwracalną wersję półsumatora, którą można zbudować bez FANOUT! z kwantowych bramek logicznych, przedstawiono na marginesie.

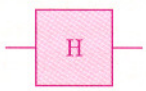


Półsumator kwantowy; znaczenie symbolu ⊕ jest opisane niżej.

Klasyczne bramki logiczne opisujemy tabelkami prawdy, a kwantowe – macierzami. Ważnym przykładem kwantowej bramki 1-bitowej jest bramka Hadamarda. Jej działanie, opisane prostą macierzą o wymiarach 2×2,

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

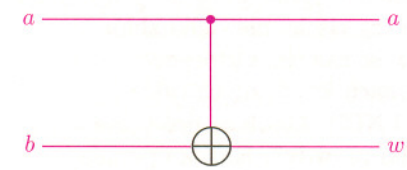
generuje superpozycje stanów bazowych $|0\rangle$ i $|1\rangle$. Widać, że stan $|0\rangle$ przechodzi w $(|0\rangle + |1\rangle)/\sqrt{2}$, a stan $|1\rangle$ w $(|0\rangle - |1\rangle)/\sqrt{2}$.



Bramka Hadamarda

Najważniejszą kwantową bramką logiczną jest tak zwane kontrolowane zaprzeczenie (controlled NOT; C-NOT) opisane macierzą:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



C-NOT

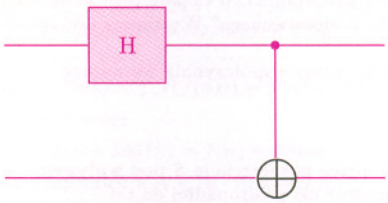
Jest to bramka 2-bitowa, odwracalna i „prawie" uniwersalna, w tym sensie, że z niej i skończonego repertuaru bramek 1-bitowych można zbudować sieci realizujące dowolne obliczenia kwantowe.

Aby komputer kwantowy mógł poprawnie działać, konieczne jest spełnienie także innych warunków. Musi być precyzyjnie określony wymiar przestrzeni Hilberta układu kwantowego. Musimy więc znać *dokładnie* liczbę atomów,

elektronów, kropek kwantowych czy innych obiektów, których stany będą qubitami. Są to bowiem nasze stopnie swobody, które wykorzystujemy do przechowywania danych i wykonywania obliczeń. Ważne jest, że rozmiar przestrzeni Hilberta rośnie wykładniczo wraz ze wzrostem liczby cząstek (rozmiarem układu). Tu bowiem kryje się niezwykła moc komputerów kwantowych. Ważna jest też możliwość przygotowania właściwego stanu początkowego do obliczeń (RESET komputera kwantowego), na przykład przez osiągnięcie stanu podstawowego. Może to wymagać zaawansowanych metod chłodzenia, jak w przypadku komputerów zbudowanych w oparciu o jony w pułapkach magnetycznych. Kolejnym warunkiem jest również możliwość wykonywania pomiarów kwantowych. Układ fizyczny, który ma odgrywać rolę komputera kwantowego, musi być także dobrze odizolowany od otoczenia. Oddziaływanie powoduje splątanie, czyli nietrywialne korelacje kwantowe między oddziałującymi obiektami. Z jednej strony splątanie między qubitami jest niezbędnym elementem obliczeń kwantowych. Z drugiej strony splątanie qubitów z otoczeniem nieuchronnie prowadzi do tzw. dekoherencji. Dekoherencja oznacza, że qubitu nie da się dłużej opisać za pomocą wektora w przestrzeni Hilberta. W przypadku choćby „śladowego" oddziaływania komputera kwantowego z otoczeniem jedynym wyjściem jest korekcja błędów. Wykazanie możliwości kwantowej korekcji błędów było istotnym etapem w rozwoju tej dziedziny. Dlaczego stara (i nowa) płyta gramofonowa szumi, a płyta kompaktowa nie? Bo jedna jest analogowa, a druga cyfrowa. Korekcja błędów jest możliwa jedynie w przypadku cyfrowym i to właśnie jej stosowanie decyduje o jakości dźwięku muzyki odtwarzanej z płyt kompaktowych. Mimo że na pierwszy rzut oka komputer kwantowy wygląda na maszynę analogową, da się przedstawić w postaci cyfrowej. Ciekawe, że kwantowe kody poprawiające błędy same wykorzystują splątanie stanów wielu qubitów. Dość paradoksalnie splątanie qubitów wewnątrz komputera kwantowego jest pozytywne, pozwala bowiem „wyplątać się" z nieuniknionego splątania qubitów z otoczeniem i ratuje przed dekoherencją.

Mając do dyspozycji bramkę C-NOT i bramkę Hadamarda, możemy ze stanów bazowych otrzymać dowolny z czterech stanów Bella – maksymalnie splątanych stanów dwu qubitów. Stany Bella odgrywają wielką rolę w informatyce kwantowej oraz w zrozumieniu podstaw mechaniki kwantowej. To właśnie na ich przykładzie ilustruje się (i weryfikuje doświadczalnie!) słynny „paradoks" Einsteina–Podolskiego–Rosena (p. poprzednie artykuły). Układ generujący stany Bella pokazany jest obok. Widzimy, że z podstawowych stanów wejściowych produkowane są na wyjściu nastepujące:

$$
\begin{aligned}
|00\rangle &\rightarrow |00\rangle + |11\rangle \\
|01\rangle &\rightarrow |01\rangle - |10\rangle \\
|10\rangle &\rightarrow |10\rangle - |11\rangle \\
|11\rangle &\rightarrow |01\rangle + |10\rangle
\end{aligned}
$$



Schemat generacji par EPR

Wiemy już, jak zbudować komputer kwantowy... na papierze. Ale czy istnieją układy fizyczne, za pomocą których można faktycznie zrealizować komputer kwantowy (lub choćby jego elementy – kwantowe bramki logiczne)? Odpowiedź brzmi TAK, ale szczegółowe omówienie kandydatów wymagałoby osobnego artykułu.

Mimo iż prawie na pewno uda się zbudować urządzenia kwantowe, przeznaczone do rozwiązywania wybranych problemów (np. faktoryzacji), to nikt tak naprawdę nie wie, czy i kiedy powstanie uniwersalny komputer kwantowy. Jednak informatyka kwantowa to nie tylko komputery kwantowe i wykonywane na nich obliczenia. Burzliwie rozwija się kryptografia kwantowa: całkowicie bezpieczna metoda dystrybucji tajnego klucza kryptograficznego. Przesyłając słabe impulsy światła za pomocą komercyjnie dostępnych włókien światłowodowych umiemy już uzgodnić klucz pomiędzy partnerami oddalonymi od siebie o dziesiątki kilometrów. Trwają prace nad kwantowym uzgadnianiem kluczy poprzez swobodną przestrzeń – trudno przecież doprowadzić światłowód do sztucznych satelitów. Wiele prac w kryptografii kwantowej znajduje się już na etapie wdrożeń, a nie badań podstawowych. Zademonstrowano również niezwykły efekt teleportacji stanów kwantowych. Mimo tych (i innych) spektakularnych sukcesów jesteśmy dopiero na początku drogi. Nowe tysiąclecie zapowiada się więc bardzo ciekawie. A w minimach programowych studiów informatycznych może już niedługo pojawi się nowy przedmiot – informatyka kwantowa...