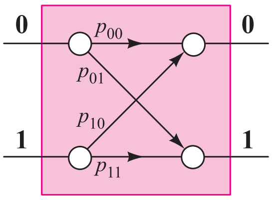
O maszynach niemożliwych

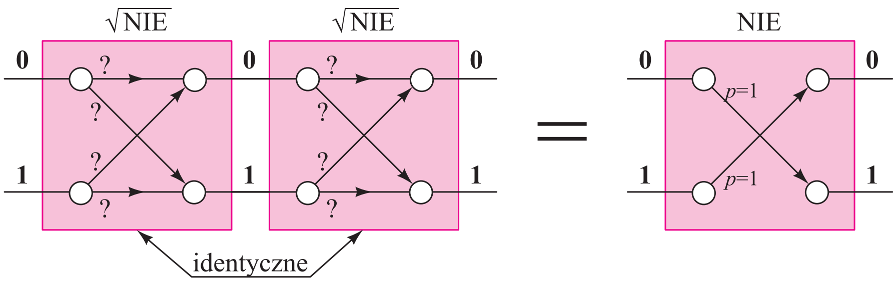
Artur EKERT

Czy są jakieś granice dla obliczeń wykonywanych przez maszyny? Oczywiście są: zarówno logiczne, jak i fizyczne. Logika mówi nam np., że żadna maszyna nie znajdzie więcej niż jedną parzystą liczbę pierwszą, podczas gdy fizyka, że żadne obliczenia nie mogą, na przykład, pogwałcić zasad termodynamiki. Co więcej, logiczne i fizyczne granice obliczeń mogą być ściśle powiązane. Powiększając naszą wiedzę o rzeczywistości fizycznej, możemy również osiągnąć nowe środki poznania logiki, matematyki i innych struktur formalnych. Zilustruję to na przykładzie maszyny, która na pierwszy rzut oka wydaje się niemożliwa do zbudowania, a jednak, uwierzcie mi, została skonstruowana przez fizyków kwantowych!
Rozważmy maszynę obliczeniową, w której dane wejściowe mogą być w jednym z dwóch stanów reprezentujących 0 i 1 (rys. 1).



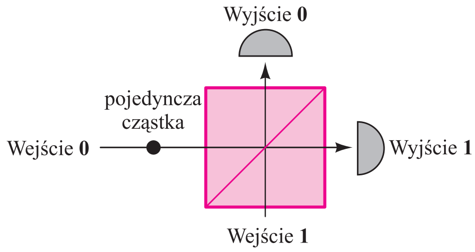
Rys. 1. Schematyczne przedstawienie najbardziej ogólnej maszyny, wykonującej przekształcenie {0,1} w siebie. Tutaj p_{ij} jest prawdopodobieństwem, z jakim maszyna daje wynik j, gdy otrzymuje na wejściu i. Działanie maszyny nie zależy od innych danych wejściowych ani przechowywanych informacji.

Maszyna ta ma tę własność, że gdy wprowadzimy dane początkowe a ($a = 0$ lub 1), to wynik, jaki otrzymamy, będzie miał wartość b ($b = 0$ lub 1) z prawdopodobieństwem p_{ab}. Może się wydać oczywiste, że jeśli prawdopodobieństwa p_{ab} są zupełnie dowolne, z wyjątkiem tego, iż spełniają warunek $\sum_b p_{ab} = 1$, to rysunek 1 przedstawia *najbardziej ogólną* maszynę, której działanie nie zależy od żadnych innych danych wejściowych ani przechowywanych informacji i która wykonuje przekształcenie zbioru {0,1} na siebie. Dwa możliwe deterministyczne rozwiązania osiągniemy wtedy, gdy przyjmiemy $p_{01} = p_{10} = 0$, $p_{00} = p_{11} = 1$ (co daje logiczną operację identyczności) lub $p_{01} = p_{10} = 1$, $p_{00} = p_{11} = 0$ (co daje operację negacji). W przeciwnym razie mamy urządzenie losowe. Załóżmy, dla przykładu, że $p_{01} = p_{10} = p_{00} = p_{11} = 0{,}5$. Tu znów może nas kusić myślenie o takiej maszynie jak o losowym przełączniku, który z jednakowym prawdopodobieństwem przekształca jakiekolwiek dane wejściowe w jeden z dwóch możliwych wyników. A jednak niekoniecznie tak być musi. Istnieje maszyna, która połączona z drugą, identyczną, realizuje negację danych wejściowych.

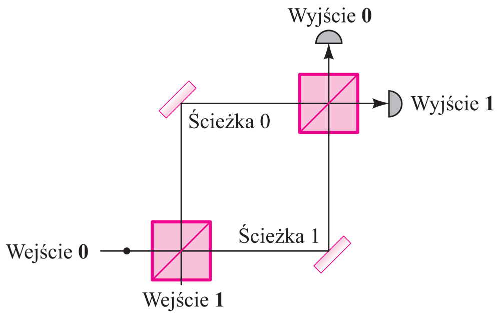


Rys. 2. Złożenie dwóch identycznych maszyn odwzorowujących {0,1} w siebie. Każda z maszyn, testowana osobno, zachowuje się jak losowy przełącznik, jednak gdy dwie maszyny są połączone, losowość znika – całkowity efekt jest operacją negacji. To oczywista sprzeczność z aksjomatami rachunku prawdopodobieństwa.

To zupełnie wbrew intuicji – sama maszyna daje 0 lub 1 z jednakowym prawdopodobieństwem niezależnie od danych wejściowych, ale dwie maszyny, jedna za drugą, działając niezależnie, wykonują operację negacji. To dlatego nazywamy tę maszynę $\sqrt{\textbf{NIE}}$. Może się wydawać rozsądne, że skoro nie ma takiej operacji w logice, to taka maszyna istnieć nie może. Ale istnieje! Fizycy badający interferencję pojedynczych cząstek rutynowo takie maszyny konstruują i niektóre z nich są tak proste, jak lustro półprzepuszczalne, tzn. lustro, które z prawdopodobieństwem 50% odbija foton na nie padający i z tym samym prawdopodobieństwem go przepuszcza. W ten sposób dwie złączone maszyny są realizowane jako sekwencja dwóch luster półprzepuszczalnych z fotonem oznaczającym w każdym z nich 0, jeśli jest na jednej z dwóch możliwych dróg, a 1 gdy na drugiej.



Rys. 3. Eksperymentalna realizacja bramki $\sqrt{\textbf{NIE}}$. Półprzepuszczalne lustro odbija połowę światła, które na nie pada. Ale pojedynczy foton się nie rozdzieli: gdy wyślemy go na takie lustro, zostanie wykryty przy wyniku 0 lub 1. Nie oznacza to jednak, że foton losowo opuszcza lustro w jednym z kierunków. W rzeczywistości foton rusza w dwóch kierunkach naraz! Może to być zademonstrowane przez złożenie dwóch luster, jak pokazano niżej.



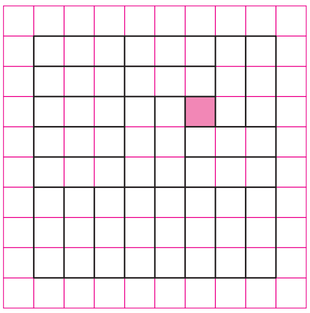
Rys. 4. Eksperymentalna realizacja złożenia dwóch bramek $\sqrt{\textbf{NIE}}$, znana jako interferencja pojedynczych cząstek. Foton, który wpada w interferometr przez wejście 0, zawsze uderza w detektor przy wyjściu 1 i nigdy nie trafia w detektor przy wyjściu 0. Każde wyjaśnienie, które zakłada, że foton obiera tylko jedną z dróg, prowadzi do wniosku, że dwa detektory powinny średnio być trafiane w połowie przypadków. Ale eksperyment pokazuje co innego!

Czytelnik może się zastanawiać, co się stało z aksjomatem rachunku prawdopodobieństwa, który mówi, że gdy E_1 i E_2 są zdarzeniami wzajemnie się wykluczającymi, to prawdopodobieństwo zdarzenia (E_1 lub E_2) jest sumą prawdopodobieństw E_1, E_2. Można argumentować, że przejście $0 \to 0$ w złożonej maszynie może się dokonać na dwa wykluczające się sposoby, mianowicie $0 \to 0 \to 0$ lub $0 \to 1 \to 0$. Ich prawdopodobieństwa wynoszą odpowiednio $p_{00}p_{00}$ i $p_{01}p_{10}$. Zatem suma $p_{00}p_{00} + p_{01}p_{10}$ przedstawia prawdopodobieństwo przejścia $0 \to 0$ w nowej maszynie. Jeśli p_{00} lub $p_{01}p_{10}$ jest różne od zera, prawdopodobieństwo to również będzie różne od zera. A jednak umiemy zbudować maszyny, w których p_{00} i $p_{01}p_{10}$ są różne od zera, ale prawdopodobieństwo przejścia $0 \to 0$ w złożonej maszynie jest równe zero. To co jest nie tak z powyższym rozumowaniem?

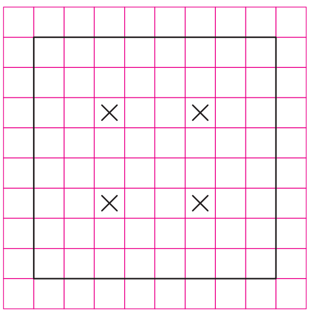
Jedna rzecz, która nie jest w porządku, to założenie, że procesy $0 \to 0 \to 0$ i $0 \to 1 \to 0$ wzajemnie się wykluczają. W rzeczywistości te procesy zachodzą jednocześnie. Nie możemy się tego dowiedzieć z teorii rachunku prawdopodobieństwa. Dowiadujemy się tego z najlepszej dostępnej obecnie teorii fizycznej, konkretnie z mechaniki kwantowej. Teoria kwantów wyjaśnia zachowanie maszyny $\sqrt{\textbf{NIE}}$ i dokładnie przewiduje prawdopodobieństwa wszystkich możliwych wyników, bez względu na to, jak połączymy maszyny. Ta wiedza powstała jako rezultat hipotez, eksperymentów i odrzucania przypuszczeń. W ten sposób upewnieni przez fizyczne doświadczenia, które potwierdzają tę teorię, logicy są teraz upoważnieni do wprowadzenia nowej operacji logicznej $\sqrt{\textbf{NIE}}$. Dlaczego? Dlatego, że jej wierny model fizyczny istnieje w naturze.

Przedstawmy teraz trochę matematycznej „maszynerii” mechaniki kwantowej, która może być użyta do opisania kwantowych maszyn obliczeniowych od najprostszej, takiej jak $\sqrt{\textbf{NIE}}$, do kwantowego uogólnienia uniwersalnej maszyny Turinga. Gdy przychodzi do formułowania przewidywań, mechanika kwantowa wprowadza koncepcję *amplitud prawdopodobieństwa* – liczb

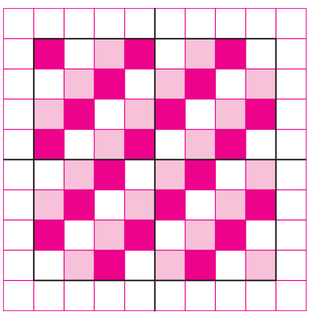
Rozwiązanie zadania M 979.
Przykład odpowiedniego pokrycia przedstawia rysunek.



Udowodnimy, że klocek 1×1 może znajdować się tylko w miejscach zaznaczonych na rysunku krzyżykiem.



Oznaczmy pola szachownicy tak jak niżej.

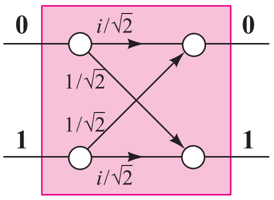


Pól zacieniowanych słabo i mocno jest po 21, pól zaś białych jest 22. Ponieważ każdy klocek 3×1 pokrywa po jednym polu każdego rodzaju, więc klocek 1×1 musi znajdować się na polu białym. Zauważmy, że jeśli odbijemy nasze pokolorowanie pól względem osi zaznaczonych na rysunku, to klocek 1×1 musi znowu znajdować się na polu białym. Jedyne pola, które są „niewrażliwe” na owe odbicia to cztery pola zaznaczone krzyżykiem na poprzednim rysunku.

Liczba zespolona c to liczba postaci $c = a + bi$, gdzie a oraz b to liczby rzeczywiste, natomiast $i^2 = -1$. Moduł liczby c to liczba $|c| = \sqrt{a^2 + b^2}$.

zespolonych c takich, że wielkości $|c|^2$ mogą być przy właściwych warunkach interpretowane jako prawdopodobieństwa. Gdy przejście (np. takie, jak: „maszyna złożona z dwóch identycznych części-maszyn startuje ze stanu 0, produkuje wynik 0 i nie wpływa na nic więcej") może się dokonać na wiele sposobów, amplituda prawdopodobieństwa całego przejścia jest sumą nie prawdopodobieństw, ale amplitud prawdopodobieństw dla poszczególnych przejść składających się na całe przejście.

W maszynie $\sqrt{\textbf{NIE}}$ amplitudy prawdopodobieństwa przejść $0 \to 0$ i $1 \to 1$ wynoszą $i/\sqrt{2}$, a amplitudy prawdopodobieństw przejść $0 \to 1$ oraz $1 \to 0$ są równe $1/\sqrt{2}$. Oznacza to, że maszyna $\sqrt{\textbf{NIE}}$ zachowuje wartość danych wejściowych z amplitudą prawdopodobieństwa $c_{00} = c_{11} = i/\sqrt{2}$ i neguje z amplitudą $c_{01} = c_{10} = 1/\sqrt{2}$. Aby uzyskać odpowiednie prawdopodobieństwa, podnosimy do kwadratu moduły amplitud prawdopodobieństwa i otrzymujemy $1/2$ zarówno dla zachowania jak i dla zanegowania danych początkowych. To opisuje zachowanie pojedynczych maszyn $\sqrt{\textbf{NIE}}$ z rysunku 1. Gdy połączymy dwie takie maszyny jak na rysunku 2, to aby obliczyć prawdopodobieństwo wyniku 0 przy danych na wejściu 0, musimy dodać amplitudy prawdopodobieństwa wszystkich „ścieżek obliczeń" do tego prowadzących. Są tylko dwie takie ścieżki – $c_{00}c_{00}$ i $c_{01}c_{10}$. Pierwsza z nich ma amplitudę prawdopodobieństwa równą $i/\sqrt{2} \times i/\sqrt{2} = -1/2$, a druga: $1/\sqrt{2} \times 1/\sqrt{2} = +1/2$. Dodajemy te amplitudy, a potem podnosimy moduł tej sumy do kwadratu. Okazuje się, że prawdopodobieństwo wyniku 0 wynosi zero. W przeciwieństwie do prawdopodobieństw, amplitudy prawdopodobieństw mogą się wzajemnie znosić!



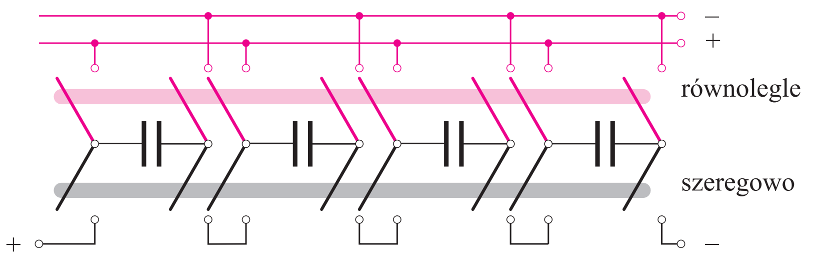
Rys. 5. Przejścia w mechanice kwantowej opisywane są przez amplitudy prawdopodobieństw.

Dodawanie amplitud prawdopodobieństwa, a nie samych prawdopodobieństw jest jedną z fundamentalnych reguł w przewidywaniach mechaniki kwantowej i stosuje się do wszystkich obiektów fizycznych, w szczególności do kwantowych maszyn obliczeniowych. Jeśli maszyna obliczeniowa rozpoczyna pracę w pewnej konfiguracji (wejście), to prawdopodobieństwo, że po jej ewolucji przez kolejne pośrednie konfiguracje znajdzie się w określonym stanie, równa się kwadratowi modułu sumy wszystkich amplitud prawdopodobieństwa przejść pomiędzy konfiguracjami pośrednimi. Amplitudy mogą się wzajemnie znosić, co określa się mianem destrukcyjnej interferencji, lub wzmacniać się wzajemnie, co określa się jako konstruktywną interferencję. Podstawowa idea obliczeń kwantowych to użycie interferencji kwantowej do wzmocnienia poprawnych rezultatów i zagłuszenia niewłaściwych.

Wymagania konieczne do praktycznego zastosowania komputerów kwantowych są bardzo wysokie. Obecnie nie wiadomo, jak, a nawet czy w ogóle, w pełni wyposażone komputery kwantowe będą rzeczywiście budowane; niemniej jednak odkrycie mechaniki kwantowej już zmieniło nasze rozumienie natury obliczeń!

Rozwiązanie zadania F 565.

Możliwy schemat dla baterii czterech kondensatorów przedstawiony jest na poniższym rysunku.



Jak widać, niezbędny jest przełącznik ośmiobiegunowy. Górne położenie sztabki przełącznika odpowiada równoległemu połączeniu kondensatorów, dolne zaś – szeregowemu.