Q# – czas na kwantowe języki programowania

W jakim kierunku rozwijać się będą języki programowania? Pytanie wbrew pozorom jest dość trudne i możemy wskazać raczej tylko tendencje, jak np. wzrastającą popularność języków funkcyjnych lub dalsze zwiększanie roli języków skryptowych czy interpretowanych. Jednakże powinniśmy też wziąć pod uwagę fakt, iż od dłuższego czasu rozwijają się nowe podejścia do obliczeń, a takim nowym modelem obliczeniowym, jaki warto wymienić, są obliczenia kwantowe.

Minie jeszcze sporo czasu, zanim na naszych biurkach zagoszczą komputery w pełni kwantowe działające w temperaturze pokojowej (ale to może stać się szybciej, niż może nam się wydawać), jednak już dziś mamy kilka eksperymentalnych instalacji maszyn kwantowych, gdzie można wykonywać kwantowe algorytmy, testować wybrane protokoły. Działają w temperaturze bliskiej zera absolutnego (zatem zwykła zamrażarka niestety nie wystarczy ;-)). Tworzone są także języki programowania dla przyszłych maszyn kwantowych, a jednym z nich jest Q#. Choć nie mamy jeszcze dostępu do wydajnych komputerów kwantowych, to jednakże można zastosować symulatory, aby rozpocząć tworzenie programów, które co prawda będą tylko symulowane, ale można już teraz zacząć uczyć się kwantowego modelu obliczeniowego. Ma on kilka niezwykłych właściwości, które będą w przyszłości stanowić o jego sile. W tym artykule chcemy pokazać wybrane przykłady obliczeń kwantowych. Naturalnie jest to bardzo skrótowe przedstawienie wybranych pojęć, jednak bez większych kłopotów znajdziemy w Internecie wiele dodatkowych informacji, zatem już teraz zachęcamy do dalszych poszukiwań.

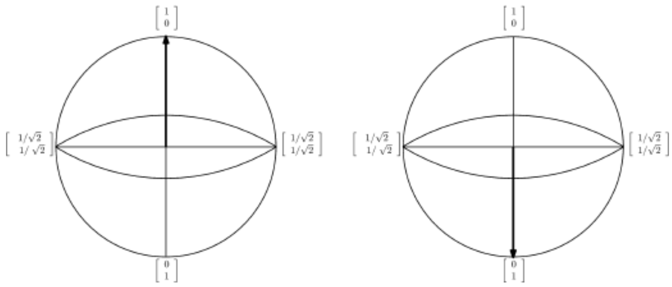
MODEL OBLICZEŃ KWANTOWYCH W PIGUŁCE

Podstawy modelu obliczeń kwantowych opierają się na wektorach i macierzach. Jednak nie będziemy tu wprowadzać wszystkich podstawowych definicji. Zaczniemy od podstawowej jednostki informacji kwantowej, czyli qubitu:

$$\mathbf{0} = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \mathbf{1} = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad |\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$

Zdefiniowaliśmy dwa podstawowe stany: zero oraz jeden. Stosujemy też notację Diraca, tj. zero zapisujemy jako $|0\rangle$. Qubit o nieznanym stanie $|\psi\rangle$ to suma dwóch podstawowych stanów zera oraz jedynki (wektory te stanowią też tzw. standardową bazę obliczeniową). Wartości alfa oraz beta to liczby zespolone i zakłada się, iż kwadrat ich modułów sumuje się do jedności. Jest to tzw. interpretacja probabilistyczna, ale same wartości alfa i beta nazywamy amplitudami prawdopodobieństwa.

Na Rysunku 1 przedstawiono wizualizację qubitu za pomocą sfery Blocha, bowiem choć mamy dwa wektory zero oraz jeden, to qubit można ukazać jako trajektorię na sferze Blocha. Na wspomnianym rysunku przedstawiono dwa bazowe przypadki stanów: zero oraz jeden. Mamy też znaczone dwa inne stany będące tzw. superpozycją stanów zero oraz jeden.



Rysunek 1. Qubit jako sfera Blocha

Kolejna istotna konstrukcja to rejestr kwantowy złożony z n qubitów:

$$Q_{reg} = q_1 \otimes q_2 \otimes q_3 \otimes \ldots \otimes q_n$$

Poszczególne qubity są połączone za pomocą operacji iloczynu tensorowego, ale istotniejszym jest fakt, ile informacji można zgromadzić w rejestrze kwantowym. Jeśli mamy n qubitów, to możemy zapisać 2^n klasycznej informacji w qubicie. Inaczej mówiąc, mamy wykładniczo więcej informacji w qubitach niż w klasycznych nośnikach informacji. Trzeba także dodać, iż nie zawsze można stosować iloczyny tensorowe do zapisu stanu rejestru kwantowego. Występują tzw. stany splątane, które nie rozkładają się na iloczyn tensorowy, np. dwóch qubitów. Stany splątane są bardzo ważnym elementem informatyki kwantowej, np. pozwalają na realizację teleportacji kwantowej.

W naszym krótkim wprowadzeniu opiszemy jeszcze operację unitarną. Przetwarzanie rejestru kwantowego realizujemy w taki sposób:

$$U|\psi_0\rangle = |\psi_1\rangle$$

co oznacza, iż stan kwantowy psi zero został za pomocą operacji unitarnej U przekształcony do stanu psi jeden. I wbrew pozorom, z punktu widzenia matematyki, jest to bardzo prosta operacja, gdyż U jest macierzą unitarną, wystarczy zatem przemnożyć wektor przez macierz, aby otrzymać nowy wektor. Upraszczając, bramki kwantowe reprezentują różne operacje unitarne.