

Wykorzystanie metod ewolucyjnych w projektowaniu algorytmów kwantowych

mgr inż. Robert Nowotniak

Informatyka kwantowa zajmuje się wykorzystaniem możliwości obliczeniowych miniaturowych układów, podlegających prawom mechaniki kwantowej. Dzięki unikalnym właściwościom takich układów możliwe jest rozwiązywanie niektórych problemów algorytmicznych w sposób znacznie bardziej efektywny niż mogą to wykonywać klasyczne algorytmy. Do problemów tej klasy należy np. faktoryzacja liczb, istotna z punktu widzenia używanych powszechnie kryptosystemów (RSA).

Celem pracy było: stworzenie środowiska symulacji komputera kwantowego (wirtualny komputer kwantowy) zaimplementowanie podstawowych algorytmów kwantowych (w pracy zaimplementowałem cztery takie algorytmy) oraz zbadanie możliwości wykorzystania metod ewolucyjnych sztucznej inteligencji w projektowaniu algorytmów kwantowych

W pracy został przedstawiony oraz wykorzystany model obliczeniowy kwantowych bramek logicznych i obwodów kwantowych. Jednym ze sposobów opisu algorytmów kwantowych są układy kwantowych bramek logicznych, czyli obwody kwantowe (ang. *quantum circuits*). Dowolny algorytm kwantowy może być wyrażony w ten sposób (obwody kwantowe są równoważne kwantowej maszynie Turinga). Podstawową różnicą pomiędzy bramkami kwantowymi, a klasycznymi bramkami logicznymi, jest to, że mogą one przetwarzać superpozycję wszystkich możliwych stanów wejściowych. Bramki kwantowe opisywane są przez macierze unitarne i wykonują uogólnione obroty w przestrzeniach Hilberta stanów rejestrów kwantowych.

W pracy zostały wykorzystane układy kwantowych bramek logicznych do symulacji obliczeń kwantowych. Zaproponowano model obiektowy dla obliczeń kwantowych, pozwalający na symulację pracy komputera kwantowego w dowolnym obiektowym języku programowania. Na jego podstawie powstała biblioteka `qclib`¹ dla języka Python. Za jej pomocą zostały zaimplementowane podstawowe algorytmy kwantowe oraz zostały zbadane aspekty obliczeń kwantowych, w których mogą być wykorzystane metody ewolucyjne sztucznej inteligencji: optymalizacji bramek kwantowych za pomocą algorytmów genetycznych oraz projektowanie całych obwodów kwantowych za pomocą programowania genetycznego.

Podstawowymi klasami zaproponowanego modelu obiektowego są: klasa `QuantumRegister`, reprezentująca rejestr kwantowy, opakowująca wektor liczb zespolonych z przestrzeni Hilberta stanów układu kwantowego; klasa `QuantumCircuit`, posiadająca uporządkowaną kolekcję obiektów, będących kolejnymi etapami obliczeń; abstrakcyjna klasa `QuantumGate`, definiująca podstawowe operacje na bramce kwantowej. Z klasy tej dziedziczą

¹<http://quantum.ics.p.lodz.pl/qclib>

konkretne bramki kwantowe (bramka sterowanej negacji, bramki Hadamarda, Toffoliego, Fredkina). W oparciu o ten model obiektowy została stworzona biblioteka dla języka Python — qclib.

W bibliotece qclib została również wykorzystana koncepcja przeciążania operatorów do wykonywania operacji na bramkach i obwodach kwantowych. Przeciążony operator `**` odpowiada wykonaniu operacji iloczynu tensorowego na macierzach bramek kwantowych, co jest równoważne połączeniu równoległemu bramek. Operator `*` opowiada natomiast składaniu odwzorowań, czyli szeregowemu połączeniu bramek w obwodzie. Dodatkowo przeciążony operator nawiasów dla klasy `QuantumGate` pozwala „wywoływać” bramki kwantowe lub całe obwody kwantowe jako pewnego rodzaju „procedury kwantowe”.

Za pomocą stworzonej biblioteki qclib zostały zaimplementowane następujące cztery algorytmy kwantowe: kodowanie supergęste, protokół teleportacji kwantowej, algorytm Grovera i generowanie stanów splątanych. Na przykładzie tych algorytmów zaprezentowano możliwość wykorzystania metod ewolucyjnych: minimalizacja liczby etapów obliczeń (istotne z punktu widzenia unikania dekoherencji układu kwantowego) lub automatyczne zaprojektowanie obwodu za pomocą ustalonego podzbioru bramek kwantowych.

Projektowanie algorytmów kwantowych jest trudnym zadaniem z powodu kilku istotnych trudności. Algorytmy kwantowe działają w zupełnie inny sposób niż algorytmy klasyczne. Na wektorach bazy przestrzeni stanów rejestru kwantowego może zostać rozpięta cała podprzestrzeń rozwiązań problemu obliczeniowego, a algorytm kwantowy przetwarza wszystkie możliwe rozwiązania w jednym cyklu — kolejne iteracje służą natomiast do tego, by maksymalizować prawdopodobieństwo uzyskania poszukiwanego rozwiązania. Amplitudy prawdopodobieństw, związane z różnymi rozwiązaniami problemów obliczeniowych, mogą interferować ze sobą, w sposób konstruktywny lub destruktywny. Wszystko to powoduje, że projektowanie takich algorytmów jest trudne do „uchwycenia” przez ludzki umysł.

Wspomaganie człowieka w rozwiązywaniu trudnych problemów jest jednym z kluczowych zadań sztucznej inteligencji. *„Programy komputerowe, które mogą „ewoluować” w sposób, naśladujący mechanizmy doboru naturalnego, potrafią rozwiązywać złożone problemy, które są trudne do pełnego zrozumienia nawet dla ich twórców.”* — John H. Holland

W pracy zostały rozważone następujące aspekty obliczeń kwantowych, w których można posłużyć się metoda ewolucyjnymi sztucznej inteligencji: projektowanie bramek kwantowych (optymalizacja macierzy unitarnych) oraz projektowanie całych obwodów kwantowych. W pierwszym przypadku zaprezentowane zostało podejście wykorzystujące prosty algorytm genetyczny do projektowania jednokubitowych bramek kwantowych oraz zmodyfikowany algorytm genetyczny, mający elementy charakterystyczne dla strategii ewolucyjnej. Automatyczne projektowanie obwodów kwantowych zostało zademonstrowane z użyciem reprezentacji obwodów kwantowych w postaci całkowitoliczbowej oraz w postaci drzew (programowanie genetyczne). Omówione podejścia zostały zilustrowane eksperymentami numerycznymi z wykorzystaniem biblioteki qclib.

Jednym z przeprowadzonych eksperymentów numerycznych było automatyczne zaprojektowanie – za pomocą programowania genetycznego – obwodu kwantowego, generującego trzykubitowy stan splątany. W eksperymencie tym zastosowano typowe dla algorytmu genetycznego parametry: licznosc populacji – 100, prawdopodobieństwo rekombinacji –

75%, prawdopodobieństwo mutacji 5%, rekombinacja i mutacja jednopunktowe. Na etapie selekcji zastosowano wybór za pomocą koła ruletki z elementem elitarności — 5 najlepiej ocenianych obwodów (posiadających najlepszy materiał genetyczny) było zawsze przenoszonych do następnej epoki.

Za pomocą tej metody został znaleziony alternatywny obwód kwantowy, generujący trzykubitowy stan splątany $\frac{\sqrt{2}}{2}(|000\rangle + |111\rangle)$. Obwód ten składa się z czterech etapów obliczeń (sterowana negacja, bramka Hadamarda i bramka T).

Przeprowadzone eksperymenty numeryczne pokazują, że zaproponowany model obiektowy dla obliczeń kwantowych pozwala na łatwą symulację pracy komputera kwantowego. Innowacyjny język opisu obliczeń kwantowych, wykorzystujący przeciążone operatory, pozwala na zwięzły zapis algorytmów. Eksperymenty z wykorzystaniem algorytmów i programowania genetycznego pokazują, że metody ewolucyjne są skutecznymi narzędziami w projektowaniu różnych aspektów obliczeń kwantowych.