УДК 681.32

В. П. Семеренко
В. В. Ткачук

ЗАВАДОСТІЙКЕ КОДУВАННЯ У КВАНТОВИХ КОМП'ЮТЕРАХ

Вінницький національний технічний університет

Анотація

Показано, що основною перепоною для створення реального квантового комп'ютера є недостатній рівень достовірності квантових обчислень. Для передачі даних по квантовим каналам запропоновано використання циклічних кодів. Доведено, що представлення циклічних кодів за допомогою теорії лінійних послідовнісних схем (ЛПС) дозволяє в максимальній мірі використати квантовий паралелізм.

Ключові слова: квантові комп'ютери, циклічні коди, лінійна послідовнісна схема (ЛПС).

Abstract

It is shown that the main obstacle to the creation of a real quantum computer is the insufficient level of reliability of quantum computations. The use of cyclic codes for the transmission of data through quantum channels is proposed. It is proved that representation of cyclic codes based on the theory of linear finite-state machine (LFSM) makes it possible to use quantum parallelism to the maximum extent.

Keywords: quantum computer, cyclic codes, linear finite-state machine (LFSM)

Вступ

Можливості збільшення продуктивності комп'ютерів в рамках послідовних принципів обробки даних вже давно вичерпали себе. Отримати суттєвий приріст в продуктивності можна лише за допомогою паралельної обробки даних та застосування принципово нових комп'ютерних архітектур [1]. В цьому напрямку дуже перспективними є квантові обчислення [2].

Як відомо, найкращим стимулом розвитку нових ідей є нагальна практична потреба в їх реалізації. Сьогодні вже можна виділити декілька основних сфер використання квантових комп'ютерів. Однією з найбільших проблем світового значення є протистояння кібератакам та надійний захист інформації [3]. З кожним роком зростає значення швидкого та професійного прийняття рішень з використанням штучного інтелекту. Важливим також є поєднання квантових та оптичних технологій обробки даних.

В цих та інших сферах використання переваг квантових обчислень (дуже висока швидкодія та паралелізм в обчисленнях) може сприяти великим досягненням як в теорії так і на практиці. Але для цього необхідно вирішити ще ряд задач. Однією з них є задача забезпечення високої достовірності обчислень.

Сучасна технологія виготовлення квантових пристроїв не дозволяє поки що уникнути великої кількості помилок, які треба виявляти та виправляти в реальному часі. Звичайно, схожа проблема притаманна і класичним комп'ютерам, тому для її вирішення вже давно використовується завадостійке кодування [4].

Основні математичні принципи кодування і декодування даних однакові для всіх типів обробки даних. Безумовно, квантові обчислення вносять свою специфіку, тому дослідження завадостійких кодів в квантових комп'ютерах є актуальною та важливою задачею.

Циклічні коди у квантових комп'ютерах

На квантовому комп'ютері можна вирішувати будь-які математичні задачі, питання полягає лише в ефективності такого застосування. Алгоритм виконання задачі, який є достатньо ефективним на класичному комп'ютері, не обов'язково буде таким на квантовому.

Квантові комп'ютери на відміну від класичних оперують на бітами, а кубітами (*quantum bit*), які можуть знаходитись не тільки в станах "0" і "1", але і в їх суперпозиції: тобто одночасно в цих

двох станах. Ще одна принципова особливість квантових обчислень: при вимірюванні кубіт переходить в стан “0” або “1”, а попередній стан втрачається. Тому стан кубіту не можна скопіювати.

Основним пристроєм квантового комп’ютера є квантовий регістр, тобто схема із n кубітів, які можуть знаходитись в тензорному (розімкнутому), або в заплутаному (зачепленому) стані $S(t)$. Стан регістра можна виміряти. На цьому регістрові і відбуваються всі обчислення квантового комп’ютера [5].

Елементарним кроком при квантових обчисленнях є операція суперпозиції над n-розрядним квантовим регістром, тобто паралельна обробка відразу всіх 2^n можливих станів. А для класичного комп’ютера подібна операція вимагає 2^n кроків. Таким чином, якщо багатокроковий послідовний алгоритм на комп’ютері з фон-нейманівською архітектурою можна замінити на однокроковий алгоритм на основі квантового паралелізму, тоді ми отримаємо максимальний виграш в швидкості обчислень.

Саме таку ситуацію ми маємо при використанні циклічних кодів на основі теорії лінійних послідовнісних схем (ЛПС). ЛПС є лінійним автоматом, який в полі Галуа $GF(q)$ в дискретні моменти часу t задається функцією переходів

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(q), \tag{1}$$

та функцією виходів

$$Y(t) = C \times S(t) + D \times U(t), \quad GF(q). \tag{2}$$

Всі алгоритми кодування і декодування циклічних кодів в [6] використовують функції (1) та (2), що є необхідною вимогою їх ефективного використання у квантових комп’ютерах.

Висновки

Проблема достовірності результатів квантових обчислень є сьогодні основною перепоною для створення реального квантового комп’ютера. В квантових каналах зв’язку завжди є завади, тому на практиці завжди мають використовуватись завадостійкі коди. Перспективними в цьому плані є циклічні коди, для представлення яких використовується теорія ЛПС. Цей математичний апарат є ефективним як для традиційних, так і для квантових комп’ютерів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Семеренко, В. П. Технології паралельних обчислень : навчальний посібник – Вінниця : ВНТУ, 2018. – 104 с.
2. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. – М.: Мир, 2006. – 824 с.
3. Горбенко Ю. І., Ганзя Р.С. Аналіз шляхів розвитку криптографії після появи квантових комп'ютер1в / *Вісник Національного університету* "Львівська політехніка". 2014. № 806. С. 40-48.
4. Николаенко С.В., Василиу Е.В. Оценка корректирующей способности помехоустойчивого кода Файра для реализации пинг-понг протокола с парами перепутанных кубитов в квантовом канале с помехами, *Захист інформації* 2012. – № 3. – С. 28-36.
5. Шпаковский Г. И. Реализация параллельных вычислений: кластеры, многоядерные процесры, грид, квантовые компьютеры. – Минск, БГУ, 2011 г., 155 с.
6. Семеренко В. П. Теорія циклічних кодів на основі автоматних моделей : монографія. Вінниця : ВНТУ, 2015. – 444 с.

Василь Петрович Семеренко – канд. техн. наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: *vasilsemerenko@gmail.com*

Ткачук Віктор Володимирович – студент групи 2КІ-16б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: *vitya.tkachuk.99@gmail.com*

Vasyl P. Semerenko – PhD, Associate Professor, Department of computer technique, Vinnytsia National Technical University, Vinnytsia, e-mail: *vasilsemerenko@gmail.com*

Victor V.Tkachyk – student, Department of computer technique, Vinnytsia National Technical University, Vinnytsia. e-mail: *vitya.tkachuk.99@gmail.com*