УДК 164; 510

Булеві квантові логічні операції

Микола Будник[1,2,3]

[1] д. т. н., г. н. с., Інститут кібернетики ім. В.М. Глушкова НАН України, просп. Академіка Глушкова, 40, 03680, Київ, e-mail: budnykmykola@gmail.com
[2] д. т. н., професор, ННІ високих технологій, Київський національний університет імені Тараса Шевченка, просп. Академіка Глушкова, 4Г, 03680, Київ, e-mail: budnykmykola@gmail.com
[3] д. т. н., професор, кафедра комп'ютерних наук, Сумський державний університет, вул. Римського-Корсакова, 2, 40007, Суми, e-mail: budnykmykola@gmail.com

У роботі запропоновано узагальнення булевих операцій для квантових обчислень. Показано, що базовий набір булевих однокубітних операцій містить 6 операцій та має 2 варіанти наборів по 4 операції. Запропоновано 9 квантових операцій додатково до 7-ми класичних (еквіваленція, диз'юнкція, кон'юнкція, імплікація, заперечення диз'юнкції, заперечення кон'юнкції, виключна диз'юнкція). В результаті отримано повний набір 16 однокубітних операцій, які забезпечують 16^4 = 65 тисяч 536 бінарних (двокубітних) логічних операцій, що відповідає кількості базових станів 16-кубітного квантового процесора. Велика кількість операцій дозволить підвищити продуктивність квантових обчислень в цифрових симуляторах квантових процесорів з точки зору паралельності обчислень та скорочення програмного коду.

Ключові слова: квантові обчислення, логічні операції, булева алгебра

Вступ. На сьогодні у галузі зв'язку та високопродуктивних обчислень активними темпами розробляють та активно впроваджують квантові технології. Багато дослідників вважають, що у найближчому майбутньому квантові технології забезпечать ключові досягнення у багатьох сферах діяльності людини, які потребують надшвидке вирішення обчислювальних задач великої складності, зокрема в криптографії та моделюванні надскладних процесів [1].

Перспективи в галузі високопродуктивних обчислень ґрунтуються на застосуванні квантових комп'ютерів, які використовують заплутані (зчеплені) квантові стани. При цьому стани включають як чисті стани окремих кубітів, так і змішані стани, які є результатом взаємодії (інтерференції) декількох кубітів. Всього кількість таких, так званих базових, станів становить 2^N, де N - кількість кубітів. Тобто для 8-кубітного квантового процессора кількість станів рівна 2^8=256, а для 16-кубітного – вже 2^{16}=65 536 станів [2].

З точки зору теорії обчислень, кожний стан – це сигнал (число), записаний у певному розряді вихідного квантового регістру, що має 2^N розрядів. На кожному такті роботи процесора кожний сигнал – це результат виконання певної логічної операції. На сьогодні в класичній теорії обчислень відомо 8 операцій, з яких одна унарна – заперечення та 7 бінарних – еквіваленція, диз'юнкція (АБО), кон'юнкція (І), імплікація, заперечення диз'юнкції (НЕАБО), заперечення кон'юнкції (НЕІ), виключна диз'юнкція (виключне АБО, сума по модулю 2, $\oplus$).

Зрозуміло, що ця кількість катастрофічно мала порівняно з потенціалом квантових обчислень. Отже, в симуляторах квантових обчислень потрібно забезпечити не сотні, а навіть тисячі логічних операцій. В даній роботі вирішується завдання збільшення кількості булевих логічних операцій для квантових обчислень.

1. Базові квантові логічні операції

Під булевими будемо розуміти операції, елементи матриць яких можуть набувати лише значення 0 чи 1. Тому операції типу Адамара, які мають нецілі значення елементів матриці, а також комплексні значення, тут не розглядаються. Також відмітимо, що квантові булеві операції мають інший смисл – це не таблиці істинності, а матричні оператори, з точки зору теорії функцій – вектор функції векторного аргументу з розмірністю вектора рівному 2. Тобто багатомісні операції не є згортками, а є векторними, тобто мають кількість результатів (виходів), яка рівна кількості входів (операндів).

З літератури відомо такі булеві квантові операції [3]

$$EQV \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad NOT \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad CNOT \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \tag{1}$$

Перші 2 операцій з них – Еквіваленція EQV (операція Паулі) та Квантове Заперечення NOT є однокубітними, а третя – Кероване Заперечення CNOT є двокубітною. З точки зору класичної теорії обчислень, однокубітна операція завжди є одномісною, в той час як 2-кубітна може бути 1- чи 2-місною, залежно від того, кубіти є розрядами одного регістра (в який записано якесь число - операнд), чи належать двом різним регістрам, в які записані різні операнди.

Для розуміння спочатку розглянемо питання про набір базових операцій, на основі яких можна реалізувати логічні обчислення. Це питання не є принциповим для квантових обчислень в тому сенсі, що для квантових обчислень їх занадто замало. З іншого боку, це дасть розуміння відмінності між неквантовими та квантовими булевими операціями.

У класичній булевій логіці прийнято, що логічні операції – заперечення, диз'юнкція та кон'юнкція є базовими в тому сенсі, що за їх допомогою можна реалізувати довільний логічний вираз. Цей результат суперечить квантовим обчисленням тому, що класична одномісна операція заперечення відсутня, вона має вигляд матриці NOT (1). Отже, в якості операції заперечення потрібно в набір базових операцій включати операцію NOT (1).

Щодо диз'юнкції (І) та кон'юнкції (АБО) теж не все так просто. У цифрових процесорах реально реалізуються електронні схеми (у квантовій інформатиці – так звані гейти) операції НЕ-АБО та НЕ-І. З точки зору класичних обчислень немає різниці, чи у даному процесорі реалізується АБО чи І, чи їх заперечення НЕ-АБО чи НЕ-І.

У квантовій інформатиці це питання принципове тому, що базові квантові логічні операції повинні бути ортогональними (у строгому сенсі по меншій мірі лінійно незалежними). Це значить, що їх скалярний добуток (тобто згортка прямого добутку їх матриць) повинен бути рівний нулю. Отже, допустимо комбінувати лише пару АБО та НЕ-І, чи пару НЕ-АБО та І. В результаті, для квантових обчислень існує 4 базових булевих операцій, причому має місце 2 варіанти їх наборів (2) чи (3)

$$EQV \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad NOT \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad HEI \equiv \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad АБО \equiv \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \tag{2}$$

$$EQV \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad NOT \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad I \equiv \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad НЕАБО \equiv \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \tag{3}$$

2. Одномісні (однокубітні) операції

Розглянуте в попередньому пункті питання про базові операції має в основному теоретичне значення, тому що цих операцій занадто мало. Єдине практичне значення має місце у випадку «квазікласичного» симулятора квантового процесора, у якому замість класичного набору операцій (заперечення, диз'юнкція та кон'юнкція) будуть застосовані квантові набори (2) чи (3).

Для збільшення кількості операцій потрібно розглянути всі можливі комбінаторні набори 0 та 1. Так як матриця має розмірність 2x2, тобто містить 4 елементи, то кількість можливих комбінацій становить 2^4=16. Тоді всі можливі 16 квантових булевих операцій зручно упорядкувати у матрицю згідно Рис.1.

$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$
EQV Еквіваленція	<X1>	НЕ І, Заперечення кон'юнкції	НЕ $\bar{I}$
$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$
<X2>	NOT Заперечення	$\overline{АБО}$ імплікація	АБО диз'юнкція
$\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$
І кон'юнкція	$\bar{I}$	<0>, НЕ <1>, Квантовий нуль, НІ	<Y2>
$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$
НЕ $\overline{АБО}$, заперечення імплікації	НЕ АБО Заперечення диз'юнкції	<Y1>	<1>, НЕ <0>, Квантова 1, ТАК

Рис. 1. Всі можливі квантові булеві операції (матриця операцій)

З рис. 1 видно, що матриця має 4 блоки по 4=2x2 елементи та симетрії, а саме – сума матриць на діагоналях блоків завжди дають одиничну матрицю (4)

$$\hat{1} = EQV + NOT = \langle X1\rangle + \langle X2\rangle = \langle Y1\rangle + \langle Y2\rangle = <0> + <1>, \quad (4а)$$

$$\hat{1} = АБО + НЕІ = I + НЕАБО = \overline{АБО} + НЕ\bar{I} = \bar{I} + НЕ\overline{АБО}, \quad (4б)$$

Тут враховано, що одномісна квантова операція має загальний вигляд (5), де Aij – це 0 чи 1, а X1,2 та Y1,2 – вхідні та вихідні логічні операнди

$$\begin{pmatrix} Y1 \\ Y2 \end{pmatrix} \equiv \begin{bmatrix} A11 & A12 \\ A21 & A22 \end{bmatrix} \begin{pmatrix} X1 \\ X2 \end{pmatrix}, \quad (5)$$

Назви операцій взяті по аналогії із класичними булевими операціями, хоч потрібно пам'ятати, що в квантових обчисленнях вони мають інший смисл. Слово НЕ означає квантове заперечення даної операції, наприклад NOT – заперечення еквіваленції EQV. Квантове заперечення NOT формально відповідає класичній сумі по модулю 2, $\oplus$ чи виключному АБО (Exclusive OR, XOR). Його смисл в інверсії від обох операндів x та y (для відмінності операнди класичних операцій позначаємо малими буками, бо вони мають інший смисл).

Штрихом зверху позначено так звані операції «часткового заперечення» $\overline{АБО}$ і $\bar{I}$, у матрицях яких стовпчики поміняні місцями. З точки зору класичної інформатики це означає, що береться інверсія від першого операнду x. Тобто воно має смисл неповного, часткового заперечення АБО лише по першому операнду x. Таке «часткове заперечення» $\overline{АБО}$ має класичний аналог – імплікацію, яка позначається як $x \to y$, та в наших позначеннях має вигляд (6)

$$\overline{АБО} : x \to y = \neg x \vee y = АБО(\neg x, y), \quad (6)$$

Отже, класична імплікація – це «часткове заперечення» диз'юнкції по першому операнду x. Квантова імплікація $\overline{АБО}$ - це «часткове заперечення» квантової диз'юнкції АБО. «Часткове заперечення» квантової імплікації НЕ$\overline{АБО}$ (7) означає, що у матриці поміняні місцями рядки. Аналогічно, з точки зору класичної інформатики це означає, що береться інверсія від другого операнду y

$$НЕ\overline{АБО} : x \vee \neg y = АБО(x, \neg y), \quad (7)$$

Для квантової операції $\bar{I}$ та його «часткового заперечення» НЕ$\bar{I}$ відсутні класичні аналоги. Проте, аналогічно (6-7) можна показати формальну відповідність з класичними функціями у вигляді (8)

$$\bar{I} : \neg x \wedge y = I(\neg x, y), \quad НЕ\bar{I} : x \wedge \neg y = I(x, \neg y), \quad (8)$$

Для «примітивних» квантових операцій <X1>, <X2>, <Y1>, <Y2> також відсутні класичні аналоги, їх визначення надається виразами (10-11)

$$\langle X1\rangle : Y1 = Y2 = X1, \quad \langle X2\rangle : Y1 = Y2 = X2, \quad (9)$$

$$\langle Y1\rangle : Y1 = X1 + X2, \quad Y2 = 0, \quad \langle Y2\rangle : Y2 = X1 + X2, \quad Y1 = 0. \tag{10}$$

2. Двокубітні операції

У загальному вигляді двокубітна булева операція має вигляд (11)

$$\begin{pmatrix} Y11 \\ Y12 \\ Y21 \\ Y22 \end{pmatrix} \equiv \begin{bmatrix} U11 & U12 \\ U21 & U22 \end{bmatrix} \begin{pmatrix} X11 \\ X12 \\ X21 \\ X22 \end{pmatrix}, \tag{11}$$

де Uij – одна із 16-ти операцій, наведена на Рис. 1. Матриця операції містить 2x2=4 блоки, кожен блок у свою чергу має 2x2 елементи і є матрицею якоїсь одномісної операції Uij. Таким чином, всього може бути реалізовано 16^4 = 65 тисяч 536 бінарних (двокубітних) логічних операцій. Наприклад, відома 2-кубітна операція Кероване Заперечення CNOT (1) – це частковий випадок операції загального виду (11), коли U12=U21=<0>, U11=EQV, U22=NOT.

Висновки. В роботі запропоновано 9 1-кубітних булевих операцій та отримано повний набір з 16-ти квантових операцій. Це забезпечує 16^4 = 65 тисяч 536 бінарних (двокубітних) операцій, що відповідає кількості базових станів 16-кубітного квантового процесора. Велика кількість операцій реалізує потенціал квантових обчислень в цифрових симуляторах квантових процесорів.

Література

[1] Wolf E.L. Quantum Nanoelectronics: An Introduction to Electronic Nanotechnology and Quantum Computing. – Wiley. – 2009. – 472 p.
[2] *Войтович І.Д., Корсунський В.М.* Перспективи квантових обчислень з використанням надпровідності // Математичні машини і системи. – 2008. – № 4. – С. 23–56
[3] *Будник М.М., Баужа О.С., Войтович І.Д., Корсунський В.М.* Вступ до квантових обчислень та квантових комп'ютерів: навчальний посібник. – Київ: Інтерсервіс, 2014. – 95 с.

Boolean quantum logic operations

Mykola Budnyk

The paper proposes generalization of Boolean logic operations intended for quantum computing. It is shown that the basic set of Boolean one-qubit operations contains 6 ones and has 2 variants of sets of 4 operations. 9 unary quantum operations are proposed in addition to 7 classical ones (equivalence, OR, XOR, AND, NOR, NAND, implication). As a result, a complete set of 16 one-qubit operations was obtained, which provides 16^4 = 65 thousand 536 binary (two-qubit) logical operations that corresponds to the number of base states of a 16-qubit quantum processor. Large number of operations will allow increase performance of computing in digital simulators of quantum processors from the viewpoint of computing parallelism and reducing the program cod.

Отримано 30.03.23