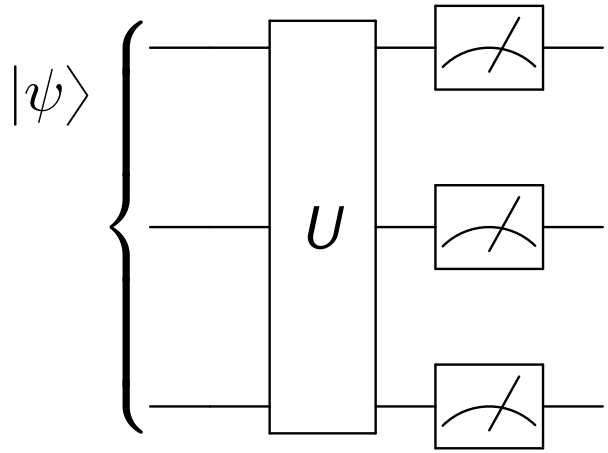
Квантові схеми. Контрольовані операції. Обертовні обчислення.

Лекція 4

28 лютого 2023

Квантові схеми

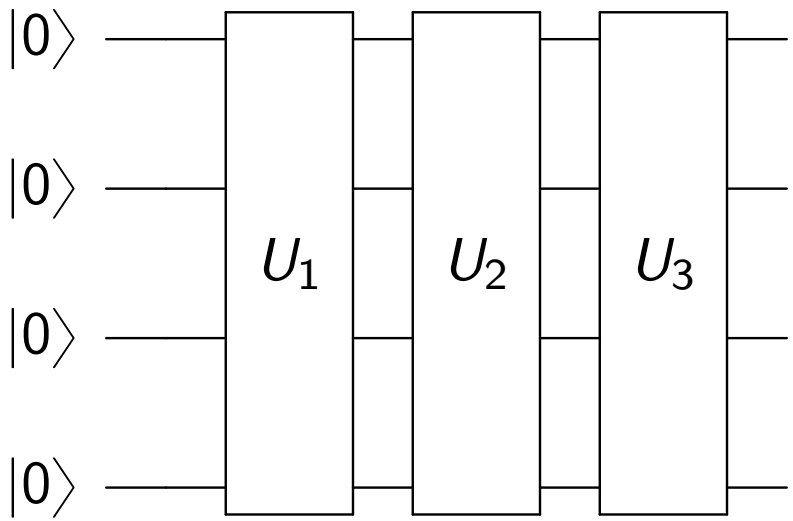
Квантова схема – це графічне зображення квантової операції, яка діє на стан багатокубітної системи $|\phi\rangle \in H = (\mathbb{C}^2)^{\otimes n}$. Наприклад, унітарна операція $|\phi\rangle \longrightarrow U|\phi\rangle$ зі стандартним вимірюванням її результату позначається як



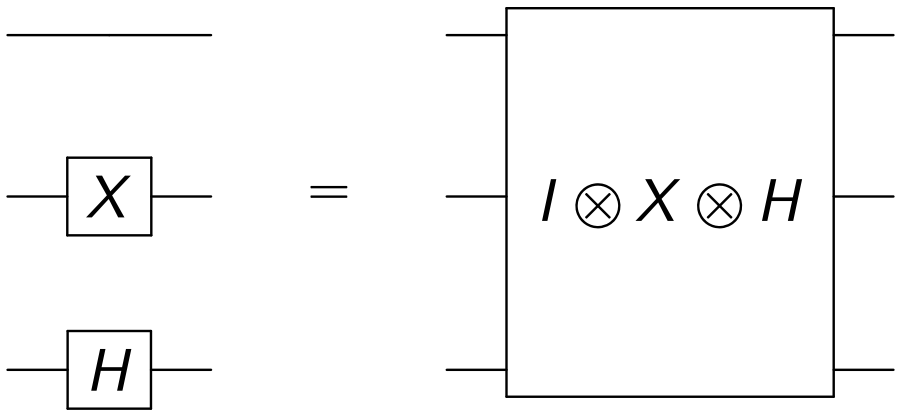
Зазвичай, схеми розглядаються для вхідного стану $|\phi\rangle = |00\ldots0\rangle$.

Квантові схеми

Послідовність унітарних операцій $U_1, U_2, \ldots, U_k$ відповідає добутку $U = U_k U_{k-1} \cdots U_1$. Але на схемі порядок відображення U_i залишається прямим.
Наприклад, $|0000\rangle \longrightarrow U_3 U_2 U_1 |0000\rangle$ відображається як



Якщо унітарна операція діє нетривіальним чином лише на частині кубітів, то її малюють лише на них. Наприклад, $I \otimes X \otimes H = I \otimes X \otimes I \cdot I \otimes I \otimes H$, що діє на трьох кубітах, відображається як



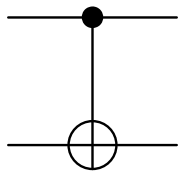
Однокубітні гейти позначають тими ж символами на схемі. Але для контрольованих операцій вводять спрощене відображення.

Контрольовані операції

Найпростішою контрольованою операцією є CNOT (також її позначають CX). Вона переставляє елементи стандартного базису за правилом

$$\mathrm{CNOT}\,|b_0 b_1\rangle = |b_0\rangle|b_1 \oplus b_0\rangle = (I \otimes X^{b_0})\,|b_0 b_1\rangle,$$

по всіх значеннях бітів b_0, b_1.
На квантовій схемі її позначають як



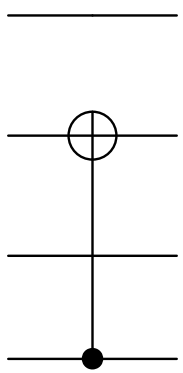
При цьому 0-й кубіт називають кубітом *контролю*, а 1-й кубіт *ціллю (таргетом)*.

Контрольовані операції

По аналогії, для n кубітів можна ввести операцію $\mathrm{CNOT}_{k,l}$, яка нетривіально діє лише на парі кубітів k, l за правилом

$$\mathrm{CNOT}_{k,l} \left| b_0 b_1 \dots b_k \dots b_l \dots b_{n-1} \right\rangle = \left| b_0 b_1 \dots b_k \dots b_l' \dots b_{n-1} \right\rangle,$$

де $b_l' = b_l \oplus b_k$. Наприклад, $\mathrm{CNOT}_{3,1}$ на схемі із чотирьох кубітів буде відображатися як



Контроль по значенню 0

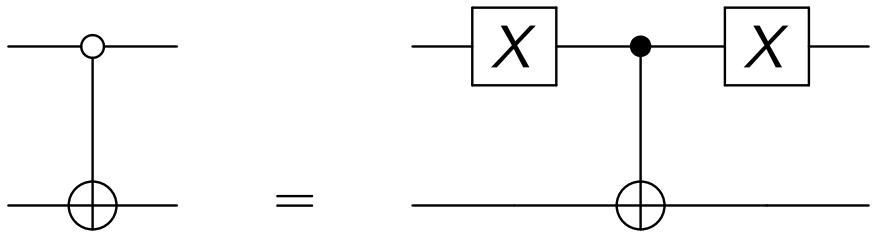
Можна ввести операцію $\mathrm{CNOT}[0]$, яка подібна до CNOT, але значення цілі змінюється на протилежне тільки якщо значення контролю було 0, тобто

$$|00\rangle \longrightarrow |01\rangle,\ |01\rangle \longrightarrow |00\rangle,\ |10\rangle \longrightarrow |10\rangle,\ |11\rangle \longrightarrow |11\rangle,$$

або ж

$$\mathrm{CNOT}\,|b_0 b_1\rangle = |b_0\rangle|b_1 \oplus b_0 \oplus 1\rangle = (I \otimes X^{1+b_0})\,|b_0 b_1\rangle.$$

На схемах вона позначається як



Не важко бачити, що $\mathrm{CNOT}[0] = X \otimes I \cdot \mathrm{CNOT} \cdot X \otimes I$.
Аналогічно можна визначити $\mathrm{CNOT}_{k,l}[0]$.

Контроль довільних гейтів

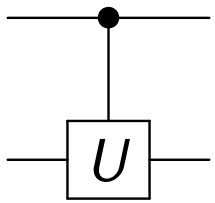
Для довільної однокубітної унітарної операції U можна визначити її контрольовану версію $\mathrm{C}(U)$, яка діє за правилом

$$|00\rangle \longrightarrow |00\rangle,\ |01\rangle \longrightarrow |01\rangle,\ |10\rangle \longrightarrow |1\rangle\, U\, |0\rangle,\ |11\rangle \longrightarrow |1\rangle\, U\, |1\rangle,$$

або ж

$$\mathrm{C}(U)\, |b_0 b_1\rangle = (I \otimes U^{b_0})\, |b_0 b_1\rangle.$$

Схематично її позначають як



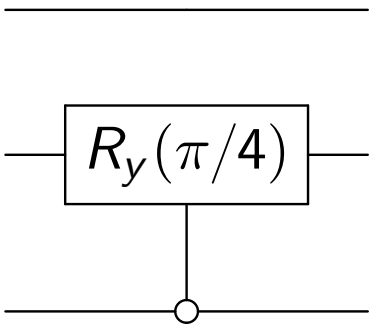
Очевидно, що $\mathrm{CNOT} = \mathrm{CX} = \mathrm{C}(X)$.

Контроль довільних гейтів

По аналогії до попереднього визначаються та позначаються на схемах операції $\mathrm{C}_{k,l}(U)$ та $\mathrm{C}_{k,l}(U)[0]$.
Наприклад, $\mathrm{C}_{2,1}(R_y(\pi/4))[0]$ діє за правилом

$$\mathrm{C}_{2,1}(R_y(\pi/4))[0] \cdot |b_0 b_1 b_2\rangle = |b_0\rangle (R_y(\pi/4))^{1+b_2} |b_1\rangle |b_2\rangle$$

по всім значенням b_0, b_1, b_2 і позначається як

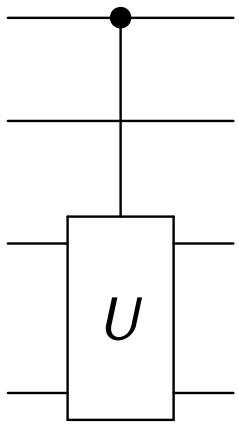


Контроль багато-кубітних гейтів

Контрольовану версію також можна визначити і для унітарної операції U, яка діє на кількох кубітах. Наприклад, нехай U це двохкубітний унітарний гейт. Тоді $\mathrm{C}_{0,(2,3)}(U)$ це операція на чотирьох кубітах, де 0-й це кубіт контролю, а $(2,3)$ це номери цільових кубітів (на яких діє U), що визначається правилом

$$|0b_1b_2b_3\rangle \longrightarrow |0b_1b_2b_3\rangle, \ |1b_1b_2b_3\rangle \longrightarrow |1b_1\rangle\, U\, |b_2b_3\rangle,$$

для всіх можливих значень бітів b_1, b_2, b_3. Даний приклад позначається як

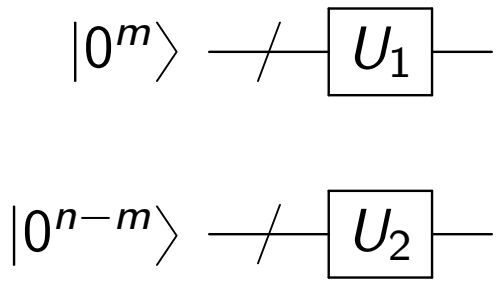


Регістри з кубітів

Регістр з кубітів це піднабір кубітів із усіх доступних, що згруповані для зручності.

Наприклад, n кубітів можна розбити на два регістри з m та $n - m$ кубітів.

На схемі регістр інколи зображають однією (перекресленою) лінією:

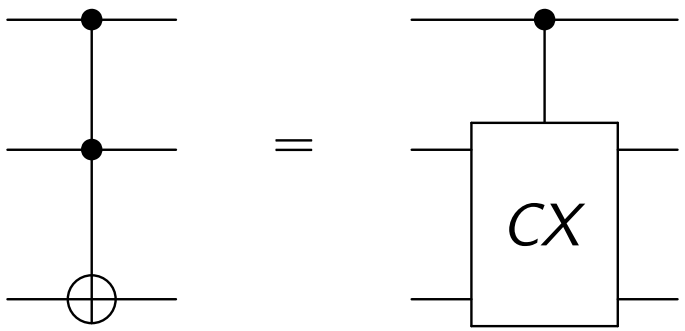


Мультиконтрольовані операції

Мультиконтрольовані це операції в яких для контролю береться не один кубіт, а декілька. Найпростішим прикладом є операція CCNOT (або ж CCX). Вона діє за правилом

$$\mathrm{CCNOT}\,|b_0 b_1 b_2\rangle = |b_0 b_1 b_2'\rangle = |b_0 b_1\rangle X^{b_0 \cdot b_1} |b_2\rangle,$$

де $b_2' = b_2 \oplus (b_0 \cdot b_1)$, тобто $b_2' = b_2 \oplus 1$ якщо $b_0 = 1, b_1 = 1$, та $b_2' = b_2$ у всіх інших випадках. На схемі її позначають як



Також її називають квантовим гейтом Тоффолі.
Не важко бачити, що $\mathrm{CCNOT} = \mathrm{C}(\mathrm{CNOT}) = \mathrm{C}(\mathrm{C}(X))$.

Загальні мультиконтрольовані операції

По аналогії до попереднього, можна розглядати мультикубітний контроль будь-якої операції, причому контроль не тільки по значенням 1 бітів.

Загалом, через $\mathrm{C}_{[c_1,c_2,\ldots,c_k],(t_1,t_2,\ldots,t_l)}(U)[a_1 a_2 \ldots a_k]$ будемо позначати операцію, де c_i це індекси кубітів контролю, a_i це відповідні значення бітів по яким іде контроль, t_j це індекси кубітів, на яких діє операція U.

В цих позначеннях $\mathrm{CCNOT} = \mathrm{C}_{[0,1],2}(X) = \mathrm{C}_{[0,1],2}(X)[11]$.

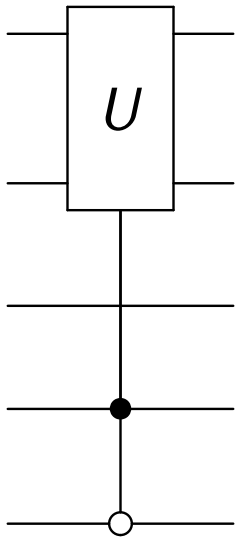
Загальні мультиконтрольовані операції

Наприклад, нехай U це двохкубітна операція. Тоді операція $\mathrm{C}_{[3,4],(0,1)}(U)[10]$ на п'яти кубітах діє за правилом

$$|b_0 b_1 b_2 10\rangle \longrightarrow \big(U\,|b_0 b_1\rangle\big)\,|b_2\rangle|10\rangle\,,$$

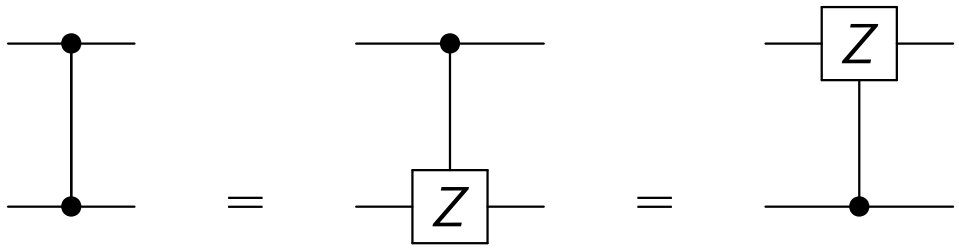
$$|b_0 b_1 b_2 b_3 b_4\rangle \longrightarrow |b_0 b_1 b_2 b_3 b_4\rangle\,, \quad b_3 b_4 \neq 10,$$

для всіх можливих значень бітів b_i. Вона позначається на схемі як

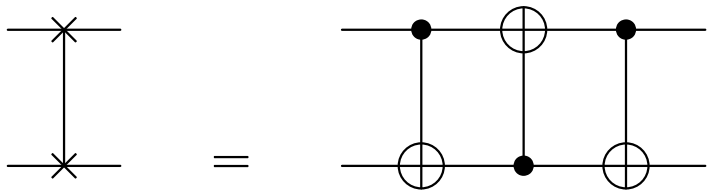


Інші позначення

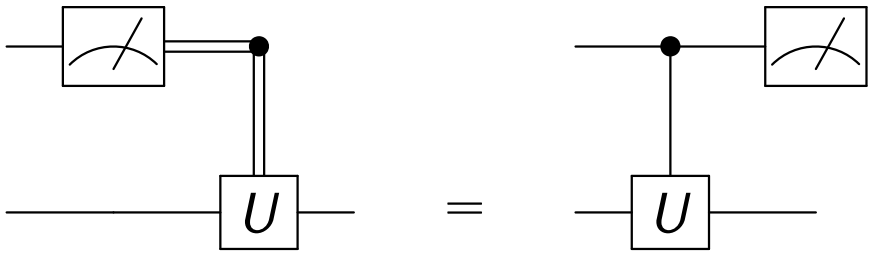
Операцію $\mathrm{CZ} = \mathrm{C}(Z) = \mathrm{C}_{1,0}(Z) = \mathrm{C}_{0,1}(Z)$ позначають як



Операцію SWAP позначають як



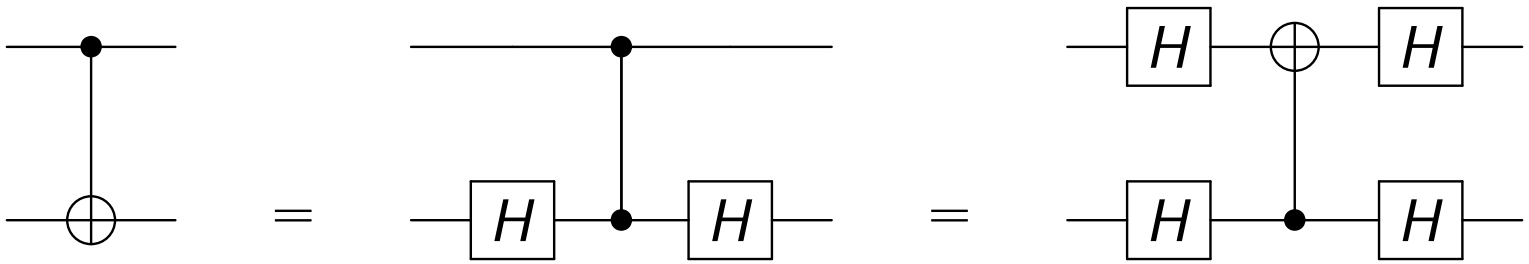
Класичний контроль позначається



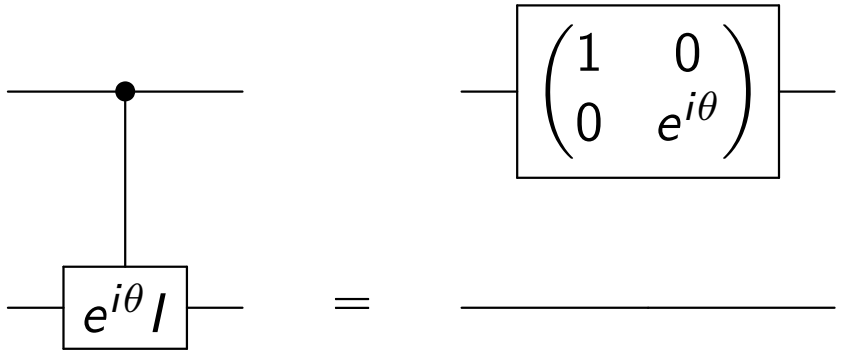
(тотожність має назву *принцип відкладеного вимірювання*)

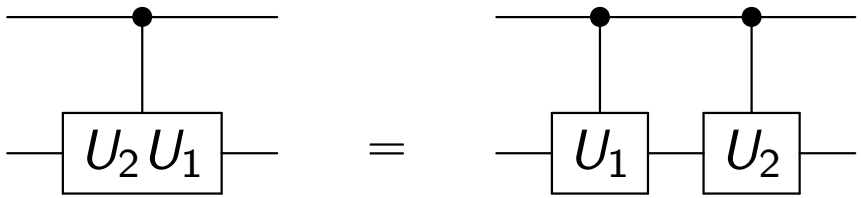
Корисні тотожності

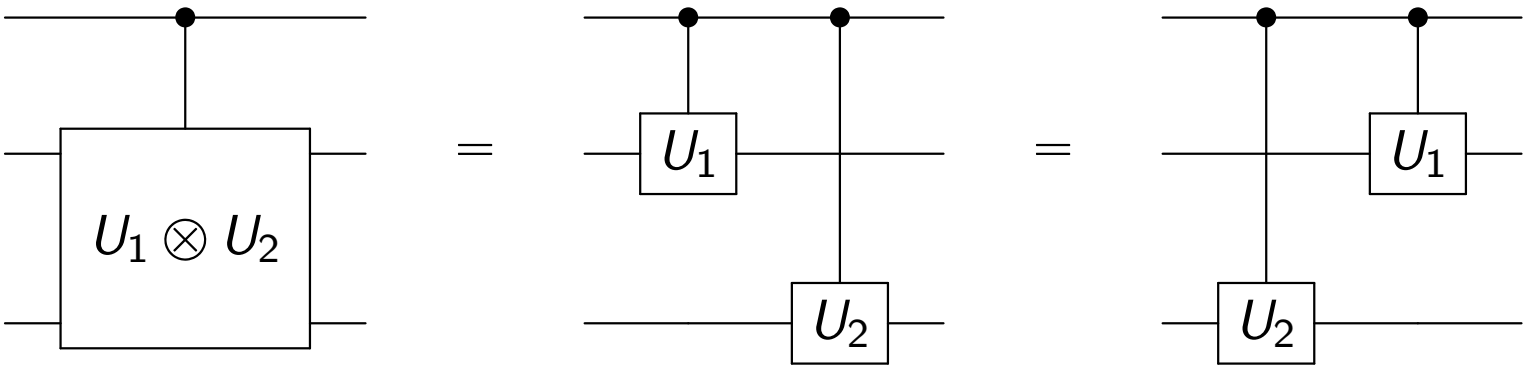
$$HXH = Z, \quad HZH = X.$$



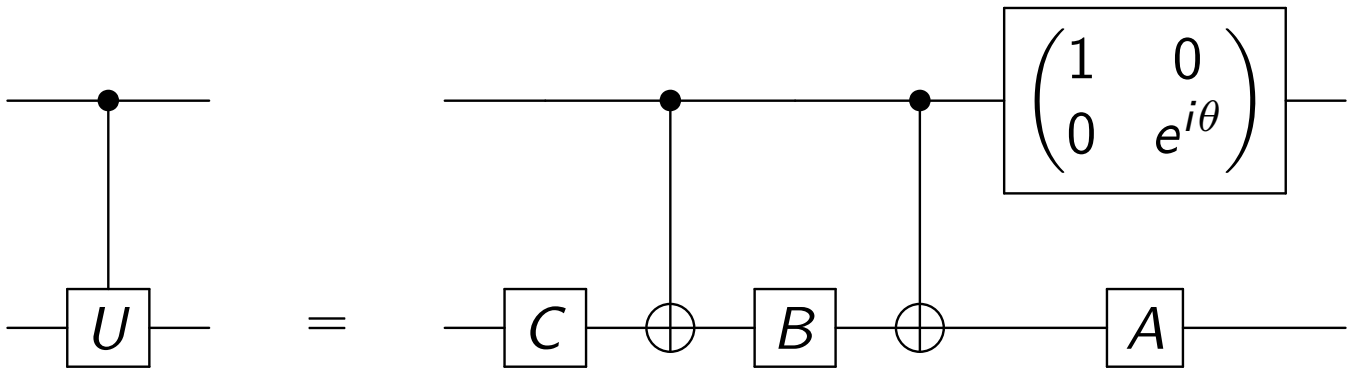
Корисні тотожності







Корисні тотожності



якщо $U = e^{i\theta}AXBXC$, $ABC = I$. Такий розклад можна отримати для довільної однокубітної U:

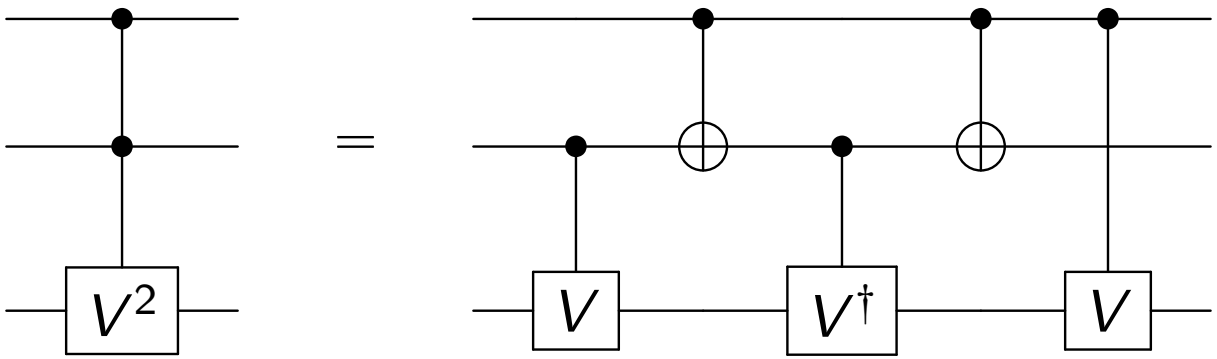
$$U = e^{i\theta}R_z(\beta)R_y(\gamma)R_z(\delta),$$

якщо взяти

$$A = R_z(\beta)R_y(\gamma/2),\ B = R_y(-\gamma/2)R_z(-(\delta+\beta)/2),\ C = R_z((\delta-\beta)/2).$$

Корисні тотожності

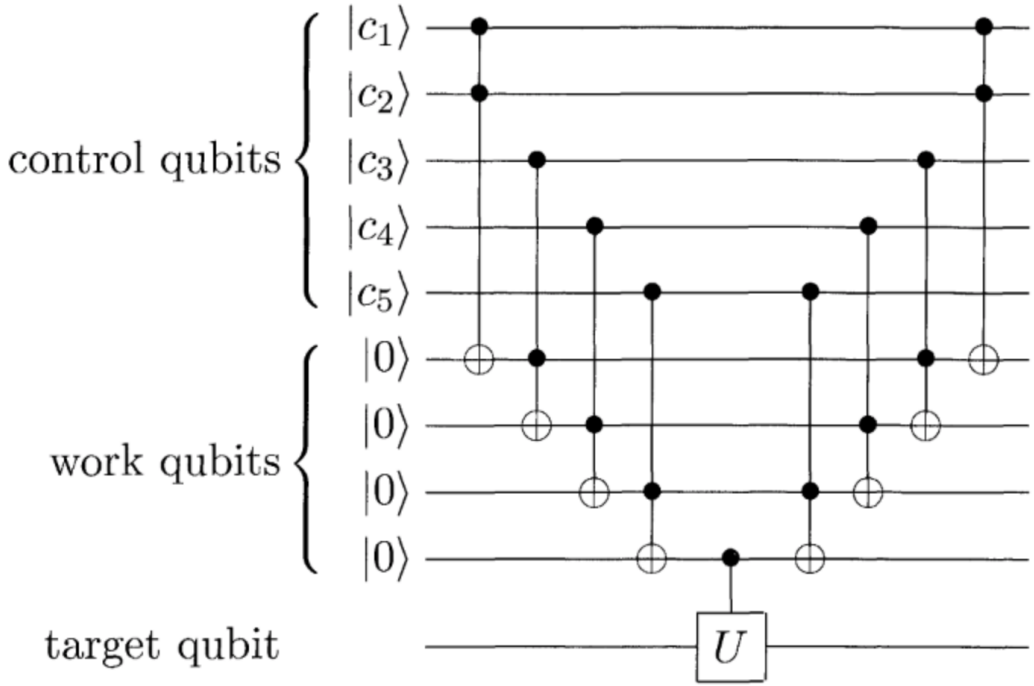
Для будь-якого однокубітного гейту V



Зокрема, можна виразити Тоффолі якщо взяти $V = e^{i\pi/4} R_x(\pi/2)$.

Корисні тотожності

Мультиконтрольовану операцію можно тотожнім чином реалізувати через 2-х контрольовані операції, але з використанням додаткових кубітів. Наприклад, схему для $C_{[0,1,2,3,4],5}(U)[11111]$ можна реалізувати як



Загалом виходить, що будь-яку мультиконтрольовану операцію можна реалізувати як послідовність CNOT та однокубітних операцій.

Обертовні обчислення

У випадку класичної логіки ми оперуємо функціями $f : \mathbf{B^n} \to \mathbf{B^m}$, які, взагалі кажучи, не є обертовними.

В квантових обчисленнях якщо унітарна U є перестановкою стандартного базису з n кубітів, то їй відповідає функція $f : \mathbf{B^n} \to \mathbf{B^n}$, яка є обертовною.

Як тоді бути з необертовними функціями?

Стандартний прийом полягає у наступному.
Для будь-якої функції $f : \mathbf{B^n} \to \mathbf{B^m}$ можна розглядати її канонічне розширення $\pi_f : \mathbf{B^n} \times \mathbf{B^m} \to \mathbf{B^n} \times \mathbf{B^m}$, яке діє за правилом

$$\pi_f(x, y) = (x, y \oplus f(x)).$$

Зрозуміло, що $\pi_f(x, 0^m) = (x, f(x))$. При цьому $(\pi_f \circ \pi_f)(x, y) = \pi_f(x, y \oplus f(x)) = (x, y \oplus f(x) \oplus f(x)) = (x, y)$.
Звідси $\pi_f^{-1} = \pi_f$, а отже π_f є обертовною.
Відповідна унітарна операція U_f діє як перестановка стандартного базису $n + m$ кубітів:

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle,$$

по всіх $x \in \mathbf{B^n}$, $y \in \mathbf{B^m}$.

Наприклад, нехай $f(a_1, a_2) = a_1 \text{ AND } a_2 = a_1 \cdot a_2$, $f : \mathbf{B}^2 \to \mathbf{B}$. Тоді

$$U_f \left|a_1 a_2\right\rangle \left|b\right\rangle = \left|a_1 a_2\right\rangle \left|b \oplus a_1 \cdot a_2\right\rangle.$$

Неважко бачити, що $U_f = \mathrm{CCNOT}$, тобто гейт Тоффолі.

Подібним чином через Тоффолі можна закодувати OR. Для XOR достатньо взяти $f_{\mathrm{XOR}}(a, b) = (a, b \oplus a)$, що на кубітах буде відповідати операції CNOT.

Звідси випливає, що якщо є класична логічна схема, в якій k гейтів типу $\mathrm{NOT}, \mathrm{AND}, \mathrm{OR}, \mathrm{XOR}$, то є відповідна квантова схема, в якій k гейтів типу $\mathrm{X}, \mathrm{CNOT}, \mathrm{CCNOT}$. Тобто складність квантової схеми є подібною.

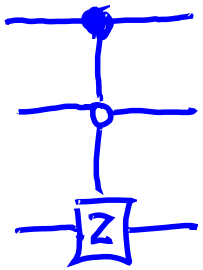
Єдиною проблемою є операції розгалуження (клонування) та нехтування (знищення). Тобто функції вигляду $f(b) = (b, b, \ldots, b)$, $f : \mathbf{B} \to \mathbf{B^n}$ та $g(b_1, b_2, \ldots, b_n) = b_i$, $g : \mathbf{B^n} \to \mathbf{B}$. Такі гейти по суті є безкоштовними в класичному випадку, але в обертовному (квантовому) випадку вимагають використання n кубітів від самого початку.
Але існують методи, як обертовні схеми робити максимально компактними. Загалом, вірне наступне твердження

Твердження
Класична логічна схема з t примітивних гейтів та s бітів (вхідні + вихідні) має обертовний аналог, що складається лише з $O(t^{1+\epsilon})$ примітивних обертовних гейтів та $O(s \log(t))$ бітів.

Завдання

31. Порахувати результат дії $\mathrm{C}_{1,0}(Y)$ на стані $|0\rangle|+\rangle$. Схема?

32. И задать схемою



$U|1\rangle|f\rangle|1\rangle = ?$

33. $f(a_1, a_2) = \neg(a_1 \text{ OR } a_2)$, $U_f\ 1 \to |00\rangle = ?$

$f: B^2 \to B \Rightarrow$ канон. розшир. $\Rightarrow U_f$