Квантовый логический элемент (вентиль) — унитарное преобразование в пространстве состояний квантового регистра. Если регистр состоит из N кубитов, то размерность пространства состояний равна 2^N, так что матрица унитарного преобразования имеет размерность $2^N \times 2^N$. Существует несколько равносильных определений унитарности, степень полезности которых зависит от решаемой задачи. Оператор U называется унитарным тогда и только тогда, когда

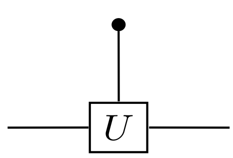
- Сопряженный оператор равен обратному, т.е. $U^\dagger = U^{-1}$;
- строки (столбцы) матрицы оператора образуют ортонормированное множество векторов, т.е. $\sum_i U_{ij}U_{ik} = \sum_i U_{ji}U_{ki} = \delta_{jk}$;
- оператор сохраняет внутреннее произведение, т.е. $\langle\phi|U^\dagger U|\psi\rangle = \langle\phi|\psi\rangle$.

Собственные значения унитарного оператора имеют вид $e^{i\alpha_n}$, $n = 1, \ldots, 2^N$. Если унитарный оператор одновременно является эрмитовым, то собственные значения равны ± 1. Среди унитарных операторов выделяют класс *специальных унитарных* операторов, у которых $\det U = +1$. Специальные унитарные операторы соответствуют вращению в гильбертовом пространстве состояний.

Управляемые преобразования

Унитарное преобразование, совершаемое в пространстве состояний квантового регистра над одним из кубитов, называется управляемым или условным, если его вид зависит от состояния остальных (одного или нескольких) кубитов. Кубит, над которым совершается преобразование называется управляемым, а кубиты, от состояния которых зависит вид преобразования, называются управляющими.

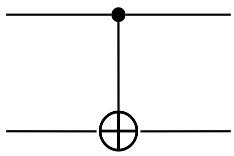
Наибольшее практическое значение имеют двухкубитовые вентили, когда один кубит является управляемым, а второй — управляющим. Графическое изображение элемента «Управляемое U», который, обычно, обозначается через CU, и структура его матрицы (в вычислительном базисе, упорядоченном по алфавиту) выглядят следующим образом:



$$CU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{bmatrix}$$

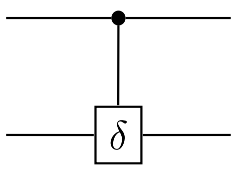
Здесь на схеме верхний провод соответствует управляющему кубиту, а нижний — управляемому, что отмечено черным кружком на верхнем проводе и вертикальной соединяющей линией. Черный кружок означает, что преобразование U совершается только тогда, когда управляющий кубит находится в состоянии $|1\rangle$.

Вместо оператора U может стоять любой однокубитовый оператор. В частности, для оператора *управляемого отрицания* получаем:



$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

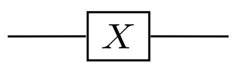
а для элемента *управляемого изменения фазы*:



$$CP(\delta) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\delta} \end{bmatrix}$$

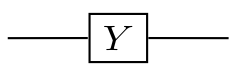
Существует несколько однокубитовых унитарных операторов, имеющих особое значение в квантовой информатике. Ниже приводятся их названия, условные обозначения на квантовых схемах и матрицы.

Элемент Паули X



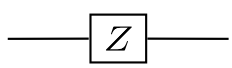
$$X = iR_x(\pi) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Элемент Паули Y



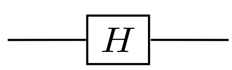
$$Y = iR_y(\pi) = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

Элемент Паули Z



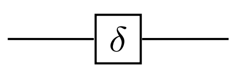
$$Z = iR_z(\pi) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Элемент Адамара



$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Элемент
изменения фазы



$$P(\delta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix} = e^{i\delta/2} R_z(\delta)$$