Disprove of intuition

Есть интуиция, что можно сделать оператор тоффоли гораздо быстрее с помощью необратимой операции reset. Операция reset работает на кубите – как измерение этого кубита относительно стандартного базиса и в зависимости от результата, либо применение к нему X если он оказался в состоянии 1, либо оставлении его в состоянии 0. Предполагаем, что операция reset работает идеально.

Объяснение интуиции.

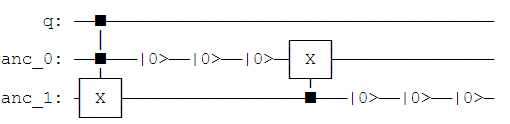
Пусть мы хотим реализовать оператор тоффоли на n кубитах пронумерованных q\_i. Идея реализации: пройдёмся по каждому кубиту и будем запоминать, если у нас уже был хотя бы один ноль. Если был – тогда в дополнительном кубите всегда будет записан ноль, если не было, тогда в дополнительном кубите должен быть один.

Используем два дополнительных кубита. Пусть кубит anc0 – хранит в себе 1, если все предыдущие кубиты в состоянии 1, и 0 если хотя бы один из них ноль. Кубит anc1 будет дополнительным и всегда будет хранить нулевое значение перед операцией. Изначально anc0 в состоянии 1.

Таким образом на шаге номер i мы хотим реализовать операцию на трёх кубит. Anc0, anc1, q\_i. Изначально anc1 в состоянии ноль. Он и должен остаться в состоянии ноль. Однако для значений anc0 q\_i таблица переходов нужна необратимая:

|  |  |
| --- | --- |
| До |anc0 q\_i> | После |anc0 q\_i> |
| |0 0> | |0 0> |
| |0 1> | |0 1> |
| |1 0> | |0 0> |
| |1 1> | |1 1> |

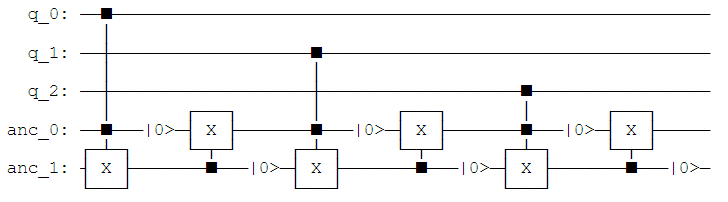
Пример схемы, которая может реализовать такую операцию с помощью операции reset:



(Здесь мы применяем трижды оператор ресет для точности)

Однако, если последовательно применить такую операцию для всех q\_i , то не для всякого чистого состояния на выходе будет результат как от оператора тоффоли.

Пример для трёх кубит:



Такая схема не будет давать ожидаемый результат например для состояния:

|000> + |111>

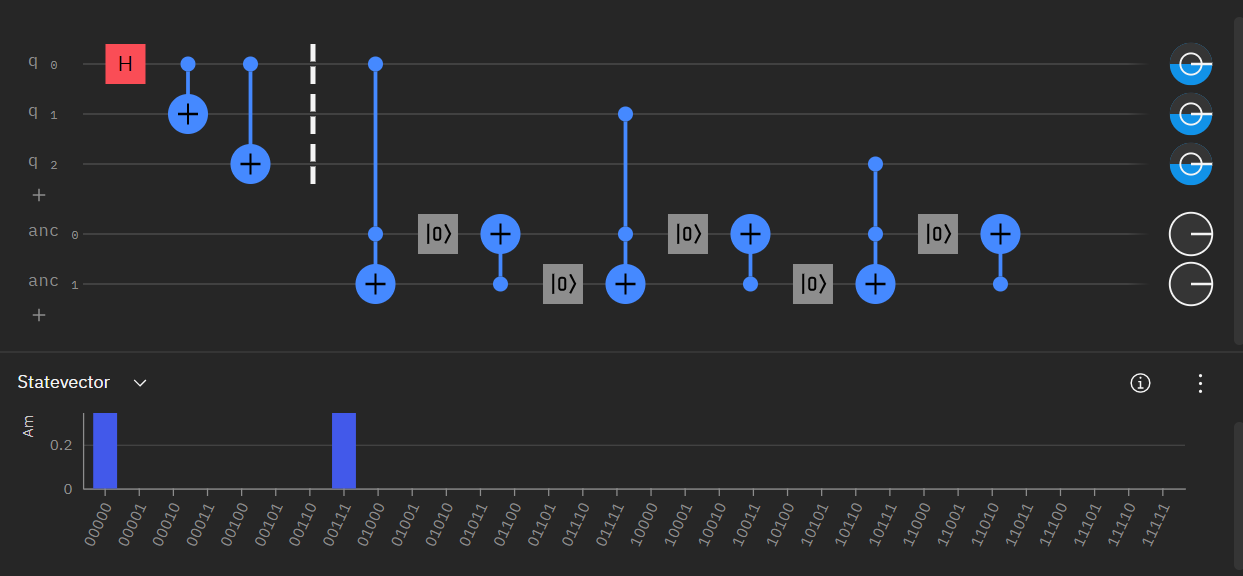
Такая схема не будет давать правильный результат ни для какого состояния, x =

Где будут наблюдаться не нулевые коэффициенты хотя бы у двух состояний для, которых показания anc0 ожидаются различными.

Пусть эти два состояния – |w1> и |w2>.

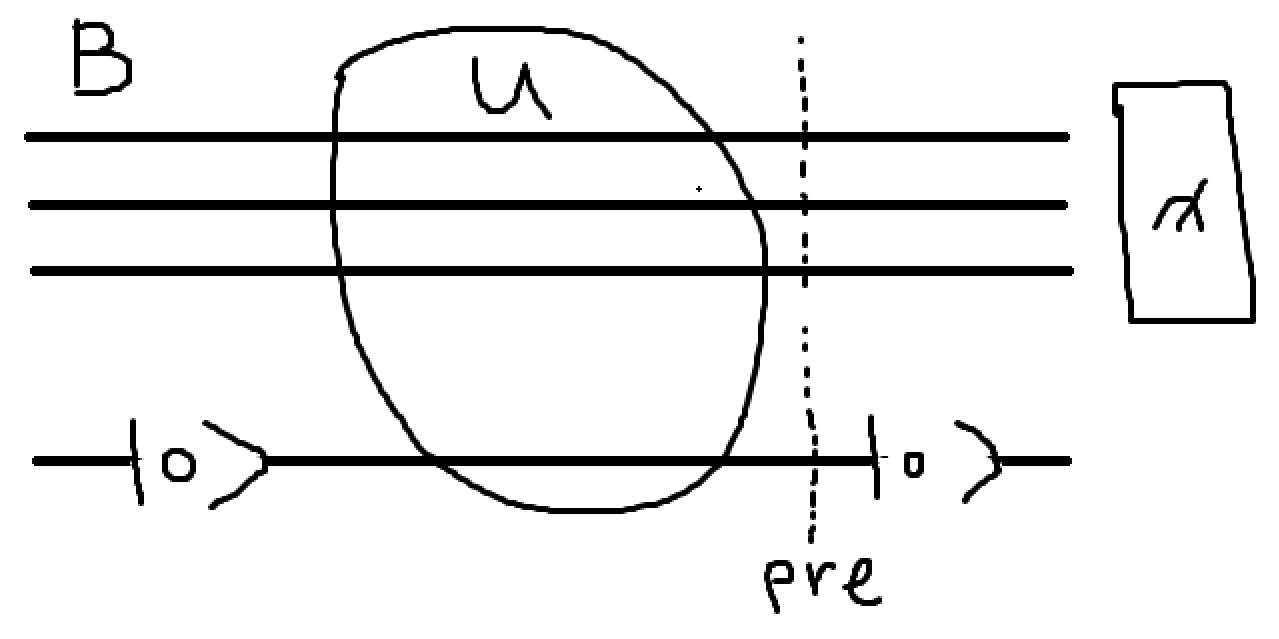
Тогда – найдётся такое i, для которого после применения операции у системы будет состояние в виде суммы (|w1>|0> + |w2>|1> + …)|0>. Тогда при применении следующей операции – при ресете anc1 произойдёт измерение и состояние из запутанного перейдёт либо в (|w1>|0> + …)|0> либо в (|w2>|1> + …)|0>. (могут змениться коэффициенты при базовых состояниях). Однако в первом случае у базисного вектора |w2>|1> будет коэффициент 0, а во втором у базисного вектора |w1>|0> будет коэффициент 0. Такое поведение наша операция не предусматривает и запутанность будет частично потеряна в следствии измерения. Так что, к сожалению, искусственно привнести необратимость в запутанное состоянии – не получится. Однако измерения для ускорения некоторых операций использовать возможно.

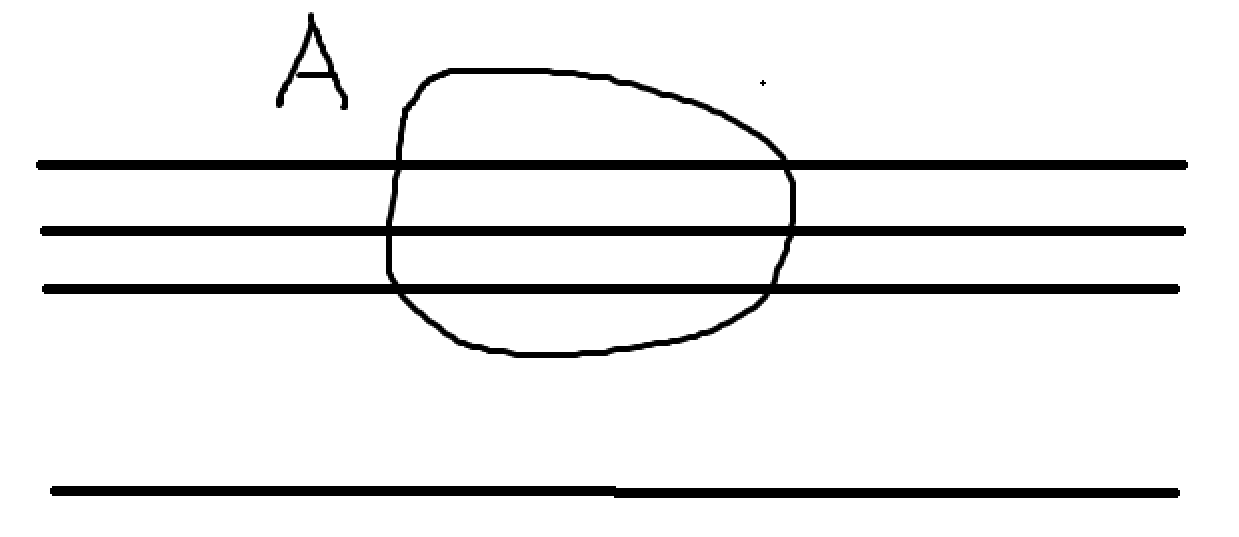
Связь между понятиями необратимости, запутанности, невозможности измерить (подсмотреть внутрь) вероятно можно понять из курса квантовой механики.



21.05

Задачи

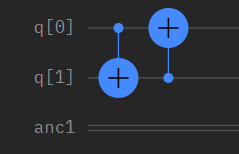
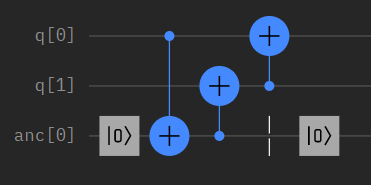




Если A|i> = B|i> для любого базисного вектора i:

1. При каких условиях A|phi> = B|phi>
2. При каких условиях при измерении основных кубит получатся одинаковые вероятности результатов.

Пример 1.

A:  B: 

Заметим, что на базисных векторах они дают одинаковые значения. Однако посчитаем результат операторов на состоянии (|00> + |11>)

A(|00> + |11>) = ((|00> + |10>))

B(|00> + |11>) -> (|000> + |110>) -> (|000> + |111>) -> (|000> + |101>) -> (|000> + |101>) -> [применение |0> ] -> с вероятностью ½ получаем |000> а с вероятностью ½ |101>.

Получили смешанное состояние, а хотели чистое.

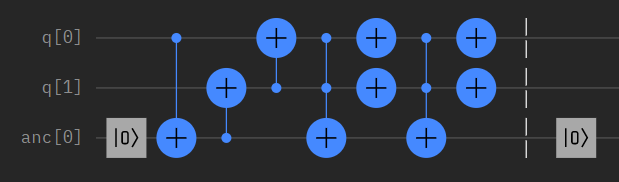
Что бы на выходе получить чистое состояние достаточное и необходимое условие:

B\_pre|phi> = |sigma> (a|0> + b|1>)

Доказательство в приложении 1

Пример 2.

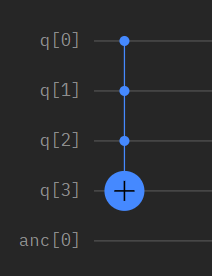
А такое же. B:

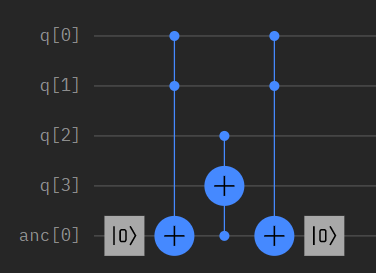


Здесь мы искусственно возвращаем anc на место. Тогда для любого чистого состояние phi

A|phi> = B|phi>

Однако здесь не наблюдается ускорение. Попробуем привести пример с ускорением. Такой пример нам всем уже очень хорошо известен.

A

B

Тут есть ускорение. Однако тут второй оператор ресет ничего не делает и схема с тем же успехом работала бы и без него. Давайте попытаемся построить пример, где он был бы нужен. Для этого хотим, что бы B\_pre|phi>|0> = |sigma>(a|0> + b|1>)

Причём, так что бы нам заранее не были известны a b. Иначе мы бы смогли и без измерения подкрутить последний кубит, поставив его на место |0>. Таким образом хотим, что бы a b зависили от |phi> и были бы разными для каких-то phi.

Допустим у нас такое получилось. Посмотрим как действует B\_pre на базисных векторах.

Пусть B\_pre|i> = |phi\_i>(a\_i|0> + b\_i|0>)

Первый случай) Пусть a\_i, b\_i ≠ a\_j, b\_j для каких-то i j

Тогда B\_pre(|i> + |j>) не может быть представлено в виде |sigma>(a|0> + b|1>)

Второй случай) Пусть a\_i, b\_i = a\_j, b\_j для любых i j

Пусть |phi1> = ∑c\_i|i>

Тогда B\_pre(|phi1>) = ∑c\_i\*B\_pre(|i>) = ∑c\_i\*(|sigma\_i>(a|0> + b|1>)) = (∑c\_i\*|sigma\_i>)(a|0> + b|1>). Заметим, что здесь коэффициенты a b не меняются от phi, а значит такого примера не найдётся!

…………………Теперь разберём второй вопрос.

Оказывается, так выполняется всегда. Доказательство:

If A|i> = B|i> => B\_pre|i> = |phi\_i>(a\_i|0> + b\_i|1>) a\_i^2 + b\_i^2 = 1

( Пусть |phi\_i> = ∑c\_i|i> )

Пусть так же |phi’> = ∑c’\_i|i>

Тогда A|phi’> = ∑c’\_i|phi\_i>

B\_pre|phi’> = ∑(c’\_i|phi\_i>(a\_i|0> + b\_i|1>)) = ∑(c’\_i(∑c\_j|j> )(a\_i|0> + b\_i|1>)) =

Можем вынести внутреннюю сумму по j наружу и поменять её местами с суммой i

= ∑∑(c’\_i\*c\_j|j> )(a\_i|0> + b\_i|1>))

Посмотрим на вероятность получение результата j при измерении сначала дополнительного кубита, а затем всех основных.

= ∑∑c’\_i\*c\_j|j> (a\_i|0> + b\_i|1>)) = ∑\_j: c\_j|j>(∑\_i: c’\_i(a\_i|0> + b\_i|1>))

При измерении

P(|j>) = (c\_j)^2 \* (∑\_i: (c’\_i\*a\_i)^2) + (c\_j)^2 \* (∑\_i: (c’\_i\*b\_i)^2) = (c\_j)^2 \* (∑\_i: (c’\_i)^2) = (c\_j^2) что и требовалось показать!

…………………………..

Приложение 1.

От противного. Пусть pre состояние не представимо, как |sigma> (a|0> + b|1>)

Тогда можно его записать так:

∑c\_i|i> (a\_i|0> + b\_i|1>), где пусть a\_m1 ≠ a\_m2 и хотя бы один из этих коэфф-ов не ноль.

C\_m1(a\_m1|0> + …) + … + C\_m2(a\_m2|0> + …)

При ресете дополнительного кубита мы с не нулевой вероятностью перейдём в состояние

C\_m1\*a\_m1\*|m1>|0> + … + C\_m2\*a\_m2\*|m2>|0>

Но заметим, что C\_m1\*a\_m1/ C\_m2\*a\_m2 ≠ C\_m1 / C\_m2, но если B|phi> = A|phi> =>

(C\_m1\*a\_m1\*|m1>|0> + … + C\_m2\*a\_m2\*|m2>|0>) = (C\_m1m1>|0> + … + C\_m2m2>|0>)

Противоречие!