УДК 004.056.55

ПОВЫШЕНИЕ БЫСТРОДЕЙСТВИЯ КВАНТОВОГО АЛГОРИТМА ГРОВЕРА ПУТЕМ ПРИМЕНЕНИЯ ИНВЕРСИИ ВОКРУГ СРЕДНЕГО

Кравченко В.О. аспирант второго года обучения кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону

Маслов И.О. студент 5-го курса кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону

Бачило А.О. студент 5-го курса кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону

Пилипенко И.А. аспирант второго года обучения кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону

Научный руководитель – Черкесова Л.В. – доцент, д.ф.-м.н., и профессор кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону

Введение Алгоритм Гровера - алгоритм квантового поиска, время выполнения которого намного быстрее классических. Он не предназначен для нахождения элемента в базе данных, его целью является поиск по входам функции, чтобы проверить, возвращает ли функция значение «true» для определенных входных данных. Это полезный метод в случае, если функция неизвестна или чрезвычайно сложна, и мы хотим найти, для каких входных значений функция возвращает истину или дает правильный вектор решения уравнения. На квантовом компьютере мы можем выразить функцию как действительный набор квантовых логических элементов, составляющих оракул (непреложная истина) и использовать алгоритм поиска Гровера, чтобы найти правильный вход с очень высокой точностью с квадратичным ускорением.

Цель работы. Целью работы являлось создание практической реализации алгоритма Гровера на языке программирования Python, со временем выполнения порядка квадратного корня из времени работы классического алгоритма неструктурированного поиска. Для этого были использованы ресурсы сервиса «Riggeti Forest», а сама реализация включает инверсию относительно среднего.

Базовые положения исследования. Во время выполнения алгоритма Гровера состояние системы устанавливается в виде суперпозиции всех возможных входных данных, и затем вероятность нахождения искомого входного сигнала увеличивается на каждой итерации алгоритма. Далее следует часть алгоритма, которая будет повторяться около $\frac{\pi}{4}\sqrt{2^n}$раз, где n-длина искомой строки. Два шага будут включены в этот цикл:

1. Применение квантового оракула,
2. Инверсия вокруг среднего.

Квантового оракула недостаточно, чтобы распознать искомый вход, потому что знак амплитуды не влияет на вероятность измерения. Необходимо искать дополнительные квантовые ворота, которые увеличивают абсолютное значение амплитуды для искомого состояния. Ответ приходит с инверсией вокруг среднего (также называемой диффузионным оператором).

Промежуточные результаты. У искомой строки длиной 2 символа амплитуда вероятности равна одной итерации. Это означает, что когда вы измеряете кубиты, вы всегда получите искомую, однако это определено не является общим случаем для более длинных строк (когда число кубитов больше двух).

Если попытаться использовать алгоритм для поиска более длинной строки, например, длинной семь символов, то вероятность определения правильного ответа после девяти итераций составляет около 99,6%. Это одно из различий между классическим и квантовым компьютером. Многие квантовые алгоритмы возвращают правильный ответ с некоторой

вероятностью, тогда как классические компьютеры уверены в результатах вычислений (при условии, что шума нет). Это происходит независимо от квантового шума, то есть неопределенность результатов является неотъемлемым свойством этого квантового алгоритма. Чтобы быть почти на 100% уверенными в ответах от квантовых компьютеров, нужно выполнить измерение несколько раз. Тем не менее, повторение алгоритма несколько раз не оказывает существенного влияния на квадратичное ускорение при больших значений длины.

Вывод. Теоретически алгоритм обеспечивает квадратичное ускорение по сравнению с классическими компьютерами. Это еще не экспоненциальное ускорение, однако и оно очень существенно. Квантовый параллелизм алгоритма поиска Гровера основывается на одновременном изменении амплитуд всех входов. Это сделано благодаря суперпозиции состояний, которая является чисто квантовой концепцией. Кроме того, поиск выполняется глобально, что указывает на значительное улучшение процедур оптимизации. С другой стороны, алгоритм Гровера чувствителен к количеству итераций. Чем больше итераций, тем меньше будет амплитуда правильного ответа, поэтому неправильный выбор этого параметра может помешать найти правильное решение. Кроме того, работа алгоритма ограничена в случае введения шума в квантовую систему, которая реальна в современных квантовых компьютерах.