Simulation and Visualization of the Bernstein-Vazirani Quantum Protocol (bvviz)

April 19, 2023

Tommy Chu
chutommy@fit.cvut.cz
FIT CTU

1 Introduction

The Bernstein-Vazirani protocol is a quantum algorithm introduced in 1992, by computer scientists Ethan Bernstein and Umesh Vazirani [1]. It showed that there can be advantages in using a quantum computer as a computational tool for more complex problems than the Deutsch-Jozsa problem [2].

It has a potential use in classical cryptography [3] and quantum key distribution and communication [4]. Shor's protocol, one of the most popular quantum algorithms (prime factorization in $O(\log n)$), uses many properties of quantum circuits leveraged in this protocol.

1.1 Problem Statement

The Bernstein-Vazirani problem is a promise problem [5]. It involves a black-box function $f_s : \{0,1\}^n \to \{0,1\}$, which takes a bit string as input and returns either 0 or 1. The function guarantees to return the dot product between x and a secret string $s \in \{0,1\}^n$, modulo 2 [6]:

$$f_s(\{x_0, x_1, ..., x_{n-1}) = x \cdot s$$

$$x \cdot s \equiv x_0 s_0 \oplus x_1 s_1 \oplus ... \oplus x_{n-1} s_{n-1}$$

The objective is to determine the secret string s of the function f_s.

2 Solution

The project bvviz implements both classical and quantum solutions for the Bernstein-Vazirani algorithm. These solutions are compared in terms of the number of queries made to the oracle function f_s, computational time, accuracy, and overall complexity.

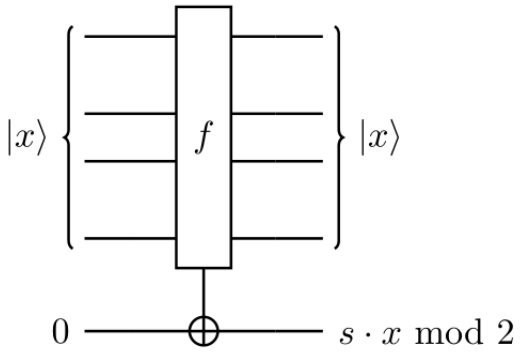

Figure 1: The reversible circuit of the Bernstein-Vazirani oracle (image source: Qiskit)

2.1 Classical algorithm

The implementation of the classical algorithm finds the secret string by evaluating the function $f_s(x)$ n times with the input values $x = 2^i = 1 \ll i$ for all $i \in \{0, 1, ..., n-1\}$. By querying the i^{th} bit, the i^{th} bit of the secret string (s_i) is determined.

The bvviz implementation of the classical algorithm is also the most efficient since no more than one bit of information can be revealed by a single query to the oracle. The complexity of the classical approach is $O(n)$

2.2 Quantum algorithm

On the other hand, bvviz's implementation of the quantum algorithm obtains the hidden secret string s with certainty* in a single query to the oracle function $f_s(x)$, resulting in a complexity of $O(1)$.

This is achieved by introducing input qubits $|0\rangle_n$ into an equal linear superposition of the 2^n basis states by applying n Hadamard gates.

An additional auxiliary qubit, carrying the output bit of information, is set to $|-\rangle$ using a single Hadamard and Pauli-X gate [7].

The state fed into the quantum oracle function f_s is

$$H^{\otimes n}|0\rangle \otimes HX|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^{n-1}} |x\rangle \otimes |-\rangle$$

The oracle function f_s flips each qubit q_i that satisfies $f_s(2^i) = 1$, which change the sign of these states. This is also known as phase kick-back [8].

Since all quantum gates are their own inverses, n Hadamard gates are applied to obtain the final result:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^{n-1}} (-1)^{s \cdot x} \longrightarrow^{H^{\otimes n}} |s\rangle$$

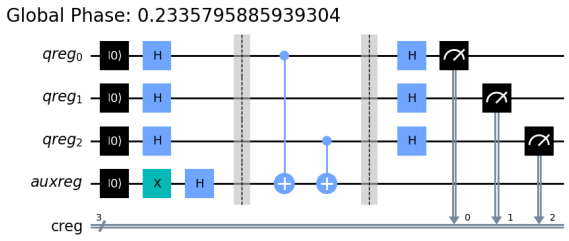

Figure 2: An implementation of the Bernstein-Vazirani protocol for a secret string 101

3 bvviz

bvviz is a web application that allows users to run and visualize quantum simulations of the Bernstein-Vazirani protocol.

The underlying problems of quantum technology are often misunderstood. This application guides users to understand both benefits and constraints of quantum computing.

3.1 Quantum simulation

Upon visiting the application, a preconfigured experiment is run by default. However, users have the freedom to customize the simulator device, including the backend system, number of shots, secret string, or their own noise and transpiler model.

This allows users to gain full control over the quantum hardware that is being simulated to run the Bernstein-Vazirani experiment.

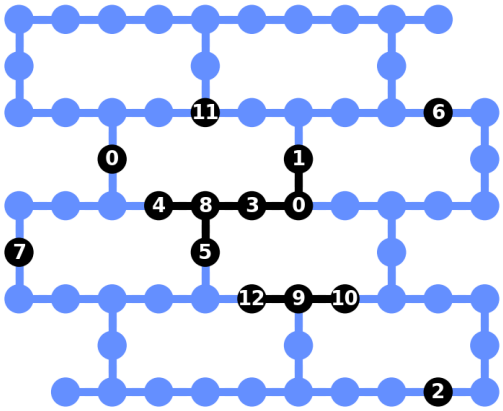

Figure 3: The quantum register mapping of a preconfigured Brooklyn quantum system with sabre layout and stochastic routing

3.2 Result visualization

As a result of the quantum simulation, metrics, plots, and charts are generated to help users understand the impact of the noisy quantum devices.

Users are encouraged to take a closer look at the experimental settings, analyze the results, think about the statistics, and come up with independent conclusions and their own way of understanding limitations of quantum computing.

Results are loaded with intertwined correlations and patterns that can lead to interesting insights and discoveries.

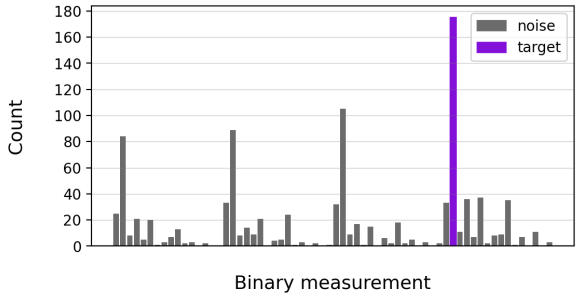

Figure 4: A count chart of an experiment with secret string 11001 and 1000 shots

If users find the provided statistics inadequate or lacking, they are free to download the quantum circuit (OpenQASM 2.0) and the measurements at the bottom of the bvviz page.

3.3 Purpose

bvviz helps those who are new to quantum computation not only to learn about the Bernstein-Vazirani algorithm, but also to gain a deeper understanding of the capabilities of quantum technology, which is currently very much limited by the unreliable hardware.

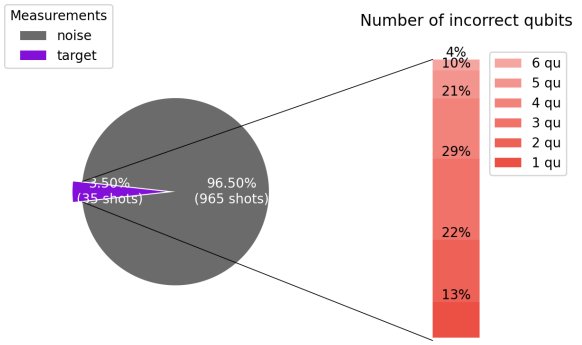

Figure 5: The metrics of an experiment performed on a very noisy device

4 Conclusion

The simulation and visualization of the Berstein-Vazirani protocol works properly and as expected. The application does a decent job of delivering the results.

The project was designed and developed in a modular manner, which makes the project easily expandable. Additional integration of new metrics, statistics and plots would be pretty straightforward. With a few modifications, it could be adapted to simulate and visualize other quantum protocols such as Simon's, Deutsch-Jozsa's, and Grover's algorithms.

References

[1] E. Bernstein, and U. Vazirani, "Quantum complexity theory," SIAM J. Comput., vol. 26, no. 5, pp. 1411–1473, 1997, doi: 10.1137/S0097539796300921.

[2] D. Deutsch, and R. Jozsa, "Rapid Solution of Problems by Quantum Computation," Proc. Roy. Soc. London Ser., vol. 439, no. 1907, pp. 553–558, Dec. 1992, doi: 10.1098/rspa.1992.0167.

[3] H. Xie, and L. Yang, "Using bernstein-vazirani algorithm to attack block ciphers," 2018.

[4] M. Ampatzis, and T. Andronikos, "Qkd based on symmetric entangled bernstein-vazirani," Entropy, vol. 23, no. 7, p. 870, Jul. 2021. [Online]. Available: http://dx.doi.org/10.3390/e23070870

[5] O. Goldreich, "On promise problems: a survey," Springer Berlin Heidelberg. [Online]. Available: https://doi.org/10.1007/11685654_12

[6] "Bernstein-Vazirani Algorithm," 2022. (learn.qiskit.org/course/ch-algorithms/bernstein-vazirani-algorithm)

[7] P. Young, "Physics 150, quantum computing," University of California, Santa Cruz. [Online]. Available: https://young.physics.ucsc.edu/150/

[8] S. Eduard, "Phase kickback," University of California, Santa Cruz. [Online]. Available: https://eduardsmetanin.github.io/PhaseKickback.pdf