Quality check of the Quantum Random Number Generator for weather forecast

Womanium Project report by Amit Modhwadia

Quantum-AI-for-Climate	
Team name :	**Solo Qubit**
Team Member Name :	Amit Modhwadia
Enrollment ID :	WQ24-OdfMsSyLDN6hEms

Index

[A] Problem Statement

Climate change is one of the biggest challenges in mankind's history. To tackle it, we need to use simulation models that can generate accurate weather forecasts. One type of simulation model is the Monte Carlo Simulation and Uncertainty Analysis, which uses random numbers to simulate various scenarios of climate processes. Quantum computers have shown great potential in generating random numbers. however, the quality and true randomness of these numbers remain uncertain. Ensuring the randomness of these quantum-generated numbers is crucial for the reliability of the simulation models. Therefore, This project aims to evaluate the quality of random numbers produced by quantum computers, specifically focusing on their randomness and suitability for use in climate simulation models.

[B] Project description and Literature review

In this century use of random numbers is everywhere from cryptography to predicting the climate change. That is why generating random numbers and checking the quality of randomness is crucial.

The goal of this project is to utilize a Quantum Random Number Generator (QRNG) to produce high-quality random numbers and subsequently evaluate the quality of these generated random numbers. The validated random numbers will then serve as input for a Monte Carlo simulation model to perform weather forecasting.

Monte Carlo Simulations in Climate Modelling

Monte Carlo model is a stochastic simulation method. This model is widely used in climate modelling to assess the uncertainty and variability of climate predictions. By generating multiple simulations with different random inputs, we can explore a range of possible future climates and better understand the probability of various outcomes.

- Principle of Monte-Carlo simulations
    - i. Monte-Carlo simulations are used for processing large amounts of data to calculate minimum, maximum, average, and mean values.
    - ii. These simulations are numerical methods that handle probabilistic phenomena.
    - iii. Monte-Carlo methods calculate unknown quantities by statistical sampling.

Monte-Carlo simulations are the model that used for detecting the huge amount of data. It works for picking some data from a huge database and to calculate the minimum, maximum, the average and the meant. This simulation can work really fast and easily. It is a numerical simulation method which takes probabilistic phenomena as the research object. As a matter of fact, it is a method of calculating unknown characteristic quantity by obtaining statistic value by sampling survey. The formulae of the average value and expected value of a certain function f(Xi) with probability of p(Xi) are given as follows:

$$\text{n}=\sum_{i=1}^{n} xi/n$$

$$F_N = \frac{1}{N}\sum_{i=1}^{n} f(Xi)/\, p(Xi\,)$$

Advantages:

- **Flexibility:** Monte Carlo simulations can be applied to a wide range of climate models and scenarios.
- **Uncertainty Quantification:** These simulations are essential for quantifying uncertainties in climate predictions.

Disadvantages:

- **Computational Cost:** Monte Carlo simulations require significant computational resources, especially when high-quality random numbers are needed.
- **Dependence on RNG Quality:** The accuracy of Monte Carlo simulations is directly tied to the quality of the random numbers used.

Existing systems generate random numbers, but we currently lack the means to evaluate the quality of this randomness. Assessing the quality is critical for applications in cryptography, simulations, and statistical sampling, as poor randomness can lead to patterns or biases. that's why we need Quantum Random Number Generators (QRNG) because randomness is one of the fundamental of quantum mechanics that will help to generate good quality random numbers

Advantages:

- **True Randomness:** Quantum processes are inherently random, offering a higher level of unpredictability compared to classical RNGs.
- **Time**: comparatively QRNGs is faster than classical RNGs.

Disadvantages:

- **Implementation Complexity:** The technology is still in its early stages and can be difficult to implement and scale.
- **Quality and Bias Concerns:** Despite their theoretical randomness, there are concerns about the quality and potential biases in the random numbers generated by QRNGs, particularly due to noise and hardware imperfections.

Evaluation of Random Number Generators

The quality of random numbers generated by both classical and quantum RNGs is typically evaluated using statistical tests such as the NIST Randomness Test Suite, TestU01, and Diehard tests. These tests are designed to detect patterns and biases that may compromise the randomness of the generated numbers.

Advantages:

- **Comprehensive Testing:** These tests provide a thorough evaluation of RNG quality, including aspects such as uniformity and independence.
- **Wide Adoption:** These test suites are widely used in both academic and industrial applications, providing a benchmark for RNG quality.

Disadvantages:

- **Specificity:** Some tests may be better suited for certain types of RNGs, and no single test suite can fully guarantee the quality of an RNG.
- **Resource Intensity:** Running comprehensive tests on large datasets can be computationally expensive.

[C] Methodology

The Quantum computers can revolutionize the way we do computation. We can use Quantum computers to speed up many sectors like finance, agriculture and weather forecasting and other sectors. specially for the weather forecasting it can use the Classical machine learning model and use Quantum computing this Hybrid model will speed up the prediction process. Classically the Monte Carlo Simulations will do the simulation and use the quantum computers to generate the random numbers and then evaluate the quality.

Objectives:

1. **Quantum Random Number Generation (QRNG):**

- Implement a QRNG to generate random numbers using quantum principles, which are inherently unpredictable and offer true randomness as opposed to classical pseudo-random number generators.

  i. **Quantum Phenomenon Utilization:**
  QRNGs use fundamental quantum phenomena, such as quantum superposition, entanglement, or the uncertainty in quantum measurement. These phenomena are unpredictable, providing a natural source of randomness.

  ii. **Measurement and Bit Generation:**
  The quantum system is measured, and due to the probabilistic nature of quantum mechanics, the outcome of the measurement is random. These outcomes are typically represented as binary bits (0s and 1s), forming the basis of the random number sequence.

  iii. **Post-Processing:**
  The raw bits generated from the quantum measurements are often subjected to post-processing to remove any potential biases or correlations, ensuring a uniform distribution of bits. The final output is a sequence of high-quality random numbers that can be used for various applications.

2. **Quality Assessment of Generated Numbers:**

- Quality Assessment of quantum random number generator (QRNG) through a series of statistical tests. These tests, including the Serial Test and Maurer's Universal Statistical Test, are applied to evaluate the randomness and unpredictability of the generated sequences. By analysing the distribution and compressibility of the sequences, we determine whether the QRNG produces statistically random numbers suitable for applications in simulations, and other fields where high-quality randomness is essential.

i. **Serial Test**: The Serial Test examines the distribution of overlapping m-bit blocks within a sequence. By comparing the observed frequencies of these blocks with the expected frequencies, the test determines whether the sequence exhibits the uniformity expected of a random sequence.

ii. **Maurer's Universal Statistical Test**: This test evaluates the compressibility of the sequence. A highly compressible sequence is likely to contain patterns, indicating a lack of randomness. The test computes a statistic based on the average distance between reoccurrences of the same blocks and uses it to calculate a p-value, which determines whether the sequence passes the randomness test.

3. **Monte Carlo Simulation for Weather Forecasting:**

- Use the high-quality random numbers as input to a Monte Carlo simulation model to predict weather patterns. Monte Carlo simulations rely on random sampling to obtain numerical results, and in this context, it will be used to simulate the probabilistic aspects of weather forecasting.
- Once the QRNG-generated numbers pass the randomness tests, they can be integrated into a Monte Carlo Simulations model for weather forecasting. Monte Carlo methods rely heavily on high-quality random inputs to simulate a wide range of possible future weather scenarios.

  i. **Simulation Setup**: The QRNG-generated numbers, validated through the statistical tests, are used as random inputs in the weather forecasting model. These inputs simulate various environmental variables, such as temperature, humidity, wind speed, and precipitation, over multiple iterations.
  ii. **Scenario Generation**: The randomness of the QRNG numbers ensures that the simulations cover a diverse range of possible outcomes, reflecting the inherent uncertainty in weather systems.
  iii. **Outcome Analysis**: The results from these simulations provide a probability distribution of possible weather conditions, helping meteorologists make more informed predictions and prepare for a range of potential scenarios.

[D] Demonstration (Code)

- The code demonstration for **Quantum Random Number Generatio** and **Quality Assessment of Generated Numbers** is in Github repository.

Results

The QRNG will generate random numbers, which will then be subjected to quality testing. The output of these tests includes p-values, which are compared against a significance level (typically set at 0.01). If the p-value is greater than this threshold, the sequence is considered random; otherwise, it fails the test, indicating potential patterns or non-randomness. If the sequence passes the quality tests, these random numbers will be used in simulations to generate weather forecasts.

Conclusion

By applying these tests, we can quantify the randomness of sequences generated by a QRNG. This process is crucial for validating the reliability of quantum-generated random numbers for use in sensitive applications, such as Monte Carlo Simulations for weather forecasting. The validated random numbers ensure that the simulations explore a comprehensive range of scenarios, improving the accuracy and reliability of weather forecasts. As a result, this approach enhances our ability to predict and prepare for various weather conditions, ultimately contributing to better decision-making in climate-related fields.

References

I] Application of Monte-Carlo Simulations in Environment and Chemistry Zhiyu Yang* King's Edgehill School, Windsor, Nova Scotia, Canada https://doi.org/10.54097/hset.v17i.2430

II] Inderscience. "New approach to generating truly random numbers may improve Internet security, weather forecasts." ScienceDaily. ScienceDaily, 22 February 2010. <www.sciencedaily.com/releases/2010/02/100222082529.htm>.

Jacak, M.M., Jóźwiak, P., Niemczuk, J. et al. Quantum generators of random numbers. Sci Rep 11, 16108 (2021). https://doi.org/10.1038/s41598-021-95388-7

III] Lo, S.-C.; Shih, Y.-C. A Genetic Algorithm with Quantum Random Number Generator for Solving the Pollution-Routing Problem in Sustainable Logistics Management. *Sustainability* **2021**, *13*, 8381. https://doi.org/10.3390/su13158381

Iv] Bassham, L. , Rukhin, A. , Soto, J. , Nechvatal, J. , Smid, M. , Leigh, S. , Levenson, M. , Vangel, M. , Heckert, N. and Banks, D. (2010), A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762 (Accessed August 7, 2024)