**Data Analysis**

**4.1 Analysis Methodology**

With all required data collected the next step was analysis. In total 8 empirical tests of randomness were performed. These consisted of:

* The Chi-Squared Test
* The Kolmogorov-Smirnov Test
* The Serial Test
* The Gap Test
* The Poker Test
* The Runs Test
* The Serial Correlation Test
* The Birthday Spacings Test

Many of these tests would have been provided in the Dieharder test suite, including the Kolmogorov-Smirnov and Birthday Spacings tests, however after technical issues regarding the set-up of a test battery the test suite shown above had to be produced manually within R Studio. The data analysis was completed in R primarily due to the facilities provided by the language for handling and visualising datasets as well as its wide array of test libraries that provided the functions necessary to produce the test suite shown above. Additional libraries such as ggplot2 and rjson also made R the obvious choice for analysis as the JSON datasets could easily be imported, processed, and graphed within R Studio. Although similar tools existed within languages like Python or MATLAB, the ggplot2 library available with R could produce much higher quality figures compared to Python alternatives like Matplotlib or Plotly while also providing a substantial amount of control to the user.

A screenshot of a computer code

Description automatically generated

*Figure 43. The R analysis program importing libraries and JSON data*

**4.2 Chi-Squared Test of Dice and Coin Simulation Data**

The first test used in this investigation was the Chi-Squared test, which is an empirical test designed to calculate a V value from a sequence of random numbers and compare that value to a distribution table to determine the probability that such a sequence could be produced. The main caveat of the Chi-Squared test that limited its use to only dice and coin data is the distribution table which only considers sequences with up to 101 exactly potential outputs. As all the pseudorandom sequences sampled in this investigation had a minimum of 100 potential outputs, it wasn’t feasible to apply Chi-Squared testing to them. However, for coin and dice data that had a maximum number of possible outputs of either 2 or 6, these datasets were easily mappable to the distribution table.

A math equation with numbers and symbols

Description automatically generated

*Figure 44. The Chi-Squared Equation (****Google, 2023****)*

A table of numbers with numbers

Description automatically generated

*Figure 45. The Chi-Squared Distribution Table (****University of Queensland, 2023****)*

The equation to determine the V value, seen in figure 44, was produced in R manually following the method seen in *The Art of Computer Programming Volume 2: Semi-numerical algorithms* (**Knuth, 1998**).

A computer code with text

Description automatically generated with medium confidence

*Figure 46. A screenshot of the Chi-Squared equation using C# Dice Simulation data*

Figure 46 shows the implementation of the Chi-Squared equation into R using dice simulation data. The *CDice1* list contains the frequency of observed values (Yn) produced by the first implementation of the C# dice simulation while the expected values (np) of each dice face occurring is set to 83.333… (Total Iterations (500) \* Probability of Outcome (1/6)). Every outcome in each dataset has its observed value compared against its expected value producing a V value for each dataset. Eight V values were produced from the collected dice data, two from C#, three from Python, one from JavaScript, one from Random.org, and one from physical dice.

A graph of different colored lines

Description automatically generated

*Figure 47. A Scatterplot Showing the Frequency of Dice Outcomes*

The frequency of observed values for each of the dice datasets is shown in figure 47. The most immediately noticeable trend is given by the JavaScript dataset which features a noticeably lower frequency of 1s and 6s but the largest frequency of 2s,3s,4s and 5s with all these outcomes occurring significantly more than expected. The remaining datasets all followed a similar trend, with the observed frequency of all possible outcomes occurring between 65 and 95 times.

|  |  |
| --- | --- |
| Data Source | V Value |
| C# Unseeded Rand | 1.192 |
| C# Seeded Rand | 4.024 |
| Python Randint | 3.064 |
| NumPy Unseeded Randint | 2.536 |
| NumPy Seeded Randint | 3.88 |
| JavaScript Rand | 37.12 |
| Random.org Data | 4.936 |
| Real Data | 6.28 |

*Figure 48. A Table of Results for the Chi-Squared Test of Dice Roll Data*

To compare the V values shown in figure 48 to the distribution table the degrees of freedom must be calculated. This can be done simply by subtracting 1 from the number of possible outcomes (k), in this case producing 5 degrees of freedom. A suitable random sequence is found between the .95 and .1 distributions while V values closer to .995 or .01 are considered too likely or too unlikely to be viable.

The C# unseeded rand implementation placed between the .95 and .9 distributions allowing it to be considered satisfactorily random. The seeded rand implementation placed between .9 and .1 which while closer to the expected values is still satisfactorily random.

In comparison to the C# data, all three Python sequences rated between the unseeded and seeded Rand data with no value scoring above or below the previous results. The Python Randint implementation placed between the .9 and .1 distributions classifying it as suitable. Both versions of the NumPy implementation also placed between the .9 and .1 distributions. Interestingly for Python even the mathematics centric NumPy library was unable to match C# and reach a distribution between .9 and .95.

The JavaScript dataset placed in the .01 distribution. This was by far the largest V value scored by any of the generators surveyed and as a result the dataset was considered unsuitable as a random number source. The highly unlikely nature of this data could also be seen in figure 47 in which the cause of this value can be assumed to be from the low frequencies recorded for outputs of 1 or 6.

The Random.org dataset was placed between the .9 and .1 distributions. Considering the claim of Random.org that all results produced through their site can be considered true random, this distribution placing was not unexpected. This dataset’s V value being only slightly higher than the Python or C# generators also presents an interesting argument regarding the validity of the pseudorandom generators. Assuming the data given by Random.org is truly random, then it’s possible the pseudorandom generators surveyed are capable of effectively simulating almost-true random conditions.

The real dice dataset placed between the .9 and .1 distributions. Much like the Random.org dataset, this placing was not unexpected as a true random generator will more often than not produce results with a good level of ‘reliable’ randomness. Besides JavaScript, the real dice scored the highest V value out of the generators sampled although since only one set of 500 samples were collected, it is possible that different rolling methods could have produced a noticeably different V value. Regardless the dice and rolling method used can be classified as satisfactorily random.

A graph of blue and pink bars

Description automatically generated

*Figure 49. A Bar Chart Showing the Frequency of Coin Outcomes*

The Chi-Squared testing of the coin data was completed the same as with the dice data. Observed values of heads and tails for each data source were compared against the expected values (np = 250) and when analysing this result with the distribution table 1 degree of freedom was used. Eight V values were produced from the coin flip datasets, two from C#, three from Python, one from JavaScript, one from Random.org, and one from a physical coin.

The frequency of observed values for each data source is shown in Figure 49. Interestingly, with the exception of the real coin values, every generator sampled produced more tails than heads. However, while some datasets had a noticeable difference in total heads vs tails such as the C# unseeded dataset, the NumPy datasets produced an almost even split of heads to tails.

|  |  |
| --- | --- |
| Data Source | V Value |
| C# Unseeded Rand | 1.352 |
| C# Seeded Rand | 0.8 |
| Python Randint | 0.968 |
| NumPy Unseeded Randint | 0.008 |
| NumPy Seeded Randint | 0.008 |
| JavaScript Rand | 0.128 |
| Random.org Data | 0.512 |
| Real Data | 0.128 |

*Figure 50. A Table of Results for the Chi-Squared Test of Coin Flip Data*

The C# datasets were both placed between the .9 and .1 distribution again allowing the dataset to be considered acceptably random. While both implementations remained valid methods of pseudorandom generation the use of the binary restraint on possible outputs causing neither to fall into the lower .95-.9 distribution could imply that the use of limitations on the generator does impact performance.

The Python datasets were all placed between the .9 and .1 distribution which remained consistent with the dice simulation results. Unlike with the dice simulation results, the NumPy implementations were able to produce the exact same results and had the same V value which enforces the idea that the restriction on possible outputs has a noticeable impact on generator performance.

The JavaScript dataset was placed between the .9 and .1 distribution. Compared to the dice simulation V this is a significant improvement for the JavaScript implementation as in this test it was considered satisfactorily random. It was unclear why the dice simulation produced a sequence that contained such a significant decrease in 1s and 6s, but it is evident that this irregular pattern did not persist in the coin simulation. No pseudorandom generator is designed to perform optimally in all tests or simulations and the improvement in distribution showed that the JavaScript generator could still be considered valid for random number generation.

The Random.org dataset placed between the .9 and .1 distribution. As with the dice simulation data, this result was not unexpected for this data source and the consistent satisfactorily random output shown supports the idea that the data gathered is from a true random source.

The real coin dataset scored identically to the JavaScript dataset. As seen with the Python data repeated V values are entirely possible however unlike what was shown before these values came from completely different sources. While this does aid in showing the validity of the JavaScript generator, it must be considered that the limited possible outcomes of a coin flip presents a scenario where similar or matching outputs between data sources is far more likely.

**4.3 Kolmogorov-Smirnov Test of Empirical Distribution**

After the analysis of the dice and coin simulation data, the investigation moved to focus on the numeric sequence data provided by the pseudorandom generators. The first test used on this data was the Kolmogorov-Smirnov test which focused on the distribution of data between the minimum and maximum potential values. To pass this test a generator must show an empirical distribution, and as such an empirical weighting, of all data provided. This is given by a 1-sample test value which must not score above the critical value of 0.501 (0.5 + 0.001 (the upper bound of N=100)) and with datasets containing multiple implementations a 2-sample test value which must not score above the value of *α* (0.05) to be classified as empirically distributed. The main caveat of this test was that it was designed for data between 0 and 1 so in order to adjust the outputs provided, division by 100 was used to ensure data normally in integer form between 0 and 100 was in the correct format.

A screenshot of a computer code

Description automatically generated

*Figure 51. A screenshot of the KS function using C# rand data*

Figure 51 shows the implementation of the Kolmogorov-Smirnov test with the C# data. When a data source contained more than one data set, both 1 sample and 2 sample tests were performed. The results of the testing are shown in figure 50. To visualise the empirical distribution of the data sets, the *ecdf* function provided by R was also used to calculate plottable empirical distribution data points.

|  |  |  |  |
| --- | --- | --- | --- |
| Data Sources | 1 Sample Test Statistic | 2 Sample Test Statistic 1 | 2 Sample Test Statistic 2 |
| C# Unseeded Rand | 0.5 | 0.046 | 0.592 |
| C# Seeded Rand | 0.5 | 0.592 | 0.046 |
| C# Cryptographic Rand | 0.51842 | 0.592 | 0.592 |
| Lehmer Int Version 1 | 0.15921 | 0.42 | N/A |
| Lehmer Int Version 2 | 0.3444 | 0.42 | N/A |
| Lehmer Real Version 1 | 0.50074 | 0.042 | N/A |
| Lehmer Real Version 2 | 0.50002 | 0.042 | N/A |
| Python Randint | 0.5 | 0.048 | 0.042 |
| Python Unseeded Random | 0.50118 | 0.048 | N/A |
| Python Seeded Random | 0.50215 | 0.048 | N/A |
| NumPy Unseeded Randint | 0.5 | 0.038 | N/A |
| NumPy Seeded Randint | 0.5 | 0.048 | 0.038 |
| JavaScript Rand | 0.5 | N/A | N/A |
| Middle Square Method | 0.51594 | N/A | N/A |
| Random.org Data | 0.50399 | N/A | N/A |
| Park White Noise Data | 0.47854 | 0.338 | 0.192 |
| Sea White Noise Data | 0.49299 | 0.192 | 0.456 |
| Roundabout White Noise Data | 0.57062 | 0.338 | 0.456 |

*Figure 52. A Table of Results for the Kolmogorov-Smirnov Test*

A graph of a number of data

Description automatically generated with medium confidence

*Figure 53. A Scatter Graph Showing the Distribution of C# Rand Data*

Both the unseeded and seeded C# implementations of rand were shown to have an empirical distribution of results while the cryptographic implementation failed both 1-sample and 2-sample KS testing. Figure 53 shows the empirical distribution of all three implementations. While the unseeded and seeded implementations follow an expected upwards trend from 0 to 1, the cryptographic implementation, while still following an upwards trend, shows far less distributions between 0.2 and 1.0 on the Y axis.

A graph of a number of numbers and a number of numbers

Description automatically generated with medium confidence

*Figure 54. A Scatter Graph Showing the Distribution of Lehmer Generator Data*

By far the most successful implementations of the Lehmer Generator were versions 1 and 2 of the Real based generators which passed both the 1-sample and 2-sample KS tests. Although able to pass the 1-sample tests, version 1 and 2 of the Integer based generators failed the 2-sample tests. The reason for this can be seen in figure 54, which shows the Real implementations following the expected upwards trend seen in figure 53 while the Integer version 1 begins around 0.4 instead of 0 and Integer version 2 shows almost no upwards trend at all.

A graph of a number of data

Description automatically generated with medium confidence

*Figure 55. A Scatter Graph Showing the Distribution of Python Rand Data*

The integer sequence Randint generators within Python and NumPy performed better than the real/decimal sequence Random generators, with all three of the Randint functions passing the 1-sample and 2-sample KS tests. Although they failed the 1-sample test, the unseeded and seeded Random functions did pass the 2-sample test and as shown in figure 55 all five of the Python implementations showed an empirical distribution.

A graph with blue dots

Description automatically generated

*Figure 56. A Scatter Graph Showing the Distribution of JavaScript Rand Data*

The JavaScript dataset passed the 1-sample KS test although was unable to perform the 2-sample test due to lack of alternate implementations available within the language. Figure 56 shows the distribution of the JavaScript data which followed the expected trend. The empirical distribution shown, in addition to the results of the coin simulation data, helps to confirm the potential validity of the JavaScript implementation despite its original poorer performance when simulating dice rolls.

A graph with blue dots and white text

Description automatically generated

*Figure 57. A Scatter Graph Showing the Distribution of Middle Square Method Data*

As expected, the Middle Square dataset did not pass the 1-sample KS test and was unable to complete a 2-sample test due to lack of additional data. The distribution shown in figure 57 also confirms the unsuitable nature of the Middle Square method as a pseudorandom generator, in which the methods repeating cycle of values are seen as a series of unconnected lines rather than a trend of data points. While other unsuitable generators sampled in this investigation such as the integer based Lehmer generators show a similar horizontal instead of vertical trend, the Middle Square dataset is the best example of this.

A graph with blue dots

Description automatically generated

*Figure 58. A Scatter Graph Showing the Distribution of Random.org Data*

The Random.org dataset failed the 1-sample KS test, with a test statistic just 0.0299 away from the critical value. When visualised in figure 58, the trend shown by the data mostly corresponds with what is expected however features several breaks throughout the distribution, these being at 0, 0.2, 0.7 and 0.9, which could explain why the dataset was only just beyond the point of passing. Overall, the data is visibly similar to that seen in figures 56 or 53.

A graph showing a number of different colored lines

Description automatically generated

*Figure 59. A Scatter Graph Showing the Distribution of White Noise Data*

The Park and Sea white noise datasets passed both the 1-sample and 2-sample KS tests while the Roundabout dataset could only pass the 2-sample tests. When viewing the distribution of the white noise data in figure 59 all three datasets show unique trends unseen with any of the other generators. All three trend upwards, however only the Park and Roundabout data reach the max Fn(x) value of 1.0 as the Sea data achieves a maximum of 0.8. All three datasets show a section of horizontal trending although this trend is most significant in the Park and Sea data.

A graph of a graph

Description automatically generated

*Figure 60. A Scatter Graph Showing the Distribution of all Collected Rand Data*

When all the data is graphed together, the most noticeable outliers are the white noise data and the C# cryptographic data. This was likely due to the differences in format that these generators produced, with the white noise data covering a far larger range of possible outputs and the cryptographic generator providing a secure sequence that shouldn’t match any results from reproducible pseudorandom generators. The remaining generators all mostly conform to an empirical distribution and this is reflected both in figure 60 and the results within figure 52.

**4.4 Serial Test of Empirical Distribution**

While the Kolmogorov-Smirnov test focused on the distribution of whole datasets, the Serial test instead compares the empirical distribution of sets within the data. This test provides two output statistics: a test statistic, and a P-value. While the test statistic can be used for comparison between generators, where a lower value indicates a dataset where the observed number of sets more closely match the expected number of sets, the P-value or Probability value represents the likelihood that the data provided was able to achieve its test statistic. Much like with the Chi-Squared test an ideal generator will provide a P-value that is neither too large nor too small, with the best performing generators being the ones able to score the value closest to 0.5.

|  |  |  |
| --- | --- | --- |
| Data Sources | Test Statistic | P-Value |
| C# Unseeded Rand | 1.2 | 0.76 |
| C# Seeded Rand | 1.5 | 0.69 |
| C# Cryptographic Rand | 139 | 7.1e-30 |
| Python Randint | 5.4 | 0.14 |
| Python Unseeded Rand | 3.9 | 0.27 |
| Python Seeded Rand | 9 | 0.03 |
| NumPy Unseeded Randint | 2.8 | 0.43 |
| NumPy Seeded Randint | 1.4 | 0.7 |
| JavaScript Rand | 5 | 0.17 |
| Random.org Data | 3.4 | 0.33 |
| Lehmer Int Version 1 | 87 | 0.1e-19 |
| Lehmer Int Version 2 | 223 | 4.9e-48 |
| Lehmer Real Version 1 | 3.9 | 0.28 |
| Lehmer Real Version 2 | 0.34 | 0.95 |
| Middle Square Data | 726 | 4.2e-157 |
| Park White Noise Data | 250 | 6.5e-54 |
| Roundabout White Noise Data | 230 | 1.1e-49 |
| Sea White Noise Data | 237 | 5.2e-51 |

*Figure 61. A Table of Results for the Serial Test*

A graph of colored rectangular bars

Description automatically generated with medium confidence

*Figure 62. A Bar Chart Showing P-Values of Collected Serial Test Data*

The unseeded and seeded Rand data from C# performed well in the Serial test, scoring close to the optimal P-value and being among the lowest test statistics scored. However, the same couldn’t be said about the cryptographic data which failed to pass the test with both its test statistic and P-value. The most likely explanation for this is that the cryptographic sequence produced focused on avoiding expected or predictable sequencing to allow for its use in secure systems.

All Python datasets passed the Serial test, with the NumPy unseeded implementation achieving the best P-value of any dataset and the NumPy seeded implementation scoring one of the lowest test statistics. An obvious outlier within the Python data was the Seeded Rand implementation which had a high test statistic and the lowest non-anomalous P-value meaning the serial sets it had produced were highly unlikely.

The JavaScript dataset passed the Serial test, however performed poorer than other implementations in regard to both test statistic and P-value. The values given for the JavaScript generator were close to those of the Python Randint implementation, with JavaScript scoring a lower test statistic and a P-value only 0.03 higher.

The Random.org data also passed, with the second-best P-value recorded. This was not mirrored in the test statistic however, which while still low was beaten by the NumPy implementations and the C# implementations. This overall decent performance does help to reinforce the claim that Random.org is a true random number generator, with sequences being considered satisfactorily random across multiple tests.

As with the KS tests previously, the integer versions of the Lehmer Generator failed to pass the Serial test, producing not only incredibly high test statistics but also anomalous P-values so small the sequences produced had to be considered too unlikely to be valid. In contrast, the real versions of the Lehmer Generator passed the Serial test, although version 2 did produce the highest P-value of any implementation, making it too likely to be considered valid. Version 1 performed better, however, with the fourth best P-value recorded.

The Middle Square data, as expected, failed the Serial test with the worst test statistic and P-value recorded for any dataset. This was obviously due to the repetitive nature of the method which would begin to iterate when the seed used for calculations would constantly loop back to itself. Due to this being a test of distributed sets within the data, the hundreds of repeated pairs were penalised heavily.