Zufallszahlen: Das Experiment

Heidi, Pascal, Tom, Karl

Institut für Physik Humboldt-Universität zu Berlin

"Gott würfelt nicht" (Albert Einstein)

Eine deterministische Weltsicht ist einer der wichtigsten Grundlagen der Naturwissenschaften, in denen es das Ziel ist, vergangene Experimente zu begründen und zukünftige vorherzusagen. Umso paradoxer erscheint es somit, dass Zufallszahlen durchaus viele wichtige Anwendungen in der Physik haben und umso schwieriger, diese Zufallszahlen auf physikalischem Wege experimentell zu erzeugen. Dieser Herkulesaufgabe aber werden wir uns im Folgenden annehmen.

Was ist echter Zufall eigentlich?

Zufall ist ein allgegenwärtiger Begriff unseres Lebens. Zu definieren was Zufall aber eigentlich ist und inwieweit unser Leben zufällig ist, ist allerdings eine hochkomplexe philosophische Fragestellung. Nehmen wir einen allseits bekannten Zufallszahlengenerator: den Würfel.

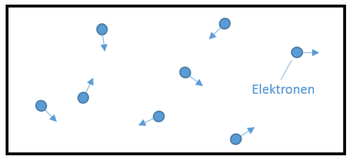
[1]

In erster Betrachtung ist das Ergebnis eines Würfelwurfs völlig zufällig in der Hinsicht, dass man diesen nicht vorhersagen kann. Würde man allerdings alle Anfangsbedingungen wie Abwurfhöhe, Abwurfwinkel und alle Randbedingungen wie z.B die Beschaffenheit des Tisches auf dem gewürfelt wird kennen, so könnte man zumindest theoretisch das Würfelergebnis vorhersagen. Da diese Kenntnisse und Berechnungen jedoch heute in der Praxis schwer bis gar nicht realisierbar sind, spielt dies beim Würfeln keine Rolle, weshalb es sich trotzdem um eine „Wahre Zufallszahl“ handelt. Mit der Erzeugung solcher wahren Zufallszahlen wird sich im folgenden beschäftigt.

Zur Erzeugung wahrer Zufallszahlen in Form von physikalischen Experimenten wollen wir nun zwei präsentieren:

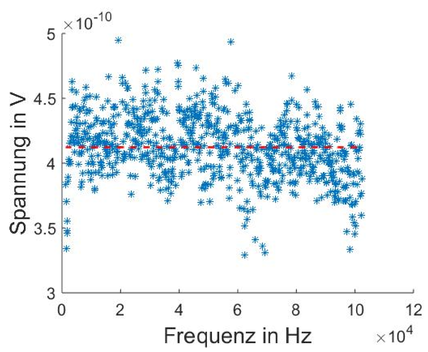
Thermisches Rauschen

Das thermische Rauschen ist eigentlich ein ungewolltes Störphänomen, welches jegliche elektrische Messungen überlagert. Zu unserem Glück ist dieses Rauschen allerdings nicht nur störend, sondern auch zufällig.



Ursache des Rauschens ist die thermische Energie der Elektronen. Abhängig von ihrer Temperatur bewegen sich die Elektronen mit einer bestimmten Geschwindigkeitsverteilung durch das Material und stoßen an dessen Wänden hin und her. Diese Bewegung der Elektronen führt bei der Spannungsmessung an einem Widerstand zu einer zusätzlichen, fluktuierenden Spannung (dem Rauschen).

Messung

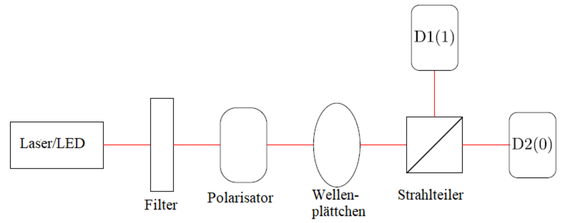


In der obigen Abbildung ist eine Messung des Spannungsabfalls an einem Widerstand für verschiedene Frequenzen gezeigt. Die rote Linie zeigt den ohmschen Widerstand und die darum verteilten Punkte zeigen die Spannungsmessungen mit Rauschen. Aus den auf diese Art und Weise erzeugten zufälligen Zahlen lässt sich jetzt ganz einfach ein Binärcode aus Zufallszahlen erstellen.

Auch das thermische Rauschen könnte man theoretisch vorhersagen wenn man die initialen Geschwindigkeiten aller Elektronen kennen würde, so könnte man die Spannungsfluktuationen berechnen.

Optisches Experiment

Es wurden 2 Möglichkeiten der optischen Erzeugung mit demselben Experiment getestet. Zum einen mithilfe der Aufteilung von polarisiertem Laserlicht über einen Strahlteiler und zum anderen über die Verteilung der Ankunftszeiten auf den genutzten Detektoren.



Konzeptioneller Aufbau

Im dargestellten Aufbau wird von den Detektoren zusätzlich der zeitliche Verlauf der Photonen-Detektionen aufgenommen, um aus deren Differenz die Ankunftszeiten zu berechnen.

Messung

Mithilfe des Strahlteilers kann bei richtiger Einstellung der Polarisation des Lichts, gerade mit 50% Wahrscheinlichkeit, ein Photon auf einem der beiden Detektoren gemessen werden. Wenn man nun den Detektoren 0 und 1 zuordnet und deren Signale den zeitlichen Verlauf der Messungen zuordnet, ergibt sich direkt eine zufällige Bitfolge.
Aus den selben Messdaten können über die Verteilung der Ankunftszeiten, welche exponentiell abfallen sollten, weitere Zufallszahlen erzeugt werden. Indem die Ankunftszeiten in Bereiche mit gleicher erwarteter Anzahl an Events eingeteilt werden, kann über Vergleich der Anzahl an Events aufeinanderfolgender Bereiche eine zufällige Bitfolge erzeugt werden. Eine weitere Möglichkeit besteht in dem Vergleich aufeinanderfolgender Ankunftszeiten.

Ergebnisse

In beiden Experimenten konnten Zufallszahlen erzeugt werden. Jedoch lag die Anzahl und Rate an erzeugten zufälligen Bits im Fall des optischen Aufbaus weitaus höher, mit bis zu 100 k-Bits/s im Gegensatz zu 130Bits/s. Dazu ist zu sagen, dass im optischen Aufbau die Raten theoretisch nur von der Detektor-Totzeit beschränkt werden, welche bei ca. 35ns liegt, wodurch Raten in der Größenordnung von 10 M-Bits/s erreichbar sein könnten. Im Fall der Rauschmessungen sollten jedoch auch durch Optimierung und Automatisierung Raten von mehreren 10 k-Bits/s erreichbar sein.
Die Güte der Zufallszahlen wurde weiterhin untersucht, wobei sich keine deutlichen Unterschiede ergaben, jedoch in allen erzeugten Bitfolgen der Runs-Test nicht bestanden wurde.

Vergleich der Experimente

Da es sich bei den vermessenen Eigenschaften des optischen Experiments (Polarisation und Emission) um quantenmechanische Phänomene handelt, die selbst unter Kenntnis aller Randbedingungen nicht vorhersagbar sind, handelt es sich tatsächlich um wahre Zufallszahlen im Gegensatz zur thermischen-Rauschmessung. Jedoch wäre auch mithilfe einer Rauschmessung bei sehr geringen Temperaturen eine Erzeugung von wahren Zufallszahlen möglich, indem das sogenannte Stromrauschen untersucht wird.

Zusammenfassung

Im Allgemeinen ist die Erzeugung mithilfe des optischen Experiments schneller, jedoch sind die genutzten Komponenten sehr viel teurer, der Aufbau schwieriger zu kalibrieren und aufgrund der vorgenommenen Tests kein deutlicher Unterschied zwischen der Güte der Zufallszahlen erkennbar. Unter der Annahme, dass die Rate im Falle der Rauschmessungen leicht erhöht werden kann, sollte dieser Aufbau für einen einfachen Zufallsgenerator mit nicht hoher Güte bevorzugt werden.