

Aufbau eines Quantenzufallsexperiments für SchülerInnen

Wissenschaftliche Hausarbeit zur Ersten Lehramtsprüfung an
Realschulen nach der LPO I

Eingereicht von
Qerimi, Linda

Gutachter: Prof. H. Weinfurter

Erste Staatsprüfung für das Lehramt an Realschulen Bayern
Ludwig-Maximilians-Universität München

Erklärung zur Hausarbeit gemäß § 29 (Abs.6) LPO I

Hiermit erkläre ich, dass die vorliegende Hausarbeit von mir selbstständig verfasst wurde und dass keine anderen als die angegebenen Hilfsmittel benutzt wurden. Die Stellen der Arbeit, die anderen Werken dem Wortlaut oder Sinn nach entnommen sind, sind in jedem einzelnen Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht.

Diese Erklärung erstreckt sich auch auf etwa in der Arbeit enthaltene Zeichnungen, Kartenskizzen und bildliche Darstellungen.

Ort, Datum

Unterschrift

Inhaltsverzeichnis

1. Einleitung	7
2. Grundlagen	8
2.1 Zufallszahlen.....	8
2.2 Zufallszahlengeneratoren.....	9
2.2.1 Pseudozufallszahlengenerator	9
2.2.2 Physikalische Zufallszahlengeneratoren	11
2.3 Lichtquelle	13
2.4 Abschwächung der Laserstrahlung	16
2.5 Detektoren	19
3. Versuchsaufbau und -durchführung	23
3.1 Experimenteller Aufbau	23
3.2 Signalaufnahme.....	27
3.3 Austausch des Strahlteilers	30
4. Testung der Zufallszahlen	31
4.1 Bestimmung von Pi.....	31
4.2 Chi-Quadrat-Test	32
4.3 Kettenlängentest.....	38
4.4 NIST Analyseprogramm.....	40
5. Schülergerechte Integration des Experiments	41
5.1 Analyse	41
5.2 Konzept für die Schüleranleitung	43
5.3 Bildungsplan	47
5.4 Testung anhand einer Stichprobe	48
5.5 Anleitung für das Experiment.....	50
Anhang.....	51
Literaturverzeichnis.....	73

1. Einleitung

Im Schülerlabor PhotonLab des Max-Planck-Instituts für Quantenoptik können Schülerinnen und Schüler Einblicke in unterschiedliche Experimente der (Quanten-) Optik erhalten und dabei selbst experimentell Erfahrungen sammeln.

Im Rahmen meiner Zulassungsarbeit habe ich mich mit der Erzeugung von Zufallszahlen beschäftigt. Primär ging es darum, wie diese für Schülerinnen und Schüler verdeutlicht werden können. Mit dem Quantenzufallszahlengenerator kann das Thema physikalisch in ein Experiment eingebettet werden.

Es ist nicht einfach, Schülerinnen und Schüler Zufälligkeit im Mathematikunterricht zu vermitteln. Hier kommt zusätzlich noch der quantenphysikalische Inhalt hinzu, der die Komplexität erhöht. Es zeigt sich jedoch, dass sich ein Lernprozess erfolgreich gestalten lässt, sobald dieser Prozess Vernetzungen zu anderen Bereichen herstellt und vor allem wenn dieser in einen Kontext eingebunden ist (Rainer Müller, 2006).

Unter diesem Aspekt habe ich mich mit folgenden Fragen beschäftigt: „Wie vermittele ich Lernenden, Zufallszahlen aus verschiedenen Perspektiven zu betrachten?“, „Lassen sich Zufallszahlen klassifizieren?“ „Warum kann man mit einem Quantenzufallszahlengenerator sehr gute Zufallszahlen erzeugen?“

Für das Experiment wird stark abgeschwächtes Laserlicht auf einen polarisierenden Strahlteiler gelenkt. Dieser lenkt das Licht entsprechend seiner Polarisation, horizontal oder vertikal, ab. Wenn nun ein diagonal polarisiertes Photon, also eine Überlagerung von horizontal und vertikal polarisiert, auf den Strahlteiler trifft, ist es allein dem Zufall überlassen welchen Weg das Photon nimmt.

Ziel dieser Arbeit war die Erzeugung von quantenoptischen Zufallszahlen zu analysieren und für Schülerinnen und Schüler zu verdeutlichen. Zudem sollen diese von einem im Alltag wahrgenommenen Zufallsverständnis abgehoben werden. Diese Arbeit nimmt Anschluss an dem Quantenzufallexperiment von Leo Führinger (2012).

2. Grundlagen

In diesem Kapitel werden die elementaren Zusammenhänge zwischen (Quanten-) Optik und den Komponenten von Quantenzufallszahlengeneratoren (engl. *Quantum Random Number Generator* kurz: QRNG) erläutert. Außerdem wird versucht, den Zufall - sowie Zufallszahlen - zu beschreiben. Anschließend wird kurz auf unterschiedliche Typen von Zufallszahlengeneratoren eingegangen.

2.1 Zufallszahlen

Wenn man Zufallszahlen definieren will, ist es notwendig sich mit der Definition von Zufall zu beschäftigen. Diese eher philosophische Frage lässt sich nicht so einfach beantworten. Man stellt fest, wie weitreichend und vielfältig Zufall betrachtet wird.

Eine frequentistische Definition von Prof. Wolfgang König, 2013 zeigt, wie versucht wird, den Zufall durch Wahrscheinlichkeit greifbar zu machen:

Die Wahrscheinlichkeit eines zufälligen Ereignisses (=des Ausgangs eines Experimentes, das man oft unter gleichen Bedingungen wiederholen kann) ist der Grenzwert der relativen Häufigkeit des Eintretens dieses Ereignisses bei vielen Wiederholungen.

Durch nähere Betrachtung hat sich herausgestellt, dass es nicht so einfach ist, den Zufall ausschließlich mathematisch zu beschreiben. Es zeigen sich vor allem bei Quantenobjekten neue Regeln, die zu berücksichtigen sind (näheres dazu unter 2.2.2.2 quantenoptische Zufallszahlengeneratoren).

Prinzipiell sind Zufallszahlen Zahlen, die aus Zufallsexperimenten entstanden sind. Dabei gilt zu unterscheiden, aus welchen Zufallsexperimenten diese Zahlen hervorgegangen sind, denn: Zufallszahlen, die mit Hilfe mathematischer Algorithmen erzeugt wurden, werden nur als Pseudozufallszahlen bezeichnet (Hagmann, 2000).

Schwieriger ist es, eine Definition für sogenannte physikalisch generierte Zufallszahlen zu finden. Diese lassen sich noch weiter unterteilen in quantenphysikalisch generierte

Zufallszahlen und in solche, die aus Experimenten mit makroskopischen Objekten (mit unkontrollierbaren Parametern), wie beispielsweise Münzwurf oder Würfelspiel resultieren.

Über die Definition von Zufallszahlen hinaus, ist es ebenfalls nötig, die Güte von Zufallszahlen, also sozusagen deren Zufälligkeit, zu quantifizieren (näheres unter Kapitel 4, Testung und Ergebnisse der Zufallszahlen).

2.2 Zufallszahlengeneratoren

Die Generierung von Zufallszahlen spielt eine wichtige Rolle für die moderne Kryptographie. Die dabei verwendeten Zufallszahlen müssen hohen Anforderungen genügen, um keine Angriffsmöglichkeiten auf die gesicherten Systeme zu ermöglichen. Sie müssen idealerweise „echt“ zufällig sein. Die Generierung qualitativ hochwertiger Zufallszahlen stellt daher ein wichtiges Thema in der Wissenschaft und Praxis dar (Chen et al. 2011).

Dem Ideal „echte“ Zufallszahlen zu erzeugen, gerecht zu werden, stellt sich als äußerst schwierig heraus. In dieser Arbeit werden für die Erzeugung von Zufallszahlen Pseudozufallszahlengeneratoren (engl. *Pseudo Random Number Generator*, kurz: PRNG), physikalische Zufallszahlengeneratoren, die sich auf die Gesetze der klassischen Physik beschränken und quantenphysikalische Zufallszahlengeneratoren genauer betrachtet.

2.2.1 Pseudozufallszahlengenerator

Der Name Pseudozufallszahlengenerator lässt bereits rückschließen, dass es hierbei nicht um eine echte Zufallszahlengenerierung geht.

So werden beispielsweise bei algorithmischen Zufallszahlengeneratoren, Zahlenfolgen mithilfe eines Algorithmus aus einem Startwert (engl. Seed) berechnet. Durch dieses deterministische Vorgehen besteht die Möglichkeit bei gleichem oder bekanntem Startwert dieselbe Bitfolge zu erzielen (Fürst, 2011). Zusätzlich wiederholt sich die Folge ab einem bestimmten Zyklus, womit die Unabhängigkeit des nächsten

Folglieds nicht mehr gegeben ist. Pseudozufallszahlengeneratoren werden trotz dieses Konzepts in vielen Prozessen verwendet, da sie sehr schnell arbeiten. Sie werden in numerischen Berechnungen zum Beispiel zur Lösung komplexer Integrale oder für Simulationen genutzt. Generell werden Pseudozufallszahlengeneratoren dort verwendet, wo der Determinismus oder die Endlichkeit einer Folge keine bedeutende Rolle spielt. Aufgrund der deterministischen Erzeugung eignen sich diese Zufallszahlen bei kryptographischen Anwendungen nur bedingt, da die Reproduzierbarkeit einer Bitfolge möglich ist. Um die Sicherheit zu erhöhen versucht man durch unbestimmte Ereignisse wie beispielsweise Mausbewegung oder Tastaturanschläge den Startwert zu erneuern (Fürst, 2011). Die Idee, unbestimmte Ereignisse für die Erzeugung von Zufallszahlen zu nutzen, steht auch bei anderen Typen von Zufallszahlengeneratoren im Vordergrund. Was für ein unbestimmtes Ereignis verwendet wird, ist letztendlich entscheidend für die Qualität der Zufallszahlen.

Beispiele für algorithmische Pseudozufallszahlengeneratoren sind das Lineare Rückgekoppelte Schiebe-Register (kurz: LFSR, Abbildung 2.1) und das Von-Neumann-Verfahren, welches Johann von Neumann 1946 erfunden hat.

Lineargekoppelte Schieberegister

Die Funktion des Schieberegisters beruht darauf, dass dessen Eingang, durch eine Verbindung der Einträge im Schieberegister bei jedem Zyklus neu berechnet wird. Durch die einfache Implementierung in Mikroprozessoren und programmierbarer Logik wird diese Art von Pseudozufallszahlengenerierung vielfach eingesetzt (Schroeder 2009).

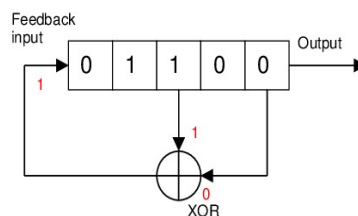


Abbildung 2.1: Funktionsweise des Linearen Rückgekoppelten Schiebe Registers: Ein Signal mit mehreren Bits wird taktgesteuert aufgenommen, vorübergehend gespeichert und wieder ausgegeben (Output). Mit einer logischen Verknüpfung (XOR) wird eine zufällige Binärfolge gebildet. Diese zufällige Anordnung hat jedoch seine Grenzen (maximal 2^5 unterschiedliche Positionen möglich). Quelle: <https://www.researchgate.net>

Von – Neumann - Verfahren

Für das Von – Neumann – Verfahren nimmt man eine beliebige sechstellige Dezimalzahl. Als nächstes wird diese Zahl quadriert. Nun nimmt man die mittleren Dezimalstellen. Diese ist die erste Pseudozufallszahl. Dann wiederholt man den Vorgang immer wieder:

$$675248^2 = 455959861504$$

$$959861^2 = 921333139300$$

$$333139^2 = 110981593300$$

... ..

Dieses Verfahren funktioniert nicht mit jeder Anfangszahl, aber bei bestimmten Startwerten sehen die Ergebnisse zufällig aus.

2.2.2 Physikalische Zufallszahlengeneratoren

Nach Hildebrandt (2002) lassen sich physikalische Zufallszahlengeneratoren wie folgt unterteilen:

- Zufallszahlengeneratoren, *welche aufgrund der Unvorhersagbarkeit von Ereignissen wegen der (komplexen) Dynamik eines makroskopischen Systems, funktionieren.*
- Zufallszahlengeneratoren, *die die Unbestimmtheit einer Messung mit mehreren möglichen Messresultaten an einem quantenmechanischen Objekt nutzen.* Zu diesen gehören quantenoptische Zufallszahlengeneratoren.

Dabei können auch andere Funktionsprinzipien zum Tragen kommen.

2.2.2.1 Klassische Zufallszahlengeneratoren

Zufallszahlengeneratoren, die aufgrund der komplexen Dynamik in makroskopischen Systemen verwendet werden, sind im Grunde genommen ein deterministisches System. Aufgrund der schwierigen Erfassung sämtlicher Parameter, die sich in dem Ereignis ergeben, erscheint das Resultat unvorhersehbar, also zufällig. Physikalische Zufallszahlengeneratoren dieses Typs können mit den Gesetzen der klassischen Physik beschrieben werden. Es gibt keine unbekanntes Bedingungen. Die Schwierigkeit liegt jedoch im gleichzeitigen Erfassen aller Parameter sowie deren zeitlichen Dynamik, um einen Ausgang voraussagen zu können. Ein gutes Beispiel ist der Münzwurf. Hätte man sämtliche Parameter (Luftreibung, Rotationsgeschwindigkeit, Steighöhe usw.) unter Kontrolle, so hätte man kein unbekanntes Endresultat (also Kopf oder Zahl) mehr. Man kann also exakt bestimmen, ob Kopf oder Zahl fällt. Die gesamten Parameter gleichzeitig zu kennen ist jedoch unmöglich.

Physikalische Zufallszahlengeneratoren stellen aufgrund der sehr komplexen Parametrisierung einen wichtigen Teil zur Erzeugung von Zufallszahlen dar. Physikalische Zufallszahlengeneratoren, die mithilfe klassischer Physik beschreibbar sind und daher im Prinzip berechnet werden können sind im kryptographischen Anwendungsgebiet aufgrund der Komplexität der Prozesse sicherer als algorithmische Verfahren (Welt der Physik, 2013).

2.2.2.2 Quantenoptische Zufallszahlengeneratoren

Die Basis von quantenphysikalischen Zufallszahlengeneratoren ist die Messung eines Quantensystems. Als Ergebnis der Messung treten die Eigenzustände jeweils mit einer bestimmten Wahrscheinlichkeit auf. Diese Wahrscheinlichkeit dient als Grundlage zur Erzeugung von Zufallszahlen (Martin Fürst, 2011). Diese Arbeit beschränkt sich auf einen Quantenzufallszahlengenerator, der auf „schwachen“ Lichtfeldern und einem Strahlteiler basiert (Abbildung 2.2).

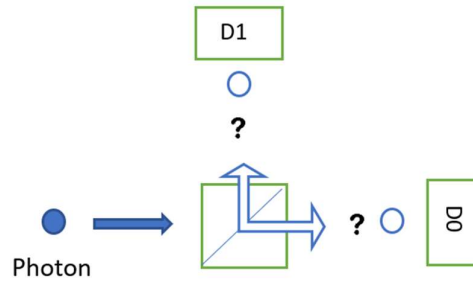


Abbildung 2.2: Zufällige Entscheidung am Strahlteiler. Ein einzelnes Photon kann mit Detektor 0 (D0) oder Detektor 1 (D1) detektiert werden. Bei welchem Detektor es ankommt bleibt bis zum Zeitpunkt der Messung ungewiss.

Durchläuft ein einzelnes Photon einen Strahlteiler, so hat dieses den quantenmechanischen Zustand $|\psi\rangle$

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|1_T\rangle |0_R\rangle + |0_T\rangle |1_R\rangle). \quad (1)$$

Nach dem Strahlteiler kann das Photon als Superpositionszustand im Ausgang „Photon transmittiert“ $|n_T\rangle$ und „Photon reflektiert“ $|n_R\rangle$ beschrieben werden. Mit $|n\rangle$ wird der Photonenanzahlzustand im jeweiligen Ausgang des Strahlteilers beschrieben. Beim idealen Strahlteiler wird das Photon mit einer Wahrscheinlichkeit von 0.5 je Detektor gemessen. Den Detektoren werden jeweils die Bitwerte 0 und 1 zugeordnet (Hildebrandt, 2002, Fürst, 2011).

2.3 Lichtquelle

Ein wichtiger Bestandteil im Experiment ist die Lichtquelle. Für den Quantenzufallszahlengenerator eignet sich entweder eine Einzelphotonenquelle oder ein Laser, der anschließend sehr stark abgeschwächt wird. In dieser Arbeit wird ein abgeschwächter Laser verwendet.

Eine Einzelphotonenquelle wäre ideal für den Versuch, kommt jedoch aufgrund des technisch hohen Aufwands und hoher Kosten für das Schülerlabor nicht in Frage.

2.3.1 Stimulierte Lichtemission

Das Akronym LASER steht für „Light Amplification by Stimulated Emission of Radiation“, d. h. Lichtverstärkung durch stimulierte Emission von Strahlung. Die Lichtemission kann einerseits spontan oder induziert erfolgen. Bereits 1916 beschreibt Albert Einstein die stimulierte Emission als Umkehrung der Absorption (Eichler und Eichler 2015). Die spontane Emission erfolgt ohne äußere Einwirkung (meist bei herkömmlichen Lichtquellen, wie z.B. einer Glühlampe). Hingegen wird für Laser die induzierte Emission, die durch ein Photon stimuliert wird, genutzt: Ein Photon trifft auf ein angeregtes Atom. Wenn die Energie des Photons der Anregungsenergie des Atoms entspricht, wird das Atom zur Emission eines weiteren identischen Photons stimuliert. Dabei zerfällt das Atom in einen niederenergetischen Zustand (Walther und Walther 2010).

Die Verstärkung des Lichtstrahls und der Austritt aus dem Medium wird durch den Resonator bestimmt (siehe Abbildung 2.3 a). Der Resonator hat zwei parallel zueinander aufgestellte Spiegel, wobei einer teildurchlässig ist. Zwischen den Spiegeln befindet sich das Lasermedium, welches ein Gas, Festkörper oder eine Flüssigkeit sein kann. Um mehr Übergänge aus stimulierter Emission als Übergänge durch Absorption zu schaffen, ist es notwendig, dass sich mehr Atome im angeregten Zustand befinden als im Grundzustand. Dies wird auch Besetzungsinversion genannt und wird durch das sogenannte „optische Pumpen“ realisiert (Tipler et al. 2015).

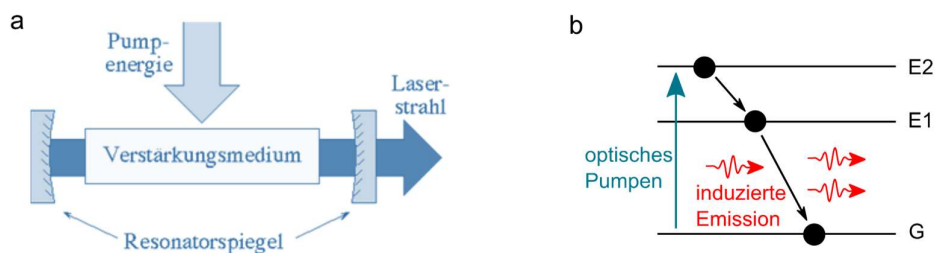


Abbildung 2.3: A, Schematischer Aufbau eines Lasers, mit einem Verstärkermedium (zum Beispiel Festkörper), zwei Resonatorspiegel und einer optischen Pumpe für die Energiezufuhr. B, Energieschema für induzierte Emission. Durch das optische Pumpen werden Atome in ein höheres Energieniveau angeregt. Dadurch kann eine Besetzungsinversion zwischen E1 und G entstehen. Sobald Atome in E1 wieder in den Grundzustand (G) „fallen“, werden Photonen mit gleicher Frequenz und Richtung ausgesendet. Quelle: <https://astro.uni-bonn.de> (a), <http://www.chemgapedia.de> (b)

Beim optischen Pumpen werden Atome durch externe Strahlung (Hilfsstrahlung) in ein höheres Energieniveau E_2 , (siehe Abbildung 2.3 b) „gepumpt“. Nachfolgend gibt es zwei Möglichkeiten: Es entsteht entweder eine spontane Emission beim Übergang zu E_1 oder ein strahlungsloser Übergang (z.B. Stoßprozess oder Auger-Effekt). Von E_1 (E = Energieniveau) aus kann das Atom nach G (= Grundzustand) stimuliert emittieren.

2.3.2 Laserdiode

Eine Laserdiode ist ein Halbleiterbauteil, das Laserstrahlung erzeugt. Die Laserdiode wird durch einen stark dotierten p-n-Übergang mit hohen Stromdichten betrieben. Durch das Einbringen von Donatoren (n), also Atomen mit mehr Valenzelektronen als das Grundmaterial, wird ein Überschuss an Elektronen erzeugt. Im Gegensatz dazu wird bei der Dotierung mit Akzeptoren (p), sprich Atomen mit weniger Valenzelektronen als das Grundmaterial, ein Überschuss an Löchern geschaffen. Durch starke n-Dotierung verschiebt sich die Fermi-Energie nach oben bis ins Leitungsband, und bei einer starken p-Dotierung nach unten bis ins Valenzband. Solche (dotierten) Halbleiter werden für Laserdioden verwendet (Eichler und Eichler 2015).

Die Emission von Licht entsteht durch Rekombination der Elektronen und Löchern am p-n-Übergang. Die Endflächen des Bauelements sind (teil-) reflektierend und bilden somit einen optischen Resonator, in dem sich eine stehende Lichtwelle ausbildet. Liegt eine Besetzungsinversion vor, wird die induzierte Emission zum dominierenden Strahlungsprozess. Die Laserdiode emittiert Laserstrahlung. Das Erzeugen der Besetzungsinversion findet in Laserdioden durch elektrisches Pumpen statt.

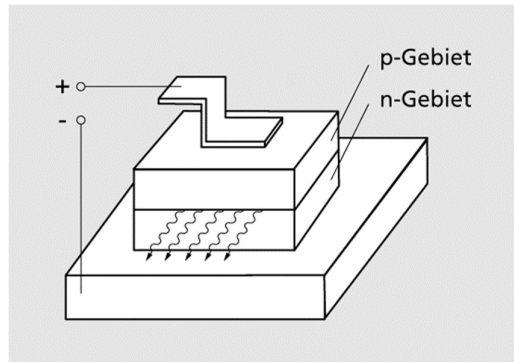


Abbildung 2.4: Darstellung des inneren Aufbaus einer Laserdiode. Durch die angelegte Spannung rekombinieren Löcher (p-Gebiet) und freie Elektronen (n-Gebiet). Die reflektierenden Endflächen bilden einen Resonator. Beim teilreflektierenden Bauelement wird die Laserstrahlung emittiert. Quelle: <https://www.lernhelfer.de/schuelerlexikon/physik>).

2.4 Abschwächung der Laserstrahlung

Die Anzahl an Photonen, die vom Laser ausgesendet werden, ist enorm. Um nur eine geringe und messbare Anzahl an Photonen zu detektieren, wird das Laserlicht durch Absorberplättchen abgeschwächt. Um die geeigneten Filter zu wählen wird der Photonenstrom genauer analysiert und die Photonenstatistik betrachtet.

2.4.1 Photonenstrom

Um den Photonenstrom des Lasers zu bestimmen muss zuerst der Strahlungsfluss Φ_S betrachtet werden. Dieser setzt sich aus der differentiellen Energiemenge dQ (Q =Strahlungsenergie) pro Zeit dt zusammen.

$$\Phi_S = \frac{dQ}{dt}; \quad \text{Einheit } [\Phi_S] = 1 \text{ W} \quad (2)$$

Der Photonenstrom ist die Anzahl der Photonen pro Zeit ($\phi = \frac{dN}{dt}$). Für (monochromatisches) Laserlicht bildet sich die Strahlungsleistung wie folgt

$$\Phi_P = h * \phi * \nu. \quad (3)$$

Im vorgestellten Aufbau mit einem Laser der Wellenlänge 630 nm, also einer Frequenz von $\nu = 475$ THz, mit konstanter Strahlungsleistung von $\Phi_p = 1$ mW, ist ein mittlerer Photonenstrom von $3,17 \cdot 10^{15}$ pro Sekunde zu erwarten.

2.4.2 Photonenstatistik

Man könnte annehmen, dass allein durch die Abschwächung des Laserstrahls die Abstände zwischen den Photonen groß genug sind, um ein gleichzeitiges Auftreffen mehrerer Photonen auf dem Detektor zu verhindern. Das Verhalten von Photonen lässt sich jedoch nur statistisch beschreiben, weshalb die Photonenstatistik betrachtet wird. Sie stellt einen Spezialfall der Bose-Einstein-Statistik mit unbestimmter Photonenzahl dar (Gross, 2003).

Es können nur einzelne Photonen nachgewiesen werden. Die Zeitpunkte, zu welchen die Photonen detektiert werden, sind stochastisch und ihr statistisches Verhalten wird durch die Lichtquelle bestimmt.

Photonenstatistik eines Lasers

Das Feld eines (Ein-Moden-)Lasers wird durch sogenannte kohärente Zustände $|\alpha\rangle$ beschrieben

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_n \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (4)$$

Hierbei ist α eine komplexe Zahl, die den kohärenten Zustand vollständig definiert. Die meisten Lichtquellen emittieren Photonen gemäß der Bose-Einstein-Statistik.

Demgegenüber betrachtet man die Poisson-Verteilung genau dann, wenn die Emission eines Photons unabhängig von der Emission eines anderen Photons ist, wie beispielsweise beim radioaktiven Zerfall. Diese Unabhängigkeit ist auch dann der Fall, wenn Photonen den Resonator verlassen. Die Poisson-Verteilung beschreibt die Photonenverteilung eines Lasers.

$$\mathcal{P}(n) = \frac{\bar{n}^n \exp(-\bar{n})}{n!}, \text{ mit } n \in \mathbb{N}_0. \quad (5)$$

Hierbei ist \bar{n} die mittlere Photonenzahl. Die Wahrscheinlichkeit, dass n Photonen in einem Zeitintervall emittiert werden, wird durch die Poisson-Verteilung beschrieben. Für die mittlere quadratische Schwankung der Photonenzahl erhält man

$$\sigma^2 = \bar{n}. \quad (6)$$

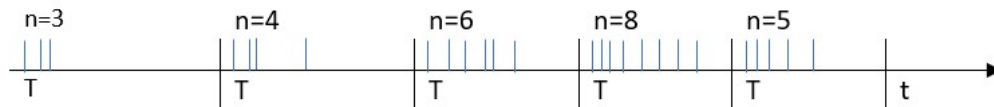


Abbildung 2.5: Zufällige Anzahl an entstandenen Photonen n , innerhalb des Intervalls der Dauer T , bei konstanter Leistung P (Quelle: Saleh und Teich 2008).

Obwohl in Abbildung 2.5 die Leistung konstant ist, ist die Zahl n der Photonen innerhalb eines Intervalls nicht gleichmäßig.

Im Gegensatz zur klassischen Theorie weist auch Laserlicht Fluktuationen in der Leistung auf. Für große Photonenzahlen geht jedoch die relative Schwankung $\frac{\Delta\sigma^2}{\bar{n}^2}$ gegen null.

Photonenstatistik einer thermischen Lichtquelle

Für thermische Lichtquellen (teilweise auch bei Laserdioden), die nur auf einer einzelnen Mode der Frequenz ω schwingen gilt:

Für eine große mittlere Photonenzahl kann die Photonenzahlverteilung, welche mit der Bose-Einstein-Verteilung beschrieben wird, durch die Boltzmann-Verteilung dargestellt werden:

$$\mathcal{P}(n) = \left(1 - e^{-\frac{\hbar\omega}{k_B T}}\right) e^{-\frac{n\hbar\omega}{k_B T}} \quad (7)$$

Bei thermischen Lichtquellen kommt es zu Intensitätsfluktuationen, die als Bunching beschrieben werden. Wenn ein Photon gemessen wurde, ist die Wahrscheinlichkeit höher, kurz darauf wieder ein Photon zu detektieren, als zeitlich später. Beim Effekt des Antibunching hingegen, werden Photonen von der Lichtquelle vollkommen gleichmäßig emittiert. Es entstehen daher keine Schwankungen. Ein Beispiel dafür ist

die Resonanzfluoreszenz eines einzelnen Atoms (Erzeugung von nicht klassischem Licht).

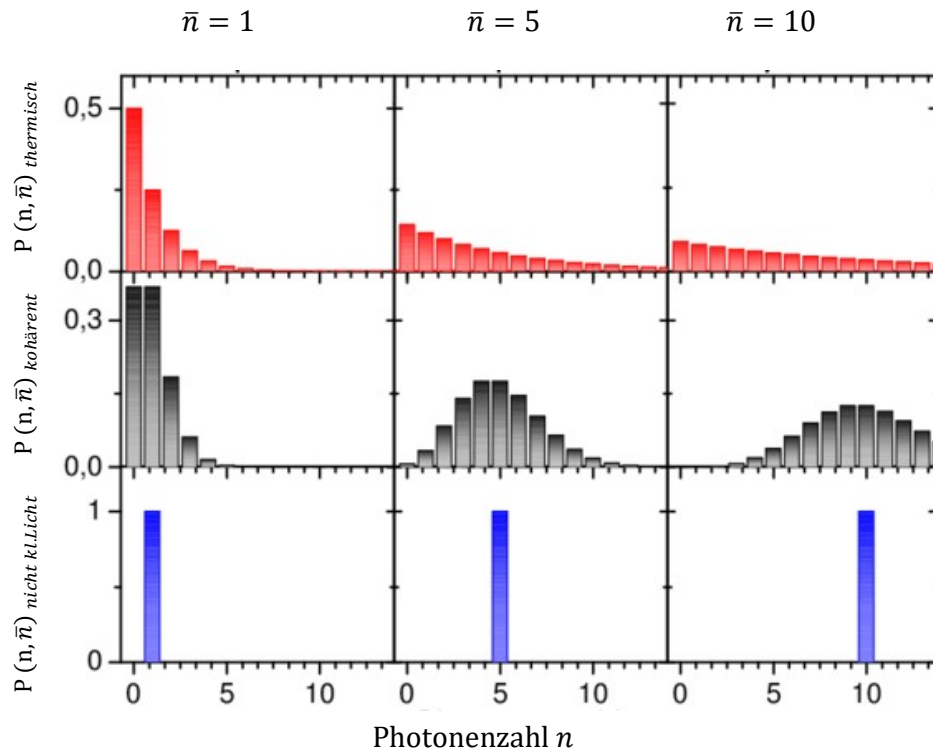


Abbildung 2.6: Es werden die Wahrscheinlichkeitsverteilungen $P(n, \bar{n})$ von drei verschiedenen Klassen von Licht unterschieden: Thermisches Licht (oben), Laserlicht (mittig) und Licht durch eine exakt definierte Anzahl an Photonen (unten). Quelle: <https://www.researchgate.net>

2.5 Detektoren

Nachfolgend werden zwei Optionen für die Detektion von Photonen beschrieben, welche für das Experiment in Erwägung gezogen wurden.

2.5.1 Photomultiplier

Ein Photomultiplier verstärkt das Signal einzelner Photonen. Ein üblicher Photomultiplier besteht aus einer Glasröhre mit einer Photokathode und einem nachgeschalteten Sekundärelektronenvervielfacher (Bronner 2010). Wenn Photonen auf die verbaute Kathode auftreffen, werden Elektronen aus dieser Oberfläche gelöst (äußerer Photoeffekt). Durch den Sekundärelektronenvervielfacher entsteht eine

Vervielfachung von Elektronen, wodurch das Signal des einzelnen Photons verstärkt und kenntlich gemacht werden kann.

Die Quanteneffizienz eines Photomultipliers ist stark von der Wellenlänge der Lichtquelle abhängig. Bei Licht der Wellenlänge 360 nm kann die Quanteneffizienz bei 40 % liegen (Typ Hamamatsu R12199 HQE), wohingegen bei 630 nm diese bei knapp 5 % liegt (Dittmer, 2017).

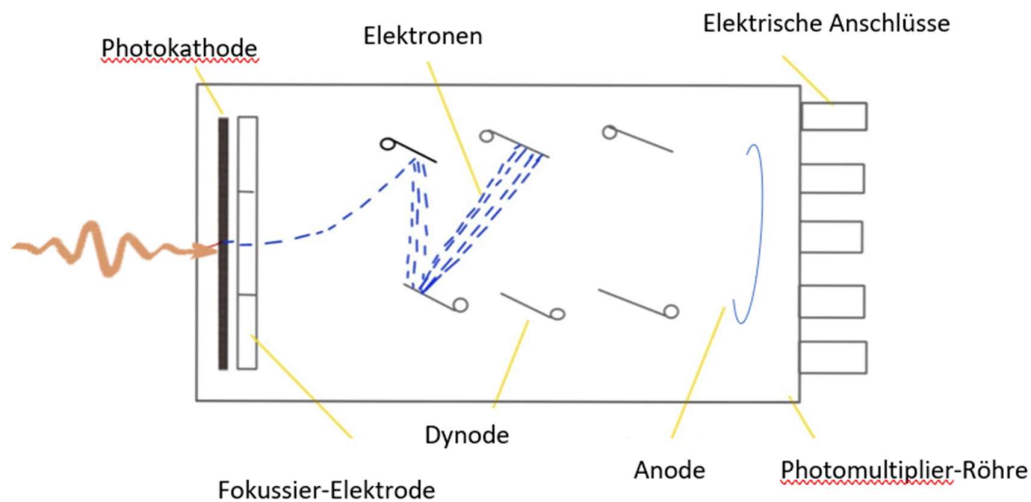


Abbildung 2.7: Darstellung eines Photomultipliers: Photonen treffen auf die Photokathode und lösen dabei Elektronen heraus. Diese Elektronen werden durch ein elektrisches Feld zur Elektrode (Dynode) beschleunigt, um weitere Sekundärelektronen zu erzeugen. Das zuvor schwache Signal der Photonen wird durch die Verstärkung kenntlich gemacht.

Da im Experiment ein Laser mit der Wellenlänge von 650 nm verwendet wird, kommt der Photomultiplier nicht in Frage.

2.5.2 Avalanche-Photodiode

Die Avalanche-Photodiode (kurz: APD) ist ein Bauelement, bei dem bereits ein einziges Photon eine inneren Elektronenlawine auslösen kann. Dadurch wird ein großer Stromimpuls erzeugt, der die Ankunft des Photons auf einem Oszilloskop oder Frequenzzähler anzeigt (Specovius 2018).

Durch eine pin-Struktur (Kombination aus p,i,n-dotiertem Halbleiter) soll die APD die Photonenabsorption maximieren, die Struktur ist in Abbildung 2.8 illustriert.

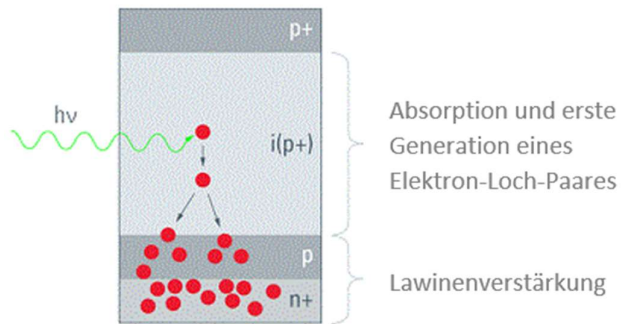


Abbildung 2.8: Schematischer Aufbau (pin-Struktur) einer Avalanche Photodiode und Darstellung des Lawineneffektes, rote Punkte zeigen Elektronen. Quelle: [wwwhttps://www.fau.de/](https://www.fau.de/)

Dabei gilt, dass die Verstärkerregionen dünn sein sollen, um die Wahrscheinlichkeit unkontrollierte Lawinen zu erhalten, zu minimieren. Mit der pin-Struktur können die Absorptions- und Verstärkungsregionen räumlich getrennt werden. Das Photon wird im i-Gebiet absorbiert. Die Photoelektronen driften durch das i-Gebiet in einen pn-Übergang und lösen, aufgrund der Durchquerung des starken elektrischen Feldes und zahlreicher Stöße mit anderen Atomen des Halbleiters, eine Lawine aus. Die in Sperrrichtung angelegte Spannung ist so groß, dass die Sperrschicht sich über die p- bis hin zu p⁺-Schicht erstreckt (Saleh und Teich, 2008).

Bei Avalanche-Photodioden ist zu berücksichtigen, dass ihre Antwort binär erfolgt. Sie können nicht unterscheiden, ob ein, zwei oder mehr Photonen gleichzeitig den Detektor treffen. Nach einem bestimmten Zeitfenster (im Experiment: Totzeit von 22 ns) kann nach einem getroffenen Photon festgestellt werden, ob der Detektor wieder getroffen wurde (Ausgangsspannung $U=1.5\text{ V}$) oder nicht (Spannung $< 1.5\text{ V}$).

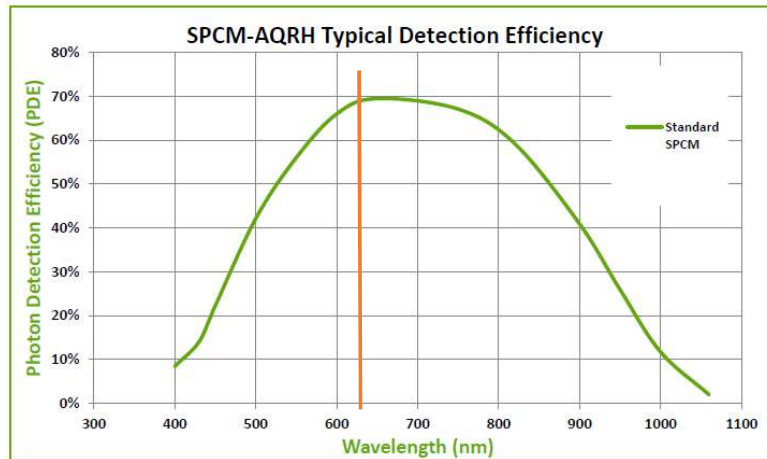


Abbildung 2.9: Effizienz der Photonendektion mit Avalanche-Photodioden (Detektor: SPCM-AQRH).

Der im Experiment verwendete Detektor (SPCM-AQRH) hat bei einer Wellenlänge von 630 nm eine Quanteneffizienz von ca. 70 % (siehe orange Markierung in Abbildung 2.9) und eine maximale Zählrate von 50 MHz.

Das Ausgangssignal weist eine Spannung zwischen 2 und 5 Volt auf und hat eine Pulsbreite von ca. 40 ns, welche mit dem elektronischen Oszilloskop nachgemessen wurde (siehe Abbildung 2.10).

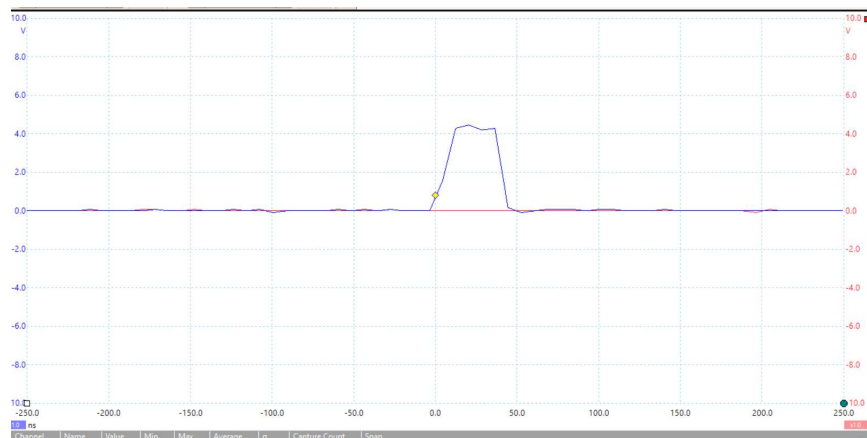


Abbildung 2.10: Detektierte Spannung durch Absorption eines einzelnen Photons.

3. Versuchsaufbau und -durchführung

3.1 Experimenteller Aufbau

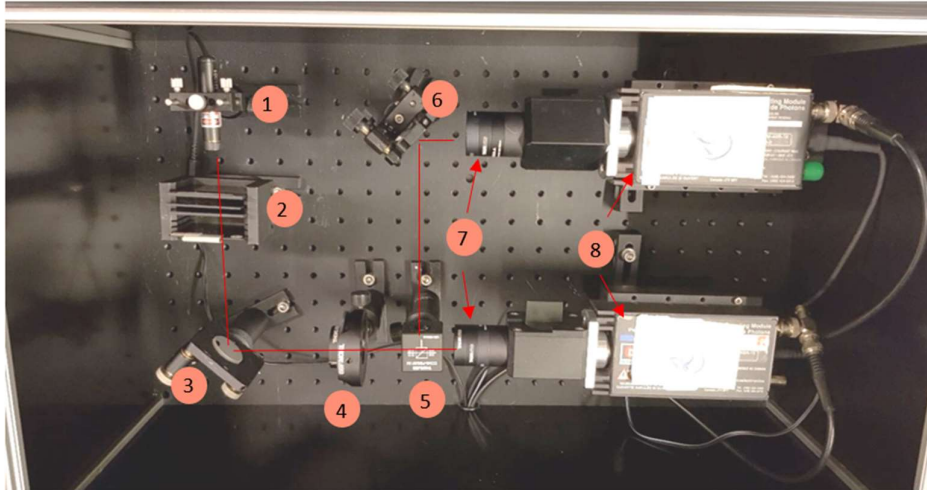


Abbildung 3.1: Versuchsaufbau bestehend aus Laser (1), Absorberplättchen (2+7), Spiegel (3+6), Wellenplatte (4), polarisierenden Strahlteiler (5) und Einzelphotonendetektoren (8) .

In Abbildung 3.1 ist der Versuchsaufbau dargestellt. Für das Experiment wird Laserlicht (1) durch die Absorberplättchen (2) stark abgeschwächt. Zusätzlich sind weitere Absorberplättchen (7) an den Einzelphotonendetektoren (8) angebracht, sodass nur noch vereinzelt Photonen detektiert werden können. Das Photon kann nun am polarisierenden Strahlteiler entweder waagrecht (horizontal) oder senkrecht (vertikal) polarisiert werden, sodass es ein Signal an einem der beiden Einzelphotonendetektoren (8) erzeugt. Der Laser emittiert linear polarisiertes Licht, welches eine bestimmte Vorzugsrichtung hat, in der er stärker polarisiert ist. Aus diesem Grund ist vor dem polarisierenden Strahlteiler (5) eine Wellenplatte $\frac{\lambda}{2}$ (4) positioniert (näheres dazu unter 3.1.2 Wellenplatte).

Der Detektor, der mit Channel A des Oszilloskops (siehe 3.2.1) verbunden ist, wird für die Darstellung der Binärzahl 1 verwendet, der Detektor, der mit Channel B verbunden ist, für die Binärzahl 0. Da man nicht weiß bei welchem Detektor das Photon ankommt, besteht die Möglichkeit eine Binärzahlenfolge zu erreichen, die nicht vorhergesagt werden kann, somit zufällig ist. Die Funktion der Einzeldetektoren (8) ist unter 2.5.2 beschrieben.



Abbildung 3.2: Der Versuchsaufbau wird gegen Hintergrundlicht abgeschirmt, um so das Signal-zu-Hintergrund-Verhältnis zu verbessern.

Der Versuch ist in einer lichtdichten Box aufgebaut. Diese wird mit einem Deckel verschlossen, um bei der Aufnahme der Messreihe keine weiteren Photonen von der Umgebung zu erfassen.

Zur Anzeige und Datenerfassung der Photonensignale am Detektor wird ein USB-Oszilloskop mit entsprechender Software (abhängig vom Hersteller) verwendet (Führinger, 2012). Diese können nur in Verbindung mit einem PC oder Laptop gelesen werden.

3.1.1 Polarisierung

Licht als elektromagnetische Welle wird mit elektrischen und magnetischen Feldern, die senkrecht zur Ausbreitungsrichtung oszillieren (=Transversalwelle), beschrieben. Das Licht, das nur eine Schwingungsebene hat, nennt man polarisiertes Licht.

Laserlicht ist polarisiert, da das Licht durch Anisotropien (zum Beispiel bei unterschiedlicher Absorption im Material oder Reflektivität an den Resonatorspiegeln) eine Polarisationsmode bevorzugt, welche immer weiter verstärkt wird.

3.1.2 Wellenplatte

Eine Wellenplatte ist ein optisches Bauelement. Sie ist notwendig, um bei Licht die Phase und die Polarisierung zu verändern. Verzögerungsplatten (Wellenplatten) sind

meist dünne Schichten aus doppelbrechenden Kristallen. Wenn Licht durch ein Medium transmittiert, regt es die Moleküle im Material aufgrund des Verhaltens wie Hertz'sche Dipole, zum Schwingen an. Normalerweise schwingen diese in dieselbe Richtung wie auch die elektromagnetische Welle (Bahr et al. 2015).

Wenn aber ein Lichtstrahl auf einen Kristall mit unsymmetrischen Strukturen trifft, wird der Lichtstrahl in zwei senkrecht zueinander polarisierte Teilstrahlen getrennt. Dies entsteht aufgrund der unterschiedlichen Brechungsindizes, welche abhängig von der Anisotropie des Kristalls sind (Bahr et al. 2015). Man nennt die Teilstrahlen auch ordentlicher und außerordentlichen Strahl (siehe Abbildung 3.3).

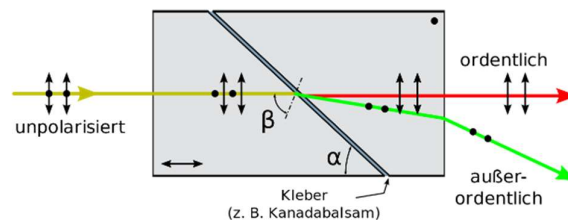


Abbildung 3.3: Schematische Darstellung der Doppelbrechung, bei dem unpolarisiertes Licht in einem Kristall in ordentlichen (hier grün) und außerordentlichen Strahl (hier rot) aufgespalten wird. Quelle: https://de.wikipedia.org/wiki/Polarisator#/media/Datei:Wollaston_Prism_DE.svg

Gebräuchlich sind Platten mit Verzögerungen von einer halben Wellenlänge ($\lambda/2$ -Platten) und einer viertel Wellenlänge ($\lambda/4$ -Platten). Diese Verzögerung bezieht sich auf eine bestimmte Wellenlänge. Da im Experiment, Licht der Wellenlänge 630 nm genutzt wird, wird eine Wellenplatte $\lambda/2$ verwendet (Phasenplättchen, 2014).

3.1.3 Strahlteiler

Ein Strahlteiler ist ein teildurchlässiger Spiegel, bei dem ein Teil des einfallenden Lichtes transmittiert und der Rest reflektiert wird. Er spaltet somit den Strahl in zwei Teilstrahlen auf. Die Eingangsoberfläche eines Strahlteilers ist mit einer dünnen dielektrischen Beschichtung bedampft, welche das Teilungsverhältnis bestimmt. Auf der Rückseite besitzen die Strahlteiler eine Breitbandentspiegelung, die Sekundärreflexionen fast vollständig verhindert.

3.1.4 Polarisierender Strahlteiler

Bei einem polarisierenden Strahlteiler teilt sich der Lichtstrahl in einen reflektierten vertikal polarisierten und einen transmittierten horizontal polarisierten Strahl auf.

Dies gelingt durch Brechung in einem anisotropen Kristall. Mithilfe des anisotropen Kristalls entstehen sowohl eine ordentliche Welle als auch eine außerordentliche Welle. Weil sie in unterschiedlichen Winkeln gebrochen werden, werden sie räumlich voneinander getrennt und sind entgegengesetzt polarisiert (Saleh und Teich 2008) (siehe Abbildung 3.4).

Eine weitere Möglichkeit für einen polarisierenden Strahlteiler ist eine dielektrische mehrlagige polarisierende Beschichtung im Strahlteilerwürfel.

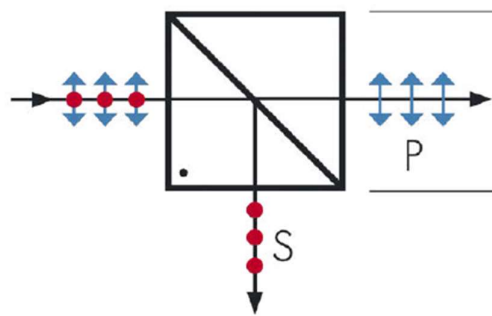


Abbildung 3.4: Schema eines polarisierenden Strahlteilers. S stellt den horizontal (senkrecht) polarisierten Lichtstrahl und P den vertikal (parallel) polarisierten Lichtstrahl dar. Quelle: <https://photonlexicon.com>

Für das Zufallsexperiment ist eine diagonale, also gleichmäßig horizontale und vertikale, Polarisation vor dem polarisierenden Strahlteiler nötig. Da Laser, wie bereits in 2.3 erwähnt, eine bestimmte Vorzugsrichtung in ihrer Polarisation haben, ist es notwendig eine Wellenplatte vor dem Strahlteiler zu platzieren. Die Wellenplatte verändert die Polarisationsrichtung des Lasers. Damit kann die Detektionswahrscheinlichkeit der beiden Detektoren an den Ausgängen des polarisierenden Strahlteilers näherungsweise gleich eingestellt werden (Hildebrandt, 2002).

3.1.5 Einzelphotonendetektor

Beim Ausführen des Experiments trifft ein schwacher Strom von Photonen auf eine lichtempfindliche Oberfläche (siehe Abbildung 3.5). Da diese mit $20\ \mu\text{m} \times 20\ \mu\text{m}$ sehr klein ist, wird der Laserstrahl mit kinematischen Spiegeln (3, 6 in Abbildung 3.1) auf diese justiert. Der Strahldurchmesser ist größer als die sensitive Fläche des Detektors. Daher werden nicht alle Photonen detektiert, was allerdings keinen Einfluss auf die Binärfolge hat.

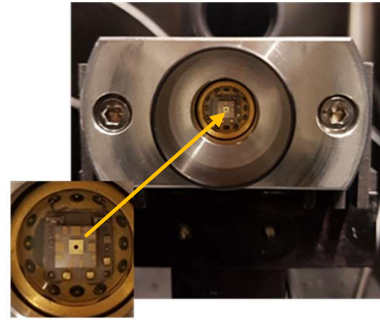


Abbildung 3.5: Bild des Einzelphotonendetektors mit einer sensitiven Fläche von $20\ \mu\text{m} \times 20\ \mu\text{m}$.

3.2 Signalaufnahme

3.2.1 Photonendetektion mit Oszilloskop

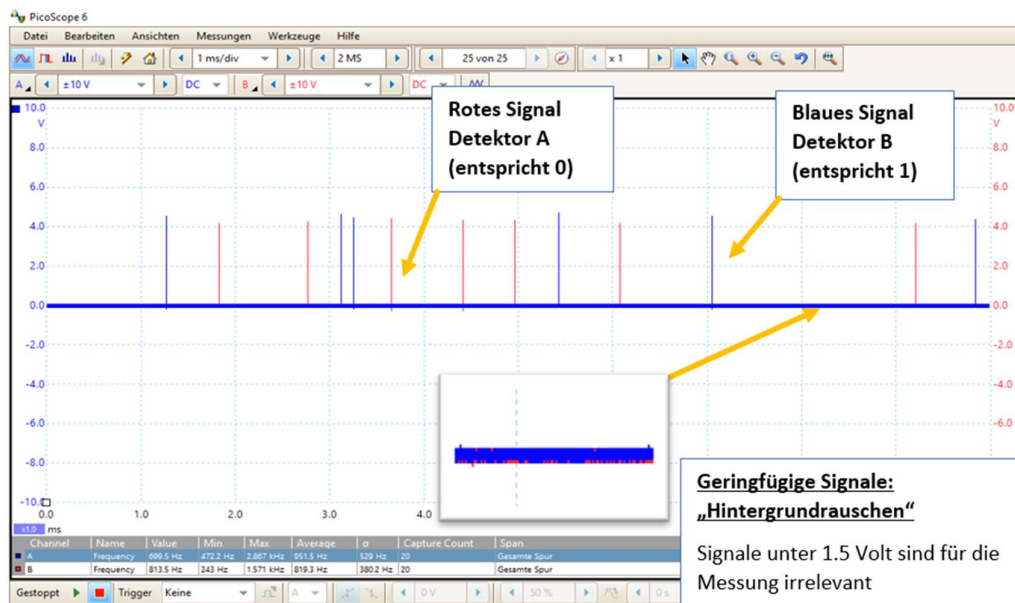


Abbildung 3.6: Signalaufnahme vom Oszilloskop mit der Software PicoScope 6.

Durch das USB-Oszilloskop können die Signale beider Detektoren ausgewertet werden. Für das Experiment wird das Pico 2207B USB-Oszilloskop mit zwei Kanälen gewählt. Dieses bietet die Möglichkeit einer digitalen Speicherung an, welche in

Kapitel 4 und 5 relevant wird. Eine Darstellung der Anzeige des USB-Oszilloskops ist in Abbildung 3.6 gezeigt. Rote Peaks entsprechen dem Signal aus Channel A, welches damit als Detektor A bezeichnet wird. Bei blauen Peaks gilt dasselbe, diese werden daher Detektor B zugeordnet. Die Anstiegsflanken der Peaks, die während des Zeitfensters eintreffen, werden gezählt und in Relation zur Dauer des Zeitfensters gesetzt. Hieraus wird die Frequenz des Eingangssignals errechnet. Beträgt das Zeitfenster beispielsweise 1s und werden in diesem Zeitfenster 48789 Impulse gezählt, ist die Frequenz 48789 Hz. Je länger das betrachtete Zeitfenster ist, desto genauer wird das Messergebnis, näheres dazu unter Abschnitt 2.4.2 (Photonenstatistik). Die Frequenz liefert die sogenannte „Klickrate“, also die „Anzahl detektierter Photonen pro Zeit“.

Um als Signal gewertet zu werden, müssen die Peaks einen bestimmten Schwellenwert überschreiten. Der Schwellenwert im Experiment liegt bei 1.5 V. Signale unter diesem Wert werden auch als elektrisches Hintergrundrauschen bezeichnet und sind nicht mit Hintergrundphotonen zu verwechseln.

Um das Photonensignal vollständig aufzulösen, muss die Abtastrate des Oszilloskops hoch genug gewählt werden. Dies garantiert, dass jedes detektierte Photon zur Auswertung benutzt wird.

Für die Auswertung der Photonensepulse wird ein bestimmtes Zeitfenster (hier 1 ms pro Division) festgelegt. Mit insgesamt 10 Divisionen ergibt dies ein Gesamtzeitfenster von 10 ms. Die Gesamtzeit wird so gewählt, dass die gewünschte absolute Anzahl an Binärzahlen mit der gegebenen Klickrate erreicht wird. Die Abtastrate ergibt sich dann aus diesem Gesamtzeitfenster und der Anzahl an Datenpunkten. Um die Photonensignale mit einer Länge von 40 ns vollständig aufzulösen, wird eine Abtastrate von maximal 8 ns pro Punkt angestrebt. Daraus ergibt sich eine Anzahl an Datenpunkten von mindestens 1.25 MS. Im Experiment wurden daher 2 MS gewählt (dies entspricht eine Samplerate 200 MS/s).

3.2.2 Binärdarstellung

Durch das USB-Oszilloskop beziehungsweise die PicoScope Software werden die Photonensignale bisher als Spannungspulse sichtbar gemacht. Die beiden Detektoren werden durch den Channel-Anschluss am USB-Oszilloskop kenntlich, jedoch fehlt die Umwandlung zu Binärzahlen, mit der die Zufallszahlen letztendlich erzeugt werden. Jeder Spannungspuls, genauer gesagt deren steigende Flanke, wird als binäres Event gezählt. Um die Messergebnisse umzuwandeln ist es dann nur noch notwendig festzulegen, welcher Detektor die Binäre „0“ und welcher die „1“ darstellt. Die Reihenfolge der ankommenden Signale am Oszilloskop legt dann die zufällige Binärzahlenfolge fest. In Abbildung 3.6 erhält man zum Beispiel die folgende Binärkette:

1001100010101

Damit die Zufallszahlen tatsächlich auch zufällig sind, ist es wichtig, dass das Detektorverhältnis jeweils nahe bei 50% liegt. Überprüft wird dies mit den Ereignisraten der Detektoren, diese müssen gleich sein (siehe Abbildung 3.7).

Im Experiment liegen sie für beide Detektoren im Bereich von 500 kHz und hatten eine Abweichung von $\pm 10\%$. Dem Ereignis, bei dem in beiden Detektoren gleichzeitig ein Photon detektiert wird, kann kein Bitwert zugeordnet werden. Diese Events werden daher nicht berücksichtigt.

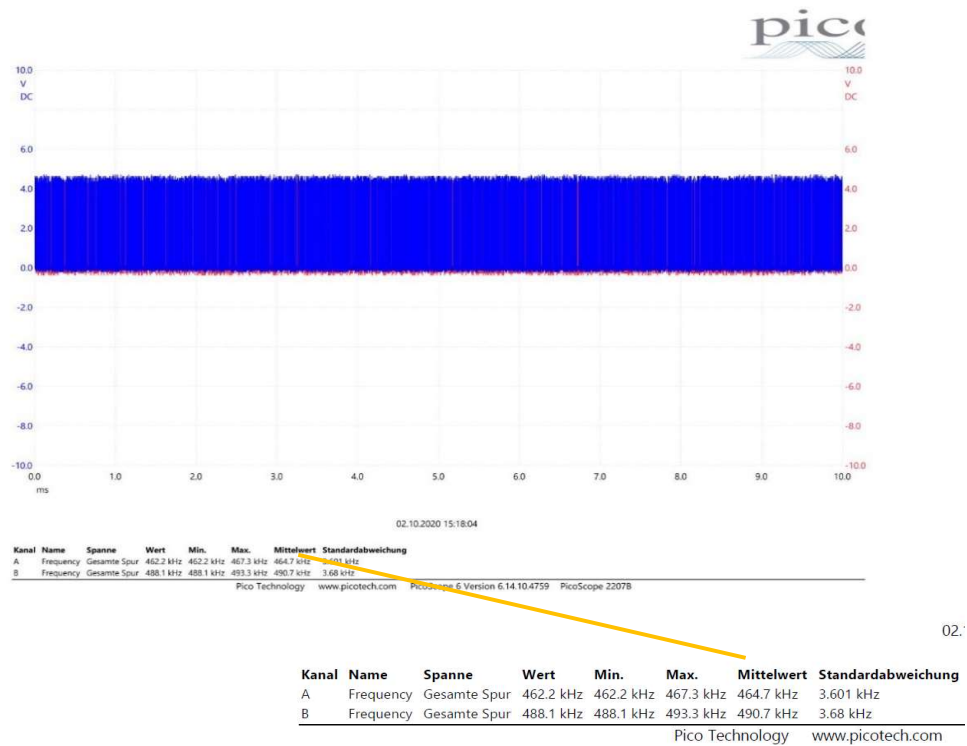


Abbildung 3.7: PicoScope Messanzeige, mit dem Fokus auf einen ähnlichen Mittelwert beider Detektorsignale.

3.3 Austausch des Strahlteilers

Zu Beginn bestand das Experiment aus einem einfachen Strahlteiler. Hierbei zeigte sich jedoch, dass trotz sehr genauer Justage des Laserstrahls, die Messwerte auf den Detektoren nicht gleichmäßig aufgeteilt waren. Die Verluste können aus dem Aufbau oder weiteren (unbekannten) Faktoren resultieren.

Durch den Austausch mit dem polarisierenden Strahlteiler und der Wellenplatte, welche eine gleichmäßige Polarisationsausrichtung vor dem Strahlteiler aktiv (durch das Drehen der Wellenplatte) ermöglicht.

Nach dem Austausch zeigten sich deutlich bessere Messwerte. Außerdem war der Einsatz der Wellenplatte ein zusätzliches Element, womit den Schülerinnen und Schülern die gleichmäßige Intensitätsverteilung für das Detektorverhältnis, nähergebracht werden konnte, näheres dazu unter Abschnitt 5.5 (Anleitung für das Experiment).

4. Testung der Zufallszahlen

Um Zufallszahlen auf ihre Güte zu überprüfen sind unterschiedliche Tests möglich. Einige bekannte und einfache Tests, wie die Berechnung von Pi nach der Monte-Carlo-Methode, der Monobit Test sowie der Run-Test der NIST Test Suite (National Institute of Standards and Technology), wurden für diese Arbeit näher untersucht (U.S. Department of Commerce, 2014). Diese drei genannten Tests eignen sich nach Bronner (2010) gut für Ausbildungszwecke, näheres in Kapitel 5.

Photonen, die in beiden Detektoren gleichzeitig detektiert werden, sogenannte Koinzidenzen, werden keinem Bitwert zugeordnet. Dies wurde bei der Programmierung (zur Auswertung der Tests) mit der Software GNU Octave berücksichtigt.

4.1 Bestimmung von Pi

Allgemein benutzt man die Monte-Carlo-Methode, um den Inhalt von Körpern und Flächen mit unregelmäßiger Begrenzung oder in großen Raumdimensionen zu berechnen.

Bezogen auf den Kreis, kann die Kreiszahl Pi mit der Monte-Carlo-Methode approximiert werden. Um das Vorgehen dieser Methode zu verstehen, beachtet man die Formel zur Berechnung des Flächeninhalts eines Kreises ($A_E = r^2 * \pi$).

Das Verhältnis des Flächeninhalts des Kreises wird durch die (zufällig) verteilten Punkte angenähert. Nun wird ein Punkt mit zufälligen Koordinaten ermittelt und in den Raum, den die Begrenzungsfläche (Quadrat) einschließt, gesetzt. Danach wird über das Verhältnis Pi angenähert

$$\frac{\text{Anzahl der Punkte im Kreis}}{\text{Anzahl der Punkte im Quadrat}} = \frac{\text{Fläche des Kreises } (r^2 * \pi)}{\text{Fläche Quadrat } ((2 * r)(2 * r))}$$

$$\rightarrow \pi = 4 * \frac{\text{Anzahl der Punkte im Kreis}}{\text{Anzahl der Punkte im Quadrat}}$$

Wenn der Abstand vom Koordinatenpunkt zum Kreismittelpunkt kleiner als der Kreisradius ist, so liegt der Punkt innerhalb, wenn er größer ist, dann liegt er außerhalb.

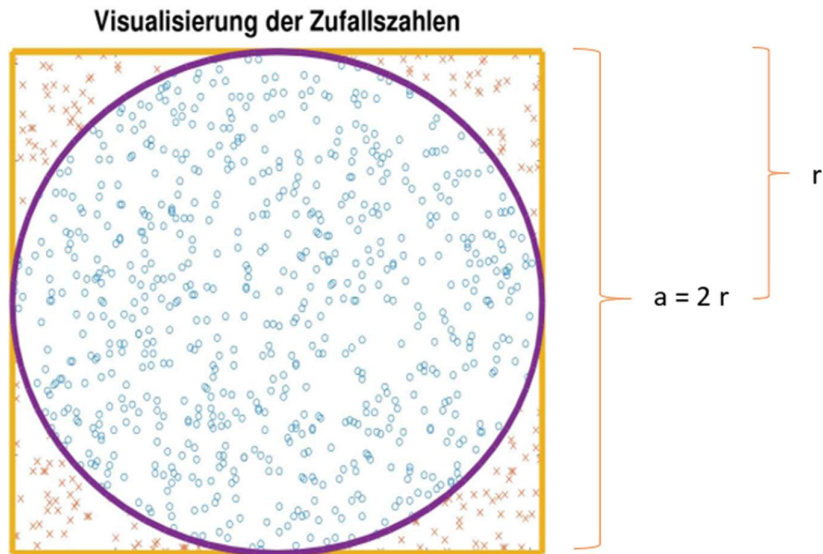


Abbildung 4.1. Beliebige Punkteverteilung im Quadrat (Seitenlänge $a=2 r$) mit zugehörigem Kreis (Kreisradius r).

Zur Berechnung von Pi werden aus der binären Bitfolge Koordinatenpaare erzeugt. Die Anzahl der Bits pro Koordinate bestimmt wie feinmaschig das Koordinatensystem ist, und damit auch wie genau Pi bestimmt werden kann. Zum Beispiel ergeben 10 Bits pro Koordinate eine Gesamtzahl von $2^{10} = 1024$ Abschnitten. Hierbei sind 10 Bits ein guter Kompromiss aus der Genauigkeit von Pi und der benötigten Anzahl an Zufallszahlen. Die Berechnung nach der Monte-Carlo-Methode ist dabei wie oben gezeigt radius- und damit auch koordinaten-unabhängig.

Aus der Messreihe konnte Pi bis auf $(3,18 \pm 0,11)$ angenähert werden. Der Fehler wurde anhand der statistischen Abweichungen von 10 Messergebnissen ermittelt.

4.2 Chi-Quadrat-Test

Der Chi-Quadrat Test überprüft, ob die beobachtete Verteilung der erwarteten Verteilung entspricht. Der Chi-Quadrat Test lässt sich folgendermaßen unterteilen:

- Der **Anpassungstest** überprüft, ob die Daten, die man erhebt, einer bestimmten Verteilung (z.B. Normalverteilung) unterliegen
- Beim **Homogenitätstest** vergleicht man mindestens zwei Stichproben, um festzustellen, ob sie einer homogenen Grundgesamtheit entstammen.
- Mit dem **Unabhängigkeitstest** wird überprüft, ob es bei der Verteilung zusätzliche Einflussmerkmale gibt, welche die Verteilung beeinflussen könnten. Es wird überprüft, ob zwei Merkmale stochastisch unabhängig sind.

Um zu überprüfen, ob die bei der Verteilung gemessenen Einsen und Nullen von der gewünschten Verteilung abweichen, wird der Anpassungstest für die Auswertung der Daten verwendet.

4.2.1 Chi-Quadrat Anpassungstest

Man betrachtet ein statistisches Merkmal X , dessen Wahrscheinlichkeit in der Grundgesamtheit unbekannt ist. Bezüglich der Wahrscheinlichkeit von X wird eine Null- und Alternativhypothese aufgestellt.

- $H_0(k)$:= (die Zahlen aus) X sind (weitgehend) gleichverteilt
- $H_1(k)$:= (die Zahlen aus) X sind **nicht** gleichverteilt

Voraussetzung für den Chi-Quadrat Test ist, dass der Zufallszahlengenerator eine Folge unabhängiger Ereignisse erzeugt. Das heißt, dass das vorherige Ergebnis eines Ereignisses keinen Einfluss auf das darauffolgende nimmt.

m Beobachtungen x_1, x_2, \dots, x_m der Zahlen X werden in k verschiedene Klassen eingruppiert. Als erstes muss bestimmt werden, wie viele Beobachtungen (im Mittel) in einer Klasse zu erwarten sind. Hierzu wird die Wahrscheinlichkeit p_i , dass eine Ausprägung von X in die Klasse i fällt, entsprechend der Nullhypothese berechnet. Die unter H_0 zu erwartende Häufigkeit wird wie folgt bestimmt:

$$n_{E_i} = p_i * m. \quad (8)$$

Mit n_{E_i} wird die erwartete Häufigkeit einer Klasse bezeichnet. Für jede Klasse i der möglichen Werte wird das Abstandsquadrat zwischen der empirischen Anzahl x_i und dem Erwartungswert $m * p_i$ gebildet. Die Werte aller Kategorien werden anschließend aufsummiert. Mathematisch ist die Bildung des Chi-Quadrat-Wertes in Gleichung 9 aufgeführt.

$$\chi^2 = \sum_{i=1}^k \frac{(x_i - m * p_i)^2}{m * p_i} \quad (9)$$

Um Ergebnisse des χ^2 -Werts beurteilen zu können, ist es notwendig die theoretische χ^2 -Verteilung mit $k-1$ Freiheitsgraden zu betrachten. Sie wird herangezogen, um die Varianz einer Stichprobe von den normalverteilten Zufallsgrößen anzunähern.

Besonders seltene Ereignisse erhalten bei diesem Test eine starke Gewichtung. Liegen die realen Werte nahe an den theoretischen Werten, ist die Nullhypothese wahrscheinlich. Weichen die Werte hingegen stark ab, so wird die Nullhypothese abgelehnt. Um zu definieren, ab wann Werte zu stark abweichen werden, wird als Prüfgröße die Quantile betrachtet.

4.2.2 Quantile

Die Quantile gehört zu den Lagemaßen der Statistik. Sie teilen eine bestimmte Menge an Daten nach p und $1-p$ auf. Für die Quantile wird die normierte quadrierte Abweichung über alle „Klassen“ aufsummiert. Die Annahme der Nullhypothese H_0 erfolgt, wenn

$$\chi^2 > \chi^2_{(1-\alpha, k-1)}, \quad (10)$$

$k-1$ sind die Freiheitsgrade und α das Signifikanzniveau. Mit α beschreibt man die Wahrscheinlichkeit, in der die Nullhypothese fälschlicherweise verworfen wird, obwohl sie eigentlich zutreffend ist (Fehler erster Art oder α -Fehler).

Beim Chi-quadrat Test gibt es Fehler erster und zweiter Art. Bei einem Test können unterschiedliche Fälle auftreten, denen entsprechende Wahrscheinlichkeiten zugeordnet werden.

1. Wenn H_0 wahr ist und H_0 trotzdem verworfen wird, begeht man einen Fehler 1. Art. Die Wahrscheinlichkeit dafür ist α . Die Wahrscheinlichkeit, dass bei Gültigkeit von H_0 die Hypothese H_0 akzeptiert wird, ist $1 - \alpha$.
2. Wenn H_0 falsch ist und die Hypothese trotzdem akzeptiert wird, begeht man einen Fehler 2. Art.

Wenn ein Messwert stark vom Erwartungswert E abweicht und dabei einen kritischen Wert überschreitet, nimmt man an, dass die Nullhypothese H_0 nicht korrekt ist und lehnen sie zugunsten der Alternativhypothese H_1 ab. Diesen „kritischen Wert“ $\chi^2_{(1-\alpha, k-1)}$ bezeichnet man letztendlich als Quantile. Numerische Werte für χ^2 sind im Anhang A.1 auf Seite 51 abgebildet.

Der kritische Wert mit der dazugehörigen (beidseitigen) Fläche α wird beispielhaft in 4.2 dargestellt:

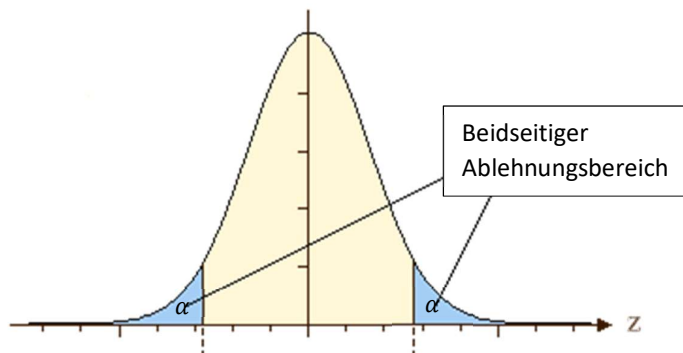


Abbildung 4.2. Mit α beschreibt man die Wahrscheinlichkeit, in der die Nullhypothese fälschlicherweise verworfen wird, obwohl sie eigentlich zutreffend ist. Die beidseitige Betrachtung des Ablehnungsbereichs findet Anwendung für Tests, die auf Gleichverteilung prüfen. Quelle: <https://www.physik.uni-wuerzburg.de>

4.2.3 Anwendung auf binäre Zufallszahlen

Ein ausführlicheres Beispiel soll verdeutlichen, warum ein Chi-quadrat Test für die Auswertung der Güte von Zufallszahlen verwendet wird.

Es gibt zwei Klassen ($i = \{1, 2\}$, $k=2$) und $m=100$ Beobachtungen ($x_1, x_2, \dots, x_{m=100}$). Die Wahrscheinlichkeit für das Auftreten eines 1-Bits / 0-Bits ist jeweils 0,5.

In einem Versuch kann die Verteilung wie folgt aussehen:

10101001001010111100	(10 x 1-Bit)
01100010101010100111	(10 x 1-Bit)
10000101111001010100	(9 x 1-Bit)
11111010100001010000	(9 x 1-Bit)
00010101010100001111	(9 x 1- Bit)

In diesem Abschnitt ergeben sich 47 1- Bit und 53 0-Bit. Für die Hypothese der Gleichverteilung von 1en und 0en muss nicht nur die Wahrscheinlichkeit für jede Klasse ($p_E = 1/2$), sondern auch die zu erwartende Häufigkeit betrachtet werden. Man stellt folgende Hypothesen auf:

- $H_0(k)$:= (die Zahlen aus) X besitzen die (theoretische) Wahrscheinlichkeitsverteilung von $p_0 = p_1 = 1/2$,
- $H_1(k)$:= (die Zahlen aus) X besitzen **nicht** die theoretische Wahrscheinlichkeitsverteilung von $p_0 = p_1 = 1/2$,

Das Signifikanzniveau α wird auf 10 % festgelegt.

Es gilt:

$$\chi^2(1) = \sum_{i=1}^k \frac{(x_i - m * p_i)^2}{m * p_i} = \frac{(47 - 50)^2}{50} + \frac{(53 - 50)^2}{50} = 0,36. \quad (11)$$

Für $df = k-1 = 1$ Freiheitsgrade ist der empirische Wert von 0,36 über dem Grenzwert $\chi^2_{(0,1;1)} = 0,02$ (siehe Tabelle im Anhang A. 1). Weil also $\chi^2 > \chi^2_{(0,1;1)}$ vorliegt, muss die Hypothese der Gleichverteilung (mit $\alpha = 10\%$) **abgelehnt** werden. Nullhypothese auf Gleichverteilung trifft nicht zu.

Der χ^2 – Wert kann zur Ereignisselektion und zur Abtrennung genutzt werden. Alternative Hypothesen können unter Umständen zu ähnlichen α –Werten führen.

Und obwohl der Wert im Beispiel 4.2.3 mit $\chi^2(1) = 0,36$ verhältnismäßig klein ist und keine allzu große Varianz vorliegt, zeigt es wie bedeutend die Anzahl der Klassen i bei diesem Test sind. Bei Binärfolgen gibt es nur zwei Klassen. Man beschränkt sich

nur auf Nullen und Einsen, und kann den χ^2 – Test nur mit einem Freiheitsgrad 1 betrachten. Um die Zufallsfolgen im Experiment nicht auf einen Freiheitsgrad zu beschränken, wird die Binärfolge in Bits zusammengefasst. Man betrachtet nun die Verteilung natürlicher Zahlen (einschließlich Null). Speziell für die Auswertung wurden Zahlen von 0 – 64, das heißt 8 bits, dessen Gleichverteilung beispielhaft in Abbildung 4.3 dargestellt ist.

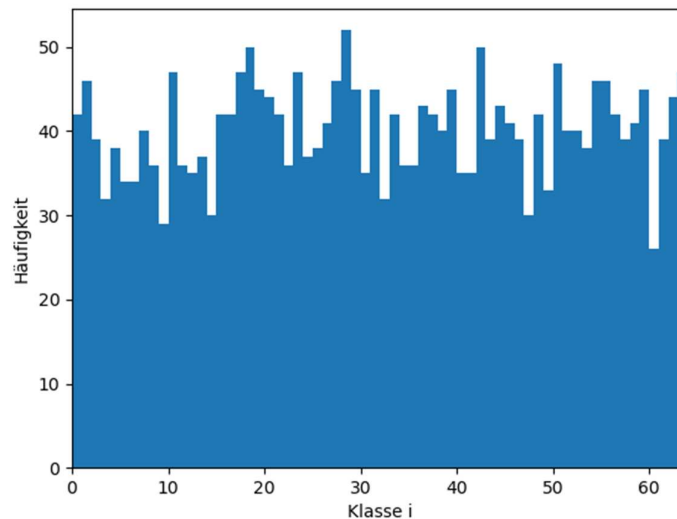


Abbildung 4.3: Beispielhaftes Histogramm einer Messung der Häufigkeit einzelner Klassen i , welche einen Wertebereich von 0 bis 64 abdecken. Sie zeigt, dass mit einer 90 prozentigen Wahrscheinlichkeit die Gleichverteilung der Werte gegeben sind.

Ergebnisse

Für die Auswertung wurden folgende Parameter beachtet:

- Detektionssignale kleiner 1.5 V werden nicht berücksichtigt (Schwellenwert < 1.5V)
- Beim χ^2 -Test wird das Signifikanzniveau von $\alpha = 10 \%$ getestet, bei Freiheitsgrad 63. Der χ^2 -Wert hierfür lautet $\chi^2_{(0,1;63)} = 49,11$.

Der empirische χ^2 -Wert lag bei 48,16. Weil also $X^2 < X^2_{(0,1;63)}$, vorliegt kann die Hypothese der Gleichverteilung (mit einem Signifikanzniveau $\alpha = 10 \%$) **angenommen**

werden. Anders ausgedrückt, die Nullhypothese trifft mit einer Wahrscheinlichkeit von 90 % zu.

4.3 Kettenlängentest

Beim Kettenlängentest überprüft man die Zufallszahlen nach der Häufigkeit von gleichbleibenden Bitsequenzen (Runs) (U.S. Department of Commerce 2014). Man betrachtet die Anzahl der vorhandenen Ketten der Länge x aus einer Binärzahlenfolge. Nach Fürst (2011) ist für den Erwartungswert der Verteilung $X_{0/1}^x$ diese unter der Annahme gleichverteilter Zufallszahlen gegeben durch:

$$E(X_{0/1}^x) = \left(\frac{1}{2}\right)^{x+2}, x \in \mathbb{N}_0 \quad (12)$$

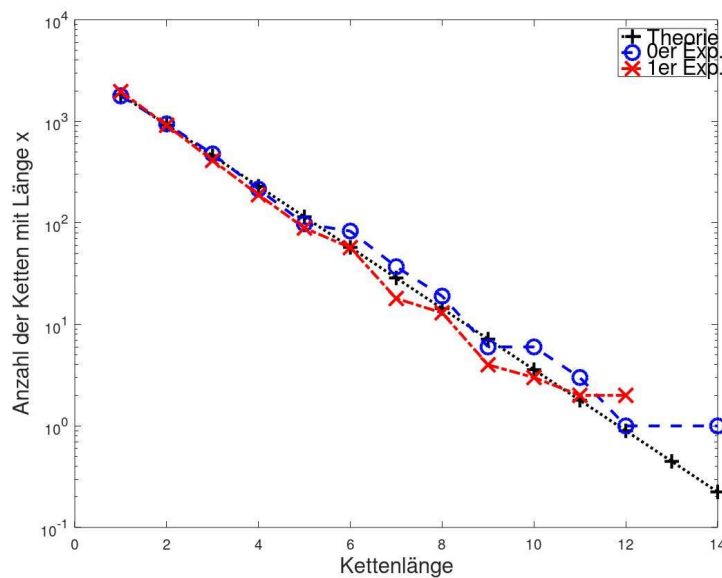


Abbildung 4.4: Häufigkeit der Kettenlängen bei einer einzelnen Messung. Der rote Graph beschreibt die Häufigkeiten bestimmter Längen für Einsen und der blaue Graph für Nullen. Wie sich die Häufigkeit theoretisch entwickelt stellt der schwarze Graph dar, Gleichung (13).

Die Wahrscheinlichkeit für eine einzelne 0 oder 1 liegt bei 0,5 (bei einem idealisiert betrachteten Zufallszahlengenerator) und halbiert sich für jede darauffolgende (gleiche) Zahl und folgt letztendlich der Formel (12) für Kettenlängen der Länge x . Um die Gesamtzahl aller vorhandenen Ketten zu berücksichtigen wird die Formel (12) mit der Länge der gesamten Bitfolge n multipliziert.

$$E(X_{0/1,n}^x) = \left(\frac{1}{2}\right)^{x+2} * n, \quad x \in \mathbb{N}_0, n \in \mathbb{N} \quad (13)$$

Die Anzahl der Ketten in Abhängigkeit der Länge x ist in Abbildung 4.4 dargestellt. Die theoretische Verteilung ist ebenfalls gekennzeichnet.

Für eine deutlichere Darstellung werden die Werte logarithmisch aufgetragen, bzw. der Logarithmus aus den y -Werten gebildet. Dadurch ergibt sich statt der exponentiell abfallenden Funktion aus Gleichung (13) eine Gerade.

$$\begin{aligned} \log_2 E(X_{0/1,n}^x) &= \log_2(2^{-x} * n) \\ &= -x * \log_2(2) + \log_2(n) \\ &= -x * \log_2(n) \end{aligned} \quad (14)$$

Darüber hinaus wird eine Geradenregression für die Häufigkeit der Kettenlängen (Einserketten und Nullerketten) erstellt. Beispielweise ergeben sich folgende Werte für die Regression der Ketten, welche grafisch in Abbildung 4.5 dargestellt sind

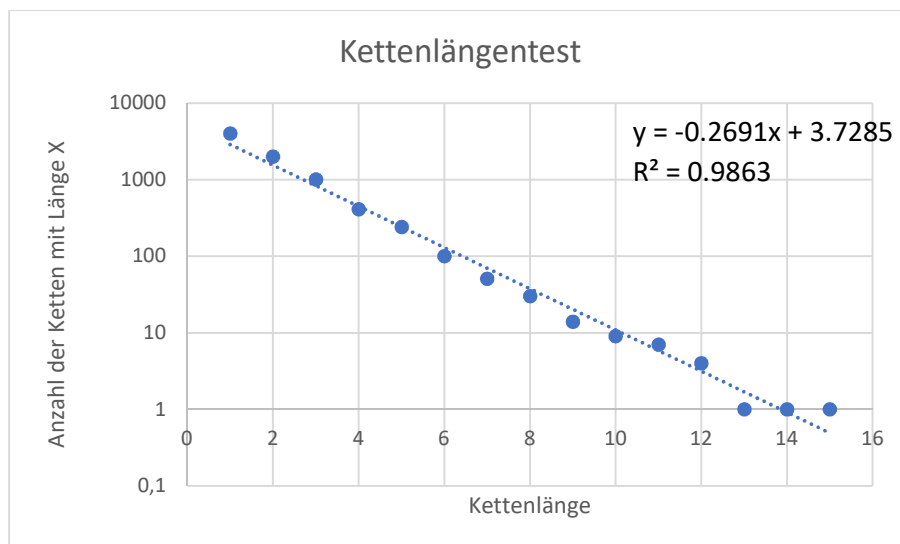


Abbildung 4.5: Beispielhafte Darstellung eines Kettenlängentest einer einzelnen Messung. Mit der Geraden beziehungsweise der indirekten Proportionalität wird der lineare Zusammenhang der Häufigkeit der vorkommenden Kettenlänge deutlich.

R^2 stellt den pearsonschen Korrelationskoeffizienten in quadrierter Form dar. Dieser Korrelationskoeffizient ist ein Maß, welches die Güte des linearen Zusammenhangs angibt. R^2 kann Werte zwischen 0 und 1 annehmen, wobei 1 für einen vollständig linearen Zusammenhang zwischen den betrachteten Merkmalen steht.

Ergebnisse

Es wurden 10 Experimente mit jeweils circa 10.000 Zufallszahlen untersucht. Der gemittelte Korrelationskoeffizient lag bei $R^2 = (0,973 \pm 0,008)$. Der Fehler wurde anhand der Abweichung von 10 Messergebnissen gemittelt.

4.4 NIST Analyseprogramm

Bei der NIST Test Suite handelt es sich um 15 einzelne Tests, die es zulassen Aussagen zu treffen, ob die Zufallszahlen nicht zufällig sind. Dabei werden beispielsweise beim Monobit Test der Anteil der Einsen/Nullen in einer Bitkette (Bitstrom) auf $\frac{1}{2}$ überprüft. Je nach Bitfolgenlänge und festgelegten Signifikanzniveau ist eine größere oder kleinere Abweichung von $\frac{1}{2}$ in Ordnung (Haahr 2020). Ein weiterer Test der NIST Suite ist der sogenannte Run-Test. Dieser prüft die Zufallszahlen auf das Fehlen von langen und ununterbrochenen Folgen von Nullen oder Einsen, da es oft bei künstlich erzeugten Zufallszahlen vorkommt, dass diese einen stärkeren Wechsel von Nullen und Einsen aufweisen. Jedoch kann bei echten Zufallszahlfolgen auch mal (wenn auch selten) eine siebenstellige gleiche Folge der gleichen Zahl vorkommen.

Wegen der unterschiedlichen Zielsetzungen der einzelnen Tests ist es sinnvoll mehrere von ihnen zu Überprüfung der Zufallszahlen zu nutzen.

Man sollte dabei beachten, dass eine hohe statistische Qualität der Ergebnisse eines Zufallszahlengenerators nicht die Sicherheit eines Zufallszahlengenerators im Einsatz impliziert. Außerdem wurde das NIST Analyseprogramm vor allem für die Analyse von Pseudozufallszahlen entwickelt. Da die Tests bei der Durchführung im Betrieb keine Rückmeldung über mögliche Fehler geben, wurde für diese Arbeit das NIST Testverfahren nicht durchgeführt.

5. Schülergerechte Integration des Experiments

5.1 Analyse

Es gibt nicht viele Konzepte, die sich mit der Einführung in die Quantenphysik im Unterricht beschäftigen. Ein Älteres, aber auch mehrmals überarbeitetes Konzept, ist das Münchener Unterrichtskonzept zur Quantenmechanik von Rainer Müller und Hartmut Wiesner (2001).

Ein weiteres, speziell für die Implementierung von quantenoptischen Experimenten, bietet die Dissertation von Patrick Bronner (2010) an. Beide Konzepte werden für diese Arbeit kurz vorgestellt.

Es handelt sich bei beiden um Konzepte, welche sich an einer Einführung zur Quantenphysik ab der 10. Klasse orientieren. Sie haben zur Strukturierung der entwickelten Schüleranleitung (siehe Anhang A.2) beigetragen.

5.1.1 Münchener Unterrichtskonzept

Beim Münchener Unterrichtskonzept werden zuerst Photonen mithilfe des Photoeffekts durch das Hallwachs Experiment eingeführt. Durch die Einführung des planckschen Wirkumsquantums werden Energie und Impuls der Photonen erarbeitet. Anschließend werden dynamische Eigenschaften, wie die Aufteilung in einem Strahlteiler und die Polarisation berücksichtigt. Vor Einführung der Quantenphysik sind Schülerinnen und Schüler folgende Beschreibungen von Licht bekannt:

Zum einen wird Licht als Lichtstrahl modelliert, um Phänomene wie Brechung oder Reflexion zu erklären. Später werden Wellenphänomene, also Beugung und Interferenz verdeutlicht. Sobald man Photonen als Lichtteilchen einführt, gilt es zu beachten, dass Schülerinnen und Schüler bereits diesen Prozess (Lichtstrahl, Lichtwelle) durchlaufen sind. Sie haben bereits Vorstellungen von Licht entwickelt und diese teilweise auch experimentell erfahren.

Deshalb thematisiert das Münchener Unterrichtskonzept die Inferenz vieler einzeln ausgesendeter Photonen am Doppelspalt, um somit eine Verbindung zum Welle-

Teilchen-Dualismus herzustellen. Dabei wird versucht, den Schülerinnen und Schüler zu verdeutlichen, dass die Quantentheorie nur statistische Aussagen treffen kann. Nach Müller und Wiesner werden dann die Eigenschaften von Elektronen und diese als Quantenobjekte beschrieben. Zum Schluss werden die SuS zur Heisenbergsche Unbestimmtheitsrelation sowie zur Schrödinger-Gleichung herangeführt.

5.1.2 Erlanger Konzept

Das Erlanger Konzept ist spezifisch auf die Implementierung der Quantenoptik im Unterricht ausgerichtet. In der Dissertation von Bronner, 2010 wird ein Unterrichtskonzept vorgestellt, das zu Beginn eine Motivationsphase zur Quantenphysik berücksichtigt.

Dabei sollen die Schülerinnen und Schüler Fragen beantworten, die gleichzeitig ihr Vorwissen und ihre Vorstellungen zur Quantenphysik anregen, wie beispielsweise „Was weiß ich über die Quantenwelt?“ oder „Wie stelle ich mir ein Quantenobjekt vor“. Als nächstes soll die Detektion von Licht besprochen werden, zuvor werden Begriffe, wie Wellenlänge und Intensität wiederholt. Durch ein Demonstrationsexperiment soll die Wahrnehmung von Licht im Auge verdeutlicht werden, um den Schülerinnen und Schülern ein Gefühl dafür zu geben, dass Licht weitaus mehr ist als die Wahrnehmung es zulässt. Mit einem interaktiven Experiment, welches in seiner Arbeit nicht näher beschrieben wird, werden Einzelphotonendetektoren erklärt. Danach wird in dem Konzept die Einzelphotonenquelle mithilfe der Photonenstatistik thematisiert.

Die Schülerinnen und Schüler erarbeiten die Eigenschaften von Strahlteiler und diskutieren, weshalb es sinnvoll sein kann, dass ein Photon unteilbar ist. Mit diesem Vorgehen will Bronner auf den Quantenzufall hinführen. In einem Lernzirkel sollen die Schülerinnen und Schüler sich intensiver mit dem Thema Zufall auseinandersetzen, dabei sollen sie sich mit dem deterministischen Zufall (z. B. Münzwurf), computergenerierten Zufall (z.B. logarithmische Formeln) und dem Zufallsprozess einzelner Photonen am Strahlteiler beschäftigen.

Zum Schluss wird die Interferenz einzelner Photonen besprochen und die Reflexion, die aufzeigen soll, dass das Verständnis für die Quantenphysik oft kontraintuitiv ist und es keine klare Vorstellung hierfür gibt.

5.1.3 Einordnung der Konzepte

Beim Erlanger Konzept ist unter anderem unklar, weshalb zuerst die Detektion von einzelnen Photonen beschrieben wird und danach erst die Einzelphotonenquelle. Die Einzelphotonenquelle ist für Schülerinnen und Schüler deutlich anspruchsvoller, weshalb eine starke Abschwächung von Laserlicht als eine möglich Alternative verwendet werden könnte. Des Weiteren erschweren stochastische Themen nach Müller (2011) (Müller 2011) Schülerinnen und Schüler den weiteren Zugang zur Quantenphysik, welche in diesem Konzept bereits nach der 3. Unterrichtsstunde (Photonenstatistik), wenn auch qualitativ, erwähnt werden. Dass die SuS den deterministischen und computergenerierten vorab erarbeiten, um an den Quantenzufall anzuknüpfen, wird aus dem Konzept für die Anleitung übernommen. Von Wiesner und Müller wird das beschriebene Vorgehen zur Aufteilung am Strahlteiler und die Polarisierung übernommen, da es verständlich und gut strukturiert aufbereitet ist.

5.2 Konzept für die Schüleranleitung

Unter Anlehnung an die unter 5.1.1 und 5.1.2 besprochene Konzepte, wurde die Schüleranleitung für den Quantenzufallszahlengenerator erstellt. Sich an alle Unterrichtssequenzen der Konzepte zu orientieren ist für eine Schüleranleitung, die in maximal einer Stunde bearbeitet werden muss, nicht möglich, dennoch wurde versucht eine ähnliche Struktur zu übernehmen.

In Anlehnung an Muckenfuß (1995) erhalten die SuS zur Motivation für die Erzeugung von Zufallszahlen Informationen zur Kryptographie.

„Ein fachlicher Inhalt kann immer nur in einem für Schülerinnen und Schüler relevanten Kontext gelernt werden. Deshalb sollte der Kontext so gewählt werden, dass er für die Lernenden „sinnstiftend“ ist.“ (Muckenfuß, 1995)

Für den Einstieg sollen die SuS ein Gefühl für selbst erzeugte Zufallszahlen bekommen. Im Labor steht deshalb eine Box mit 100 Binärwürfeln, die sie schütteln sollen um damit ihre selbsterzeugte Binärfolge zu erhalten.



Abbildung 5.1: Würfelbox (Würfel mit Binärzahlenschrift). Sie soll von den SuS zu Beginn des Experiments als physikalischer Zufallszahlengenerator genutzt werden, und anschließend als erste Reflexion zur Güte von Zufallszahlen hinführen.

Den SuS wird der Kettenlängentest nähergebracht, um qualitativ bewerten zu können, wie zufällig ihre gewürfelte Zufallszahl tatsächlich ist. Am Beispiel der Wahrscheinlichkeit für mindestens eine 4er – Kette (Nullen oder Einsen) bei 100 Würfeln, sollen die SuS erkennen, dass das Vorkommen von „Lange Ketten (> 3)“ für „gute“ Zufallszahlen sehr wahrscheinlich sind (natürlich in Abhängigkeit der Gesamtlänge der Zufallszahl). In diesem Beispiel liegt sie bei ca. 95% (näheres dazu Kapitel 5.5 Schüleranleitung). Danach wird auf die Grenzen vom Würfeln eingegangen, um zu erklären, dass auch diese Zufälligkeit ihre praktischen Grenzen hat.

Häufig werden computergenerierten Zufallszahlen zur Verschlüsselung von Daten genutzt. Deshalb werden sie in diesem Zusammenhang für die SuS kurz thematisiert. Dabei soll den SuS schnell deutlich gemacht werden, dass es sich bei computergenerierten Zufallszahlen, um sogenannte Pseudozufallszahlen handelt und somit nicht um „echte“ Zufallszahlen.

Da das Thema Zufall ohnehin schon komplex ist und dieses in einer kurzen Zeit von den SuS erarbeitet werden soll, sind in der Anleitung strukturierende Elemente berücksichtigt (siehe Abbildung 5.2).

Zufallszahlerzeugung: Übersicht

Anbei eine kleine Übersicht zu den bisherigen Themen
Zufallszahl erzeugen

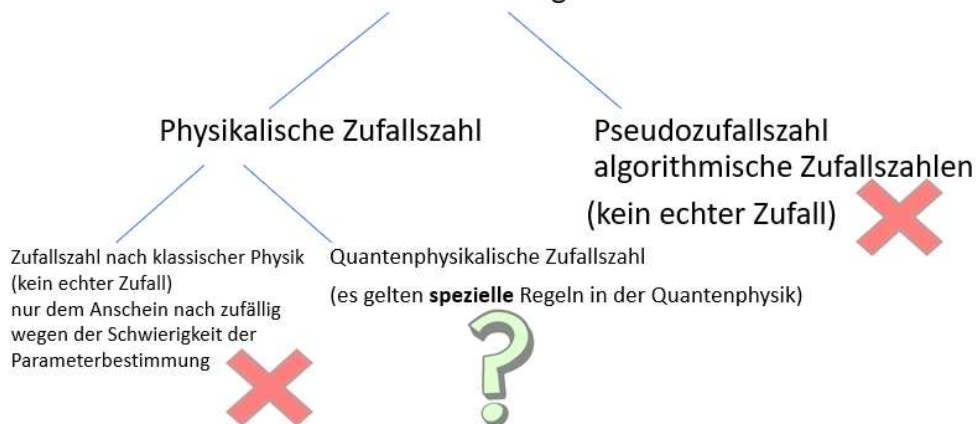


Abbildung 5.2: Orientierungsfolie aus der Schüleranleitung. Sie soll den SuS das bisher erarbeitete (Pseudozufallszahlen, und physikalisch (mittels Würfel) erzeugte Zufallszahlen als Wiederholung aufzeigen und auf das nächste Kapitel quantenphysikalische Zufallszahlen hinweisen.

Nachdem die SuS die Nachteile der mit dem Würfel erzeugten und der computergenerierten Zufallszahlen erkannt haben, beschäftigen sie sich mit der Quantenphysik. Zuerst wird auf die Grundlagen eingegangen, dabei wird der Welle-Teilchen-Dualismus thematisiert, der eine besondere Hürde für SuS darstellt (Müller und Wiesner (2001)). Um Fehlvorstellungen von Licht zu vermeiden, soll nach Kirchner Licht als Teilchen vermieden werden (Kircher und Schneider 2003). Bei beiden (Licht als Welle oder Licht als Teilchen) handelt es sich um eine Modellierung, die dabei helfen soll, einen komplexen Sachverhalt zu vereinfachen und zugänglich zu machen. Deshalb wurden in dieser Anleitung beide Bezeichnungen verwendet, jedoch mit der Transparenz, dass es sich um eine Modellierung handelt, die versucht Lichtphänomene zu beschreiben.

Nach Duit (1995) verschaffen Analogien Vertrautheit und Verknüpfungen zu Bekanntem, welches für aufbauendes Lernen im Physikunterricht besonders relevant ist (Duit 1995). Um diesen Aspekt in der Anleitung zu berücksichtigen wird versucht, die Superposition anhand vom Strahlteiler in Analogie zur Schrödingers Katze

hervorzuheben, welche ursprünglich von Schrödinger (1935) zur Verdeutlichung der Verschränkung eingeführt wurde.

Mit der Analogie soll den SuS vor allem gezeigt werden, dass quantenphysikalische Phänomene in der Alltagswelt nicht beobachtet werden können, dennoch existieren.

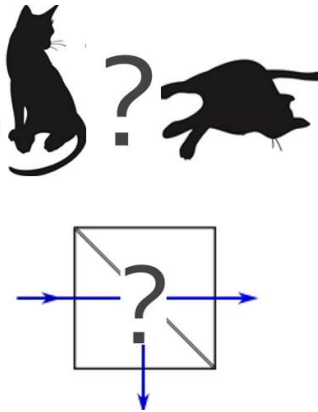
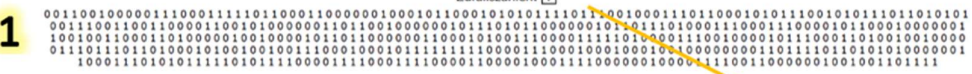


Abbildung 5.3: Abbildung aus der Schüleranleitung. Für die Analogiebildung der Superposition am Strahlteiler wird Schrödingers Katze verwendet. Mit der Analogie soll den SuS vor allem gezeigt werden, dass quantenphysikalische Phänomene in der Alltagswelt nicht beobachtet werden können. Quelle: <https://www.google.de/url?sa=i&url=http%3A%2F%2Fwww.mathisintheair.org>
https://commons.wikimedia.org/wiki/File:Beam_splitter.svg,

Sobald die SuS die Grundlagen erarbeitet haben, dürfen sie sich mit dem Versuch vertraut machen und diesen durchführen. Um die Zufallszahlen und die spätere Analyse der Zufallszahlen anschaulich und schülergerecht darzustellen, wurde eine Maske in Zusammenarbeit mit Stefan Langenfeld in Python programmiert, welche in Abbildung 5.4 dargestellt ist.

Quantenzufallsgenerator

Zufallszahlen: [?]

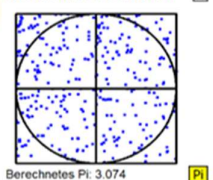
1 

2 **Detektor Verhältnis** [?]

A: B:

55 : 45

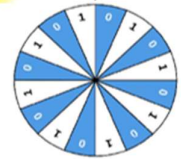
3 **Kreiszahl Pi bestimmen** [?]



4 **Kettenlängentest** [?]

Länge	Anzahl
[1]	664
[2]	291
[3]	131
[4]	67
[5]	30
[6]	13
[7]	0

5 **Glücksrad** [?]



6 [?]

Abbildung 5.4: Schülermaske, welche die SuS (Schülerinnen und Schüler) zur Bearbeitung des Experiments nutzen. In (1) sehen die SuS die Zufallszahlen in Binärdarstellung. In der Anleitung (sowie Fragezeichenkästchen) wird erklärt, welcher Detektor binär 1 und binär 0 darstellt. Das Detektorverhältnis wird prozentual für die SuS in (2) ersichtlich. Welche Rolle das Detektorverhältnis für die Qualität der Zufallszahlen spielt aber auch generelle Erklärungen/Erläuterungen zu den einzelnen Bereichen, werden den SuS über „Fragezeichenkästen“ erklärt (6). Die Berechnung von Pi (3) nach der Monte-Carlo-Methode und die qualitative Betrachtung des Kettenlängentest (5) soll den SuS bei der Analyse der Zufallszahlen helfen. Mit dem Glücksrad (5) können die SuS ihre individuelle Zufallszahl bilden (Rotationsgeschwindigkeit vom Glücksrad wird mittels der Zufallszahlen bestimmt).

Es wurden Elemente wie Fragezeichentools berücksichtigt, um den SuS eine gute Orientierung bei der Analyse der Zufallszahlen und beim Experiment zu schaffen. Durch Start/Reset erhalten die SuS neue Zufallszahlen, die sie immer weiter optimieren können, indem sie die Wellenplatte verstellen (siehe Kapitel 5.5, Schüleranleitung). Die Funktion der Wellenplatte ermöglicht bei Schülerinnen und Schülern einen direkten Bezug zur Analyse der Zufallszahlen.

5.3 Bildungsplan

Nach dem aktuellen Lehrplan werden an bayerischen Gymnasien die Grundlagen der Quantenphysik ab der 10 Klassen unterrichtet. Speziell die Eigenschaften von Photonen, sowie die Vertiefung findet erst in den darauffolgenden Jahrgangsstufen statt. Um SuS, welche noch in der Sekundarstufe I sind, die Freude und Faszination der Quantenphysik näher zu bringen, orientiert sich die Schüleranleitung an SuS mit wenig Vorwissen im Bereich der Quantenphysik.

5.4 Testung anhand einer Stichprobe

Das Experiment mit der Schüleranleitung konnte nicht von SuS Vorort getestet werden. Deshalb wurde ein digitales Konzept entwickelt, um eine Rückmeldung über das Schülerverständnis zum Experiment und vor allem der Anleitung, zu erhalten. Es wurde ein sogenanntes „Stummes Video“ aufgenommen, welches die SuS vertonen/verskripten sollten.

Da nur wenig SuS bereit waren ein Stummes Video (siehe 5.4.1) zu vertonen/verskripten, musste das Konzept des „stummen Videos“ etwas verändert werden. Mit e-learning H5P wurde ein *interaktives Video* mit anschließendem Quiz erstellt. Dabei sollten die SuS gezielte Verständnisfragen beantworten. Mittels der Schülerlaboranleitung und einer Anleitung, welche mit der Autorenumgebung für H5P umgesetzt wurde.

H5P ist eine freie und quelloffene Software zum Erstellen von interaktiven (Lern)-Inhalten für das Web. Es ist an bayerischen Schulen zugelassen. Die Lerninhalte stehen auf allen Endgeräten (Smartphone, Tablet, PC) zur Verfügung.

Der Link zum Bearbeitungstool und die Anleitung wurden an die SuS versendet (Link H5P: <https://h5p.org/node/1047391>). Mittels einer Summary-Seite (mit erreichten Punkten), die zum Ende der Bearbeitung angezeigt wird, wurde der Lernfortschritt der SuS deutlich (Beispiel Summary siehe Abbildung 5.5). Die Summary-Seite haben die SuS per E-Mail weitergeleitet (siehe im folgenden Abschnitt Ergebnisse).

Die erreichten Punkte werden hier angezeigt (im Beispiel sind es 0 von 13 Punkten).

Abbildung 5.5: Beispielhafte Darstellung eines Summaries auf H5P. Für die Bearbeitung der Fragen zum Quantenzufallszahlengenerator mittels Anleitung und Video sollen die SuS Fragen zum Versuchsaufbau beziehungsweise den Komponenten und der anschließenden Versuchsdurchführung beantworten. Die SuS beantworten Fragen zum Vorgehen, der Justage und der Analyse der ermittelten Zufallszahlen. Die erreichten Punkte werden in der oberen Leiste aufgeführt.

5.4.1 Stummes Video

Im Physikunterricht kommt die Bearbeitung von sogenannten Stummen Videos noch selten vor. Ihre Bearbeitung bietet jedoch eine gute Rückmeldung für die Lehrenden. Es kann zeigen, ob sich die SuS intensiv mit dem Versuch auseinandergesetzt haben, indem man erkennt, ob sie die korrekte Fachsprache verwenden, die Versuchskomponenten und den Versuchsablauf beschreiben. Nach Herrn Schweinberger (Mitarbeiter der LMU Physikdidaktik) und Experte bei der Erstellung von „Stummen Videos“, gilt es einige Punkte zu beachten:

- Versuchsaufbau soll in Leserichtung
- Hintergrund neutralisieren (Ablenkung vermeiden)

- Mögliche Skizze oder die Einzeichnung des Strahlengangs verdeutlichen komplexe Sachverhalte
- Abschnittsweise fokussierte Aufnahme

Unter diesen Punkten wurde das „Stumme Video“ für den Quantenzufallszahlengenerator erstellt. Anschließend wurde ein H5P-Link entwickelt, mit dem die SuS das Stumme Video interaktiv mittels der Anleitung erarbeiten können.

Ergebnisse

Anhand einer Stichprobe von 10 Schülerinnen und Schülern aus den Jahrgangsstufen 10-12 aus dem Gymnasium und der Fach- / Berufsoberschule (FOS/BOS), wurden durchschnittlich 12,6 Punkte von insgesamt 13 Punkten erreicht.

5.5 Anleitung für das Experiment

siehe Anhang A.2

A.2 Schüleranleitung

Die Schüleranleitung, welche für das Schülerlabor entwickelt wurde, folgt in den darauffolgenden Seiten.



1

Verschlüsselung durch Zufallszahlen



FACEBOOK UND WHATSAPP
Die geheime Macht der Metadaten
Sichere Kommunikation ist nur eine Seite der Medaille.
Was Facebook und Whatsapp trotzdem über uns wissen.
Michael Spehr
13.09.2010, 16:00 Uhr

<https://www.faz.net/aktuell/wirtschaft/thema/verschlueselung>

Die Verschlüsselung von Informationen ist von großer Bedeutung in der heutigen Kommunikationstechnologie, da sie einen sicheren Austausch von Daten ermöglicht. Die dabei verwendeten **Zufallszahlen** müssen hohen Anforderungen genügen. Sie müssen optimalerweise „echt“ zufällig sein. (Chen et al. 2011).

13. November 2019, 11:25 Uhr Verschlüsselung bei Smartphones
Sicher telefonieren mit dem Krypto-Handy

2

```
10110000110110001111101101110110001010000000111
00010110000110110001111101101110110001010000000
11000011011000111110110111011000101000000011100
01100011111011011101100010100000001110000110001
00011011000111110110111011000101000000011100001
01100001101100011111011011101100010100000001110
```

Unser Ziel: Gute Zufallszahlen selber erzeugen!

```
11000011011000111110110111011000101000000011100
10000110110001111101101110110001010000000111000
00110110001111101101110110001010000000111000011
01100001101100011111011011101100010100000001110
00101100001101100011111011011101100010100000001
10000110110001111101101110110001010000000111000
11000111110110111011000101000000011100001100011
00110110001111101101110110001010000000111000011
```

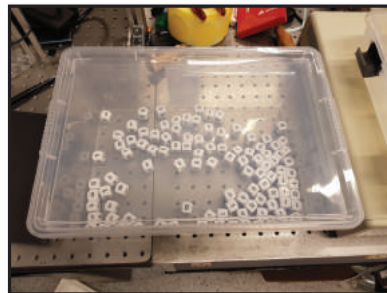
3

Ist ein Würfelexperiment zufällig?

Das ist eine Box mit genau 100 Würfeln. Diese Würfel sind speziell, denn sie haben zwar 6 Seiten, aber es bietet sich als Lösung nur 0 oder 1 an.

Nun schüttelst du die Box, sodass du eine zufällige Folge von Nullen und Einsen, eine sog. **Binärzahlenkette**, erhältst.

Wie zufällig sind die Nullen und Einsen tatsächlich?



4

Kettenlängen-Test: Wie zufällig ist die gewürfelte Binärzahlenkette?

Eine Kette ist ein Block, der aus Ziffern desselben Typs besteht. Er kann auch aus nur einer einzigen Ziffer bestehen.

Beispiel:

00101001000101010100010101000101010010101010110

In Ketten aufgeteilt:

00-1-0-1-00-1-000-1-0-1-0-1-0-1-000-1-0-1-0-1-000-1-0-1-0-1-00-1-0-1-0-1-0-1-0-1-0-11-0

Das Merkmal, mit dem hier **Zufälliges** von **Nicht-Zufälligem** unterschieden werden kann, ist die Länge der längsten Kette.

Bei 100 Würfeln ist die Wahrscheinlichkeit sehr groß, ca. 95 %, dass mindestens 4 Nullen oder 4 Einsen hintereinander vorkommen, also eine Kette der Länge 4 auftritt. (siehe [Glossar](#))

5

Kettenlängen-Test: Wie zufällig ist die zufällig gewürfelte Binärkette? (= Glossar Oberstufler)

Fragen wir uns, wie wahrscheinlich eine Einer-Kette der Länge „mindestens 4“ bei 100 Würfeln ist.

Es ist $1 \leq \text{Lauflänge}$ (hier $4 \leq 100$) in einer Bitfolge der Länge 100 erfüllt, sodass wir nun die Wahrscheinlichkeit berechnen können.

Um die Wahrscheinlichkeit zu bestimmen, teilen wir die 100 Zahlen (0en und 1 en) in 25 4er-Blöcke auf. Nun ist die Wahrscheinlichkeit, dass eine Kette der Länge 4 entsteht genau $2/16$ und dass es **NICHT** passiert, dann $1-2/16=7/8$ (=Gegenwahrscheinlichkeit).



<https://de.freepik.com>

6

Kettenlängen-Test: Wie zufällig ist die zufällig gewürfelte Binärkette? (= Glossar Oberstufler)

Jetzt ist es notwendig mit 25 potenzieren, da wir zu Beginn die 100 aufgeteilt haben, aber wir die Länge der Wahrscheinlichkeit „mindestens eines 4er-Blocks bei 100 Zufallszahlen“ betrachten wollen.

Wir potenzieren hierfür die Wahrscheinlichkeit für das Gegenereignis $(7/8)^{25} = 0,0354\dots$ und runden hier etwas auf (da es sich bei diesem Rechenweg, um eine Abschätzung handelt).

Mit einer **Wahrscheinlichkeit von ca. 95 %** gibt es bei guten Zufallszahlen eine 4er Kettenlänge. Bei nur 100 Würfeln ist die Wahrscheinlichkeit sehr hoch, dass vier Zahlen ohne Wechsel aufeinanderfolgend vorkommen. Überprüfe deine eigenen gewürfelten Zahlen.

7

Kettenlängen-Test: Wie zufällig ist die zufällig gewürfelte Binärkette?

Die Länge der Zahlenkette mit gleicher Zahlenfolge ist ein sehr gutes Unterscheidungsmerkmal, weil der echte Zufall selbst bei kurzen Folgen mit hoher Wahrscheinlichkeit relativ lange Ketten produzieren wird.

Oft sind die Ketten bei schlecht erzeugten Zufallsfolgen nicht so lang, weil versucht wird, eine gleichmäßige Verteilung von 0 und 1 sicherzustellen. Was aber dazu führt, dass es z.B. weniger oft vier hintereinander folgende gleiche Zahlen gibt, und sich somit die Zahl der „kurzen“ Ketten erhöht. **Mit der Anzahl an vorhandenen Kettenlängen kann man also Aussagen über die Zufälligkeit von Zufallszahlfolgen treffen.**

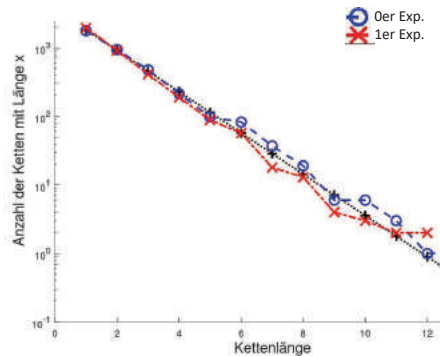
Wir haben festgestellt, wenn wir viele „kleine“ Ketten haben, ist davon auszugehen, dass die Zufälligkeit eher gering ist.

8

Kettenlängen-Test: Wie zufällig ist die zufällig gewürfelte Binärkette?

Hier ist die graphische Darstellung von 10.000 Zufallszahlen, die auf die Kettenlängen analysiert werden.

Auf der x-Achse kann man die möglichen Kettenlängen ablesen (hier bis maximal 12) und auf der y-Achse liest man die Häufigkeit der vorhandenen Ketten.

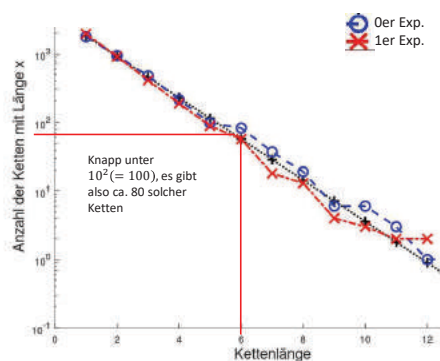


9

Kettenlängen-Test: Wie zufällig ist die zufällig gewürfelte Binärkette?

In der Abbildung rechts siehst du, dass zum Beispiel eine Kette der Länge 6, ca. 80 mal vorkommt (orientiert an den roten Messwerten, also der **1er Ketten**) und ca. 90 mal für die **0er Ketten** (blauer Graph).

Die Kette kann entweder so aussehen 111111 oder so 000000. Es ist egal, ob es Nullen oder Einsen sind, wichtig ist die Wiederholung der gleichen Zahl (0/1) hintereinander. Also kommen bei 10.000 zufälligen Binärzahlen ca. 170 mal Ketten der Länge 6 vor. Viele „Lange Ketten“ sind also keinesfalls unwahrscheinlich.



10



Christian Hesse (2016), Der schnelle Schläuermacher Statistik und Zufall S. 17

Würdest du das auch?!

11

Würfel: Zufall?

Mit dem Würfel kannst du Zufallszahlen generieren, aber was wäre wenn wir würfeln und uns die genauen Parameter wie Luftwiderstand, Masse des Würfels, Abwurfhöhe und Neigungswinkel usw. beim Würfeln bekannt sind.

Sind die Zahlen, die gewürfelt werden, noch zufällig?

Es ist zwar unmöglich, alle Parameter gleichzeitig zu kennen, dennoch sprechen wir hier bei den sog. physikalisch erzeugten Zufallszahlen nicht von Zufall, denn die *Gesetze der klassischen Physik sind im Kern eindeutig bestimmbar (Anton Zeilinger)*.

Eine weitere und sehr bekannte Alternative sind computergenerierte Zufallszahlen. Ob sich diese für „gute Zufallszahlen“ eignen, zeigt sich in den darauffolgenden Folien.

12

Computer generierte Zufallszahlen

Vom Computer erzeugte Zufallszahlen sind möglich, jedoch werden sie normalerweise **Pseudozufallszahlen** genannt.

Diese Pseudozufallszahlen werden über komplexe mathematische Modelle verwirklicht.

(Beispiel: Von Neumann Verfahren [siehe Glossar](#))

13

Beispiel: Erzeugung von Pseudozufallszahlen: Von Neumann Verfahren

Man nehme eine beliebige sechsstellige Dezimalzahl. Als nächstes wird diese Zahl quadriert. Nun nimmt man die mittleren Dezimalstellen. Diese ist die erste Pseudozufallszahl. Dann wiederholt man den Vorgang immer wieder:

$$675248^2 = 455959861504$$

$$959861^2 = 921333139300$$

$$333139^2 = 110981593300$$

...

...

Dieses Verfahren funktioniert nicht mit jeder Anfangszahl, aber bei bestimmten Startwerten sehen die Ergebnisse wirklich sehr chaotisch aus.

14

Computer generierte Zufallszahlen

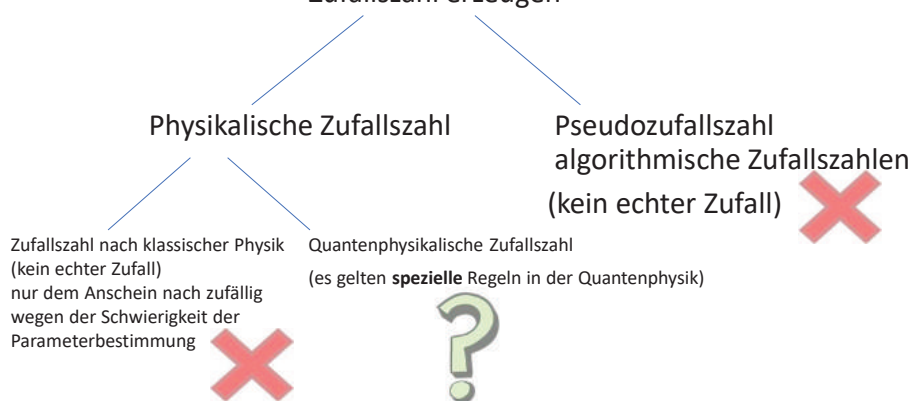
Computergenerierte Zufallszahlen sind meist mathematische Formeln (von Neumann-Verfahren [siehe Glossar](#)) nach einem bestimmten Algorithmus. Ist der **Startwert** also bekannt, kann man die gesamte erzeugte Zufallszahlreihe nachverfolgen, sodass jede einzelne Zahl nicht mehr zufällig erscheint.

Es ist zwar schwer auf den exakten Startwert zu kommen, jedoch besteht die Möglichkeit, weshalb wir auch hier nicht von „echten“ Zufallszahlen sprechen können (=Pseudozufallszahlen).

15

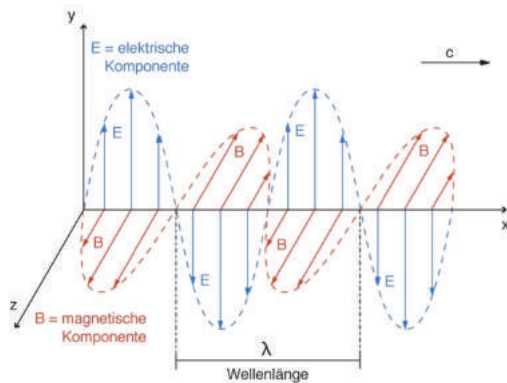
Zufallszahlerzeugung: Übersicht

Anbei eine kleine Übersicht zu den bisherigen Themen
Zufallszahl erzeugen



16

Grundlagen der Optik: Elektromagnetische Welle



Licht ist eine **elektromagnetische Welle**; d.h. sie besteht aus elektrischen und magnetischen Feldern, die senkrecht zur Ausbreitungsrichtung oszillieren (=Transversalwelle).

<http://www.chemgapedia.de/vsengine/vlu/vsc/de/ph/14/ep/einfuehrung/emwellen/ausbreitung.vlu.html>

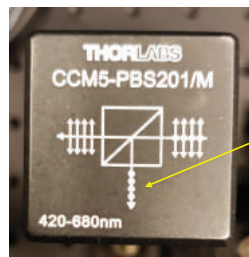
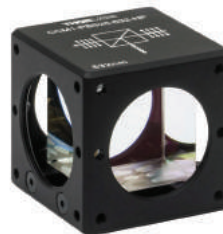
17

Grundlagen: Optik

Polarisation:

Eine Lichtwelle schwingt senkrecht zu ihrer Ausbreitungsrichtung. Wenn das elektrische Feld nur in einer Ebene schwingt, dann ist die Lichtwelle linear polarisiert.

Polarisatoren sind Filter, die nur Licht einer bestimmten Schwingungsrichtung, d. h. Polarisation durchlassen. In unserem Fall ist das Licht, nachdem es den polarisierten Strahlteilerwürfel durchquert hat, stets in dieselbe Richtung linear polarisiert. Hier ist das Licht waagrecht oder senkrecht polarisiert.



Das ist der Strahlteiler aus dem Experiment:
Photonen, die reflektiert werden (siehe Pfeil mit den **Punkten**) sind senkrecht zur Tischebene polarisiert und Photonen, die transmittiert werden (siehe Pfeil mit den langen **parallelen Doppelpfeilen**) sind waagrecht zur Tischebene polarisiert.

https://www.thorlabs.com/newgroupage9.dfm?objectgroup_id=6056

18

Grundlagen: Licht hat Wellen- und Teilcheneigenschaften

Es ist wichtig zu verstehen, dass sich Licht wie eine Welle ausbreitet, aber auch aus einzelnen Photonen besteht (Welle-Teilchen-Dualismus). Die Wellen-Eigenschaft des Lichts zeigt sich beispielsweise bei der Interferenz. Interferenz bedeutet, dass bei einer Überlagerung von zwei Wellen diese sich entweder verstärken (=konstruktive Interferenz) oder abschwächen (=destruktive Interferenz).

Licht hat aber auch Teilcheneigenschaften. Man kann es durch einzelne Energiepakete, sogenannte Photonen beschreiben (siehe z. B. hierfür das [Taylorexperiment = Doppelspaltversuch mit einzelnen Photonen](#)).

19

Grundlagen der Quantenphysik

20

Was sind Quanten?

Quantenobjekte (z.B. Photonen, Elektronen) sind weder kleine Kügelchen noch Wellen oder Wölkchen. Sie sind nichts von dem, was wir aus unserer Alltagserfahrung kennen. Es gibt kein klassisches Bild, mit dem man alle Eigenschaften von Quantenobjekten beschreiben bzw. erklären könnte.

Quantenteilchen breiten sich aus wie Wellen – Wechselwirken mit Materie wie ein Teilchen. Auch wenn Photonen nicht geteilt werden können, scheinen sie mit sich selbst wechselzuwirken (zu interferieren).

Das kleinste Quant an Energie hat die Größe, die man durch Multiplikation des planckschen Wirkungsquantum „h“ mit der Frequenz errechnen kann. $E = h * f$
Das Planck'sche Wirkungsquantum $6,626 * 10^{-34} \text{Js}$ ist eine Naturkonstante, wie beispielsweise die Lichtgeschwindigkeit $299.792.458 \frac{\text{m}}{\text{s}}$ (für Glossar)

21

Grundlagen: Licht hat Wellen- und Teilcheneigenschaften

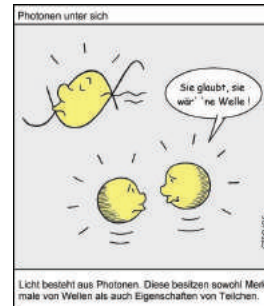
Photonen

- ... sind Quantenobjekte.
- ... sind Elementarteilchen, sie sind unteilbar.
- ... tragen elektromagnetische Energie und Impuls.
- ... können polarisiert werden.

Für Quantenobjekte (Photonen) können nur Wahrscheinlichkeitsaussagen über deren Zustände getroffen werden.

→ Der Welle-Teilchen Dualismus beschreibt das Licht aus heutiger Sicht.

→ Es ist wichtig, dass beide Charakteristika „Licht als Welle“ und „Licht als Teilchen“ gleich bedeutend sind. (Welle-Teilchen-Dualismus)



22

Grundlagen Quantenphysik:

Das faszinierende an Quantenobjekten ist, dass man bei einer größeren Anzahl an Photonen durch Wahrscheinlichkeiten gute Voraussagen treffen kann, jedoch nie für ein einzelnes. Der Quantenphysik gelingt es mittels stochastischer Verfahren eine Beschreibung für die teils widersprüchlichen Verhaltensweisen von Quantenobjekten zu finden.

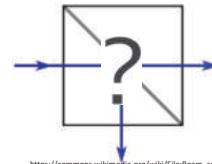
Einzelne Quantenobjekte befinden sich in überlagerten Zuständen, diese nennt man auch **Superposition**. Das bekannteste Beispiel ist Schrödingers Katze, bei der die Katze lebendig und tot gleichzeitig sein kann.

Ob sich ein einzelnes Photon entscheidet an einem Strahlteiler reflektiert oder transmittiert zu werden, bleibt zufällig. Im Strahlteilerwürfel befindet sich das Photon genauso wie Schrödingers Katze in sich überlagernden Zuständen (Reflektion/Transmission).

Für eine **Vielzahl** an Photonen kann man (im Mittel) aber Wahrscheinlichkeitsaussagen von 50 % für die Reflektion und 50% Transmission, treffen.



<https://www.google.de/url?sa=i&url=http%3A%2F%2Fwww.mathisintbeair.org>



https://commons.wikimedia.org/wiki/File:Beam_splitter.svg

23

Glossar

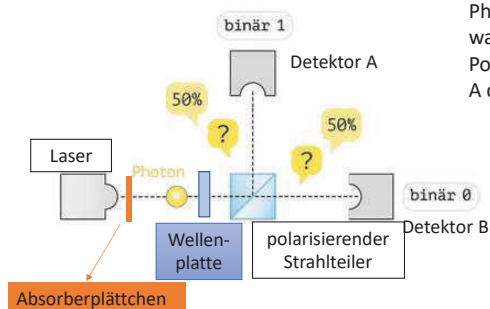
Die Vermeidung einer anschaulichen Vorstellung, wie sich Quantenobjekte „unterwegs“ verhalten, orientiert sich an der [Kopenhagener Interpretation](#).

24

Zufallszahlen erzeugen, durch den Quantenzufallsgenerator

25

Skizze: Aufbau



Laserlicht wird durch die Dunkelfilterplättchen sehr stark abgeschwächt, sodass nur noch vereinzelt Photonen an den Strahlteiler gelangen. Sobald sich das Photon am polarisierenden Strahlteiler entweder für waagrechte (horizontal) oder senkrechte (vertikal) Polarisation entscheidet, gibt es ein Signal am Detektor A oder B.

Der Detektor A wird für die Binärzahl 1 und der Detektor B für die Binärzahl 0 verwendet. Wir können nicht wissen, für welchen Detektor sich das Photon entscheidet. Dadurch erreichen wir eine Binärzahlenfolge, die nicht vorhergesagt werden kann, also echt **zufällig** ist.

Das Quanteninternet Seite 42 Abb. 1.2

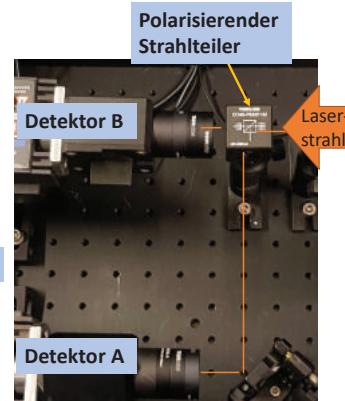
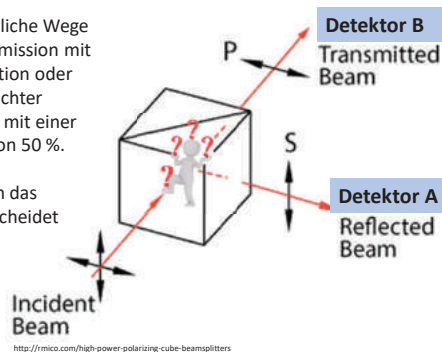
26

Strahlteilerwürfel: hier beginnt der Zufall

Die Photonen bei unserem Laser sind in einer bestimmten Richtung polarisiert. Durch den polarisierenden Strahlteiler werden die Photonen anhand ihrer Polarisation aufgeteilt und zwar in senkrechte bzw. waagrechte Polarisation.

Es gibt also zwei mögliche Wege für ein Photon, Transmission mit waagrecht polarisierter Polarisation oder Reflektion mit senkrechter Polarisation – jeweils mit einer Wahrscheinlichkeit von 50 %.

Für welchen Weg sich das einzelne Photon entscheidet ist rein zufällig.

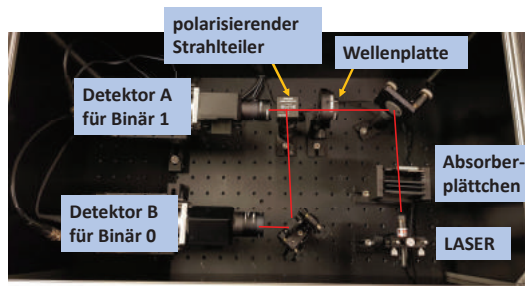


27

Realer Aufbau: Quantenzufallsgenerator

Die Zufälligkeit einzelner Photonen macht man sich beim Quantenzufallsgenerator zu nutze.

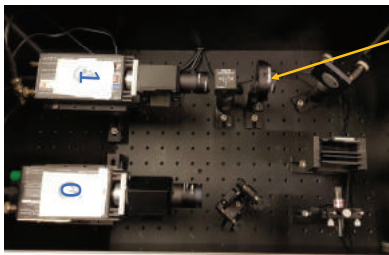
Für den Versuch benötigen wir einen Laser. Damit nur wenige Photonen die Einzelphotonendetektoren erreichen muss das Laserlicht mit Hilfe von **Absorberplättchen** und Filtern, die direkt auf die Einzelphotonendetektoren angebracht sind, stark abgeschwächt werden. Die Photonen werden rein zufällig beim **polarisierenden** Strahlteiler entweder reflektiert mit senkrechter Polarisation oder transmittiert mit waagrecht polarisierter Polarisation. Durch das Festlegen der Detektoren Transmission → binäre 0, Reflexion → binäre 1 ist das Ergebnis eine vollkommen zufällige Bitfolge.



28

Aufbau: Quantenzufallsgenerator

Es gibt Laser, die linear polarisiertes Licht emittieren, aber dieser hat nur eine gewisse Vorzugsrichtung in der er stärker polarisiert ist. Vor dem Strahlteiler, welcher optimalerweise eine 50:50 Strahlverteilung ermöglicht, ist eine Wellenplatte $\frac{\lambda}{2}$ positioniert. Durch die Wellenplatte verzögern wir sozusagen die Vorzugsrichtung des Laser in der er stärker schwingt und erreichen eine gleiche Intensität in den beiden Detektoren.



Die $\frac{\lambda}{2}$ - Wellenplatte ist ein optisches Bauelement, das die Polarisation von Licht verändert, dadurch wird die gleiche Intensität in den beiden Detektoren erreicht.

29

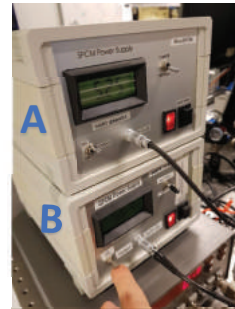
Quantenzufallsgenerator nutzen:

Schritt 0: Überprüfe, ob die Absorberplättchen aufgesetzt sind. Es kann sein, dass sie jemand entfernt hat. Wenn das der Fall ist, bitte Frau Stähler-Schöpf melden und nicht das Experiment starten.

Schritt 1: Deckel schließen. **WICHTIG!**

Schritt 2: Die Spannungsgeneratoren für die Einzelphotonendetektoren einschalten (wenn diese bereits eingeschaltet sind, weiter zu Schritt 3)

Das Einschalten der Spannungsgeräte: Drücke zuerst den schwarzen Knopf rechts danach den silbernen Schalter links



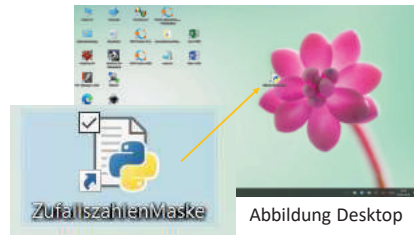
Das obere Gerät gehört zu Detektor A und das untere zu Detektor B

30

Quantenzufallsgenerator nutzen:

Schritt 3: Starte das Programm „ZufallszahlenMaske“ (Passwort vom Laptop: PhotonLab) und drücke auf Start. Sobald du auf Stopp drückst werden die Zufallszahlen ermittelt.

Achtung!
Sobald der Laser eingeschaltet wird muss der Deckel aufgesetzt werden. Die Einzelphotonendetektoren sind **sehr sensibel** und reagieren auf sämtliche Lichteinstrahlung und können daher sehr schnell zerstört werden.



Schritt 4: Laser einschalten (Schalter ist hinter der Box)



31

Erklärung zum Programm:

Quantenzufallsgenerator

Zufallszahlen:

Detektor Verhältnis

A: B:

55 : 45

Kreiszahl Pi bestimmen

Berechnetes Pi: 3.074

Kettenlängentest

Länge	Anzahl
<input type="checkbox"/>	694
<input type="checkbox"/>	291
<input type="checkbox"/>	131
<input type="checkbox"/>	67
<input type="checkbox"/>	30
<input type="checkbox"/>	13
<input type="checkbox"/>	0

Glücksrad

Eine genaue Beschreibung wie Pi berechnet wird siehst du im Fragezeichen-Tool.

Im Programm gibt es **Fragezeichen-Tools**, dort wird der Bereich erklärt und meist geschildert, wie wir die Zufallszahlen aus dem Quantenzufallsgenerator nutzen.

Photonen sorgen auf den Detektoren für Spannungsimpulse, diese werden für den Detektor A als Binärzahl 1 und für den Detektor B als 0 dargestellt. Das Bild auf dem Oszilloskop wird im Glossar genauer thematisiert.

Zufallszahlen können dafür verwendet werden um die Zahl π auf sehr vielen Nachkommastellen richtig zu berechnen. Zufallszahlen können aber auch für die Verschlüsselung von sensiblen Daten verwendet werden. → siehe [Quantenkryptographie](#)

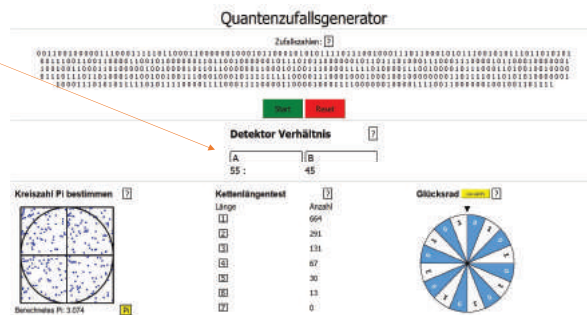
32

Quantenzufallsgenerator nutzen:

Schritt 5: Überprüfe nun durch das Programm in welchem Verhältnis die Detektoren sind.

Schritt 6: Jetzt ist es wichtig mit der Wellenplatte, die vor dem Strahlteiler positioniert ist, eine möglichst gleiche Intensitätsverteilung zu erreichen.

In der nächsten Folie ist der Arbeitsauftrag genau beschrieben.



33

Deine Aufgabe: Wellenplatte verstellen

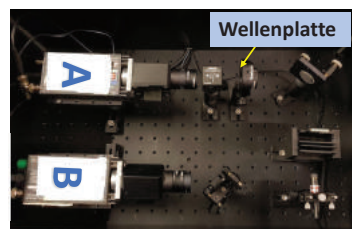
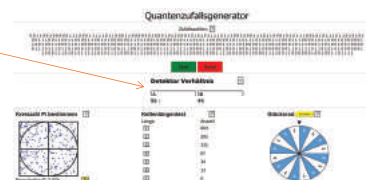
Deine Aufgabe ist es nun mittels der Wellenplatte das Verhältnis der beiden Detektoren so gleichmäßig wie möglich einzustellen.

Hierfür musst du folgende Schritte (wahrscheinlich) mehrmals durchführen:

1. Laser wieder **ausschalten**
2. Deckel öffnen
3. Wellenplatte verstellen
4. **Deckel wieder schließen**
5. Laser einschalten und dann das Programm Restarten

Sobald du auf Restart und Start gedrückt hast, kannst du auf dem Programm sehen wie sich die Veränderung der Polarisation durch Drehung des $\frac{\lambda}{2}$ - Plättchen auf die 50:50 Aussendung der Photonen auswirkt und damit direkt auf die Qualität deiner erzeugten Zufallszahlen.

Es ist sehr schwer eine gleichmäßige Verteilung herzustellen. **Viel Erfolg dabei!**

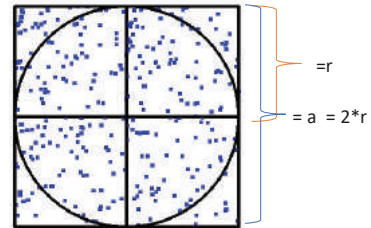


34

Qualität der Zufallszahlen

Es gibt viele Tests zur statistischen Untersuchung von Zufallszahlen. Ob deine Zufallszahlen gut oder schlecht sind erkennst du beispielsweise durch die Bestimmung der Kreiszahl Pi.

Mit der sogenannten Monte-Carlo-Methode können wir die Kreiszahl bestimmen. Die Zufallszahlen werden gleichmäßig im Quadrat verteilt. Diese gleichmäßige Verteilung ist entscheidend, denn das Verhältnis der Zufallszahlen (hier als Punkte gekennzeichnet N_K) im Kreis zur Gesamtanzahl der Zufallszahlen im Quadrat (N_Q) ist gleich dem Verhältnis der Flächeninhalte von Kreis (πr^2) und Quadrat (a^2) wobei hier $a = 2 * r$ entspricht.



$$\frac{A_{Kreis}}{A_{Quadrat}} = \frac{r^2 * \pi}{a^2} \text{ weil } (a = 2r) \Rightarrow \frac{r^2 * \pi}{(2 * r)^2} = \frac{\pi}{4} = \frac{N_K}{N_Q} \Rightarrow \pi = \frac{N_K}{N_Q} * 4$$

35

Qualität der Zufallszahlen

Beim Kettenlängentest betrachtet man bei einer zufällig erstellten Binärkette die Häufigkeit bestimmter Kettenlängen. Diese werden dir über das Programm angezeigt. Als Kettenlänge wird die Anzahl von aufeinanderfolgenden gleichen Zeichen bezeichnet.

Mathematisch kann man die Wahrscheinlichkeit für das Auftreten bestimmter Kettenlängen bestimmen siehe Glossar.

Du kannst aber auch qualitativ eine Aussage treffen. Das Auftreten einer **langen** Kette (größer 3) ist umso unwahrscheinlicher, je weniger Ketten überhaupt vorhanden sind. Am ersten Beispiel erkennst du, dass hier die Zufallszahlen eher schlecht sind.

Kettenlängentest

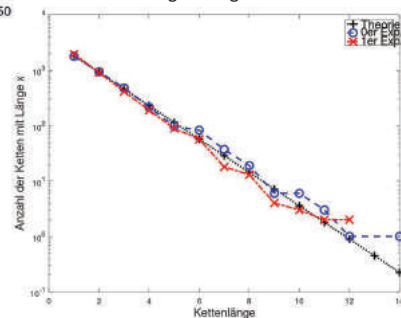
Länge

- 1
- 2
- 3
- 4
- 5
- 6

1. Beispiel aus dem Programm

Anzahl
1646
1128
786
488
360
260

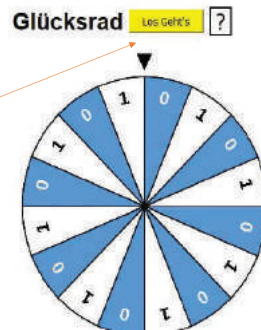
2. Beispiel aus dem Programm guter Zufallszahlen



36

Erzeugen von Zufallszahlen

Durch die ermittelten Zufallszahlen kann die Rotationsgeschwindigkeit vom Glücksrad verändert werden. Damit kannst du deine persönliche Quantenzufallszahlreihe erzeugen, die wirklich zufällig ist vorausgesetzt dein Detektorverhältnis ist gleichmäßig.
Drücke hierfür auf „Los geht's“



37

Ende vom Experiment:

Zu Beginn hast du versucht Zufallszahlen durch würfeln zu erzeugen und festgestellt, dass man an seine Grenzen kommt mit dem „Zufälligen“, doch mittels dem Quantenzufallsgenerator hast du eine gute Möglichkeit entdeckt „echt“ zufällige Zufallszahlen zu generieren, aber nur wenn man eine gleichmäßige Ausrichtung der Polarisation einstellt.

38

Oszilloskopbild interpretieren (Glossar)

Eigenschaften:
Damit der Detektor ein Photon noch als einzelnes Signal wahrnimmt, müssen 8 ns Abtastrate hinterlegt werden

Messungen:
Hier kannst du dich orientieren nach welchem Parameter deine Messung, durch die Photonendetektoren (A und B) gemessen werden soll.
Für uns ist die Frequenz relevant.

Signal Detektor A
(entspricht 0)

Signal Detektor B
(entspricht 1)

Kleine Striche: „Rauschen“
Signale unter 1.5 Volt sind für die Messung irrelevant

Mittelwert (engl. Average):
Hier erreichst du durch das Verstellen der Wellenplatte ein gleichmäßiges Maß an Lichtintensität.

Literaturverzeichnis

Bahr, Benjamin; Resag, Jörg; Riebe, Kristin (2015): Faszinierende Physik. Ein bebildeter Streifzug vom Universum bis in die Welt der Elementarteilchen. 2. Auflage. Berlin, Heidelberg: Springer Spektrum.

Bronner, Patrick (2010): Quantenoptische Experimente als Grundlage eines Curriculums zur Quantenphysik des Photons. Zugl.: Erlangen-Nürnberg, Univ., Diss., 2010. Berlin: Logos-Verl. (Studien zum Physik- und Chemielernen, 103).

Duit, Reinders (1995): Zur Rolle der konstruktivistischen Sichtweise in der naturwissenschaftsdidaktischen Lehr- und Lernforschung. In: *Zeitschrift für Pädagogik* 41 (6), S. 905–923.

Eichler, Hans Joachim; Eichler, Jürgen (2015): Laser. Berlin, Heidelberg: Springer Berlin Heidelberg.

Fürst, Martin: Quantenoptisches Verfahren zur Erzeugung zufälliger Bitfolgen.

Führinger, Leo (2012): Aufbau eines Quantenzufallsexperiments

Haahr, Mads (2020): RANDOM.ORG - Frequency (Monobit) Statistics. Online verfügbar unter <https://www.random.org/statistics/frequency-monobit>, zuletzt aktualisiert am 04.10.2020, zuletzt geprüft am 04.10.2020.

Kircher, Ernst; Schneider, Werner B. (Hg.) (2003): Physikdidaktik in der Praxis. Korrigierter Nachdr. Berlin: SPRINGER (Physics and astronomy online library).

Müller, Rainer (Hg.) (2011): Schülervorstellungen in der Physik. Festschrift für Hartmut Wiesner. Unter Mitarbeit von Hartmut Wiesner. 3., unveränd. Aufl. Köln: Aulis-Verl.

Phasenplättchen (2014). Online verfügbar unter <https://www.spektrum.de/lexikon/physik/phasenplaettchen/11125>, zuletzt aktualisiert am 04.12.2014, zuletzt geprüft am 20.06.2020.

Saleh, Bahaa E. A.; Teich, Malvin Carl (2008): Grundlagen der Photonik. 1. Auflage, [deutsche Übersetzung von] 2., vollständig überarbeitete und erweiterte Auflage [des Werkes]. Weinheim: Wiley-VCH Verlag GmbH & Co. KGaA (Lehrbuch Physik). Online verfügbar unter <http://www.wiley-vch.de/de/fachgebiete/ingenieurwesen/elektrotechnik-und-elektronik-10ee/photonic-u-laser-10ee5/grundlagen-der-photonik-978-3-527-40677-7>.

Schrödinger, E. (1935): Die gegenwärtige Situation in der Quantenmechanik. In: *Naturwissenschaften* 23 (48), S. 807–812. DOI: 10.1007/BF01491891.

Schroeder, Manfred (2009): Number Theory in Science and Communication. With Applications in Cryptography, Physics, Digital Information, Computing, and Self-Similarity. Fifth Edition. Berlin, Heidelberg: Springer Berlin Heidelberg. Online verfügbar unter <http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10266198>.

Specovius, Joachim (2018): Grundkurs Leistungselektronik. Bauelemente, Schaltungen und Systeme. 9., überarbeitete und aktualisierte Auflage. Wiesbaden: Springer Vieweg.

Statistical_Test_Suite_for_Random_and.html?id=u33_oAEACAAJ&source=kp_cover&redir_esc=y, zuletzt aktualisiert am 30.05.2020, zuletzt geprüft am 30.12.2020.

Tipler, Paul Allen; Mosca, Gene; Kommer, Christoph (2015): Physik. Für Wissenschaftler und Ingenieure. 7. Aufl. Hg. v. Jennifer Wagner. Berlin: Springer Spektrum.

U.S. Department of Commerce (2014): A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Online verfügbar unter https://books.google.de/books/about/A_Statistical_Test_Suite_for_Random_and.html?id=u33_oAEACAAJ&source=kp_cover&redir_esc=y, zuletzt aktualisiert am 30.05.2020, zuletzt geprüft am 04.12.2020.

Walther, Thomas; Walther, Herbert (2010): Was ist Licht? Von der klassischen Optik zur Quantenoptik. Orig.-Ausg., 3., aktualisierte Aufl. München: Beck (Beck'sche Reihe C. H. Beck Wissen, 2122).

Welt der Physik (2021): Wie zufällig ist Würfeln? Online verfügbar unter <https://www.weltderphysik.de/thema/chaos-und-ordnung/wie-zufaellig-ist-wuerfeln/>, zuletzt aktualisiert am 10.01.2021, zuletzt geprüft am 10.01.2021.
