Messprotokoll: Aufnahme der Quantenzufallszahl

Am 19. Juni 2009 wurden für Max Mustermann um 8:35 Uhr mit Hilfe von einzelnen Photonen 993.097 Zufallszahlen generiert. Der Zufallsgenerator steht im Quantenoptiklabor der Didaktik der Physik an der Universität Erlangen. Den wichtigsten Teil des Aufbaus mit dem Strahlteilerwürfel kann man in Bild 1 erkennen. Die einzelnen Photonen werden in einem getrennten Aufbau erzeugt. Beide Teile sind mit dem gelben Glasfaserkabel verbunden. Da einzelne Photonen unteilbare Portionen sind, können sie am Strahlteiler entweder nur reflektiert oder nur transmittiert werden. Im Experiment wurden 49,85% aller Photonen transmittiert. Insgesant gab es 988 Ereignisse, bei denen Photonen in beiden Detektoren registriert wurden. Die Leistung des Lasers zum Erzeugen der Photonenpaare betrug im Experiment 464μW. Die Verteilung von bestimmten Kombinationen ist in Tabelle 1 zusammengefasst. Die ersten binären Zufallszahlen sind auf der nächsten Seite abgedruckt. Mit Zufallszahlen kann man z. B. die Zahl π über die Monte-Carlo Methode berechnen. Mit den generierten Zufallszahlen kommt der Wert π =3,11993 heraus.

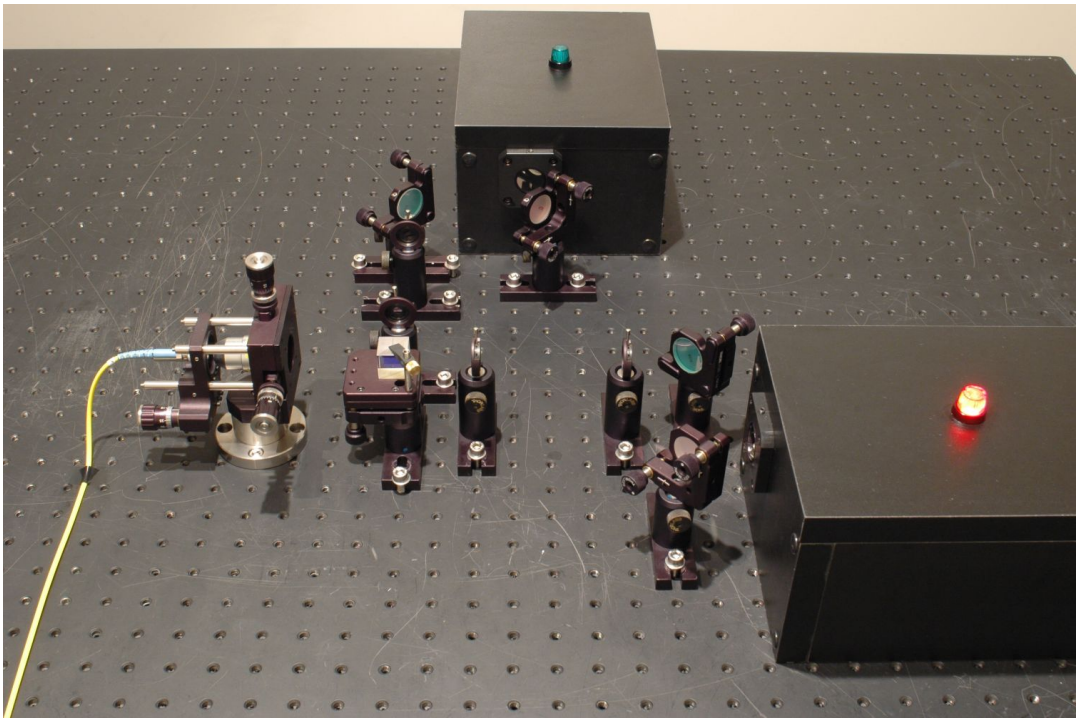


Abbildung 1: Optischer Aufbau mit 50% Strahlteiler

Kombination	Wahrscheinlichkeit
00	25,14 %
01	25,06 %
10	24,97 %
11	24,84 %

Tabelle 1: Wahrscheinlichkeiten für Ereignisse.

1 0 0 0 1 0 0 0 0 0 1 0 0 1 0 0 0 1 0 0 1 1 1 1 0 1 0 0 1 0 0 0 0 1 0 0 0 0 1 0 1 1 0 1 0 0 1
1 1 1 1 0 0 0 0 1 0 0 0 0 1 0 1 0 1 0 0 1 0 0 1 0 1 0 0 1 1 1 1 1 1 1 0 0 0 0 0 0 0 1 0 0 0 1
1 0 1 1 0 1 1 1 0 1 0 0 0 0 0 1 1 0 0 0 0 0 1 0 1 0 1 0 0 0 1 1 1 1 1 0 0 1 1 0 0 1 0 1 1 0 0
1 0 1 0 0 0 1 0 0 1 0 1 1 1 1 1 1 0 1 0 0 0 1 0 1 0 0 1 0 1 0 1 1 1 1 1 1 1 0 0 0 1 1 0 0 0 0 0
1 1 0 1 1 1 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 1 0 0 0 1 0 1 1 1 1 1 1 1 0 1 1 1 1 0 1 0 0
0 0 1 1 0 0 0 1 1 0 0 1 1 1 1 0 0 0 1 0 1 0 0 1 1 0 0 0 1 1 1 1 1 0 0 0 1 0 0 0 0 1 0 1 1 1 0
0 1 1 1 0 1 0 1 1 0 0 0 0 1 0 1 0 1 1 1 1 0 0 1 0 0 1 1 0 1 0 0 1 1 0 1 1 0 0 0 1 1 0 0 0 1 0
0 0 0 0 0 1 1 0 1 0 1 1 0 0 1 0 1 0 1 1 1 0 0 0 0 1 1 0 1 1 0 1 1 1 1 0 0 0 1 0 1 1 1 0 0 0 1
1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 1 1 0 1 0 1 0 1 0 0 1 0 1 1 1 1 1 0 1 0 0 1 1 0 1 0 1 1 1 1 0 0
0 0 1 1 0 0 0 1 0 1 0 0 0 0 0 1 1 1 0 1 0 0 0 1 1 0 1 0 0 0 1 0 0 0 0 1 0 1 0 1 0 1 1 0 1 0 1
1 1 1 0 0 0 1 0 0 1 1 0 1 1 0 0 1 0 0 1 1 0 1 1 1 0 1 1 1 1 0 0 1 1 0 0 1 1 1 1 0 0 1 0 1 1 1
0 0 0 1 0 1 0 1 0 0 1 0 1 0 0 0 0 0 1 1 0 1 0 1 1 0 0 1 1 1 0 0 1 0 1 1 1 1 1 0 0 0 0 0 0 1 0
0 0 1 1 1 0 0 1 1 0 1 1 1 1 0 1 1 0 0 0 1 1 1 1 0 0 1 1 1 1 1 1 0 0 1 1 1 1 0 0 0 1 0 0 0 1 0
1 1 1 1 0 1 1 1 1 0 1 0 1 0 0 0 0 1 0 0 0 0 0 0 0 1 1 1 0 0 0 0 0 1 0 1 1 0 1 1 0 0 1 0 1 0 0
0 1 0 0 1 0 0 1 0 0 0 0 0 0 0 1 0 1 0 0 1 1 0 1 0 1 1 0 0 1 1 0 1 1 0 0 1 1 0 0 1 1 0 1 1 0 0
1 1 1 0 0 1 0 0 1 1 0 0 1 0 1 1 1 1 1 1 1 0 0 1 0 0 1 1 0 1 0 0 0 0 0 1 0 0 0 1 1 0 1 0 0 1 0 0
1 0 0 1 1 1 1 0 0 1 1 0 1 0 1 0 0 0 1 0 1 1 1 0 0 1 1 1 1 0 1 1 0 0 1 0 0 1 0 1 1 1 1 1 1 0 1 1
1 1 1 1 0 0 0 0 1 1 1 1 0 1 1 1 0 1 0 0 0 1 1 1 0 0 1 1 1 1 1 0 1 0 0 1 0 0 0 0 0 0 0 1 0 0 1 1
0 0 0 0 1 1 1 1 1 0 1 0 0 0 0 0 1 1 1 1 0 1 1 1 0 0 1 0 0 0 0 1 0 1 0 0 1 1 1 0 0 0 0 0 0 0 0 0
1 1 0 1 0 1 0 1 0 1 1 0 1 0 1 1 1 0 1 1 1 1 1 1 1 0 0 0 1 0 1 0 1 1 1 0 1 0 1 0 1 0 0 0 1 0 1 1
1 1 0 0 1 1 1 1 1 0 0 0 1 1 0 0 1 0 1 0 1 1 0 1 0 0 1 0 1 1 1 1 0 0 0 0 1 0 1 0 1 0 0 0 0 1 1
1 0 0 1 1 0 0 0 1 0 0 0 0 0 1 1 0 1 1 1 1 0 1 1 1 1 0 0 0 1 0 1 1 0 0 0 0 0 0 1 0 0 0 0 1 0 1
0 0 0 1 1 0 0 1 1 1 0 1 0 1 1 0 1 0 1 1 0 0 0 0 0 1 0 1 1 1 1 1 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0
0 0 0 0 0 1 1 0 1 0 0 1 1 1 1 0 1 0 1 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 1 1 1 1 1 0 1 1 1 1 1 1 1
0 0 1 1 0 1 0 0 0 0 1 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 0 1 0 0 0 0 0 1 0 1 1 0 1 1 0 1 0 1 0 0
1 1 1 1 0 0 1 1 1 1 0 1 1 1 0 0 1 0 0 1 0 0 0 1 0 1 0 1 0 0 0 1 0 1 1 1 0 1 0 1 1 0 0 1 1 1 1
0 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 1 0 1 0 0 1 1 1 0 0 0 1 1 0 0 0 0 1 0 1 0 1 0 0 0 0
1 0 0 0 1 0 1 1 0 1 0 1 0 1 1 0 0 1 0 1 1 1 0 1 0 0 0 1 0 0 0 1 1 1 0 1 1 1 1 0 0 1 0 0 0 1 1
1 1 1 1 0 1 0 1 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 1 1 1 1 1 0 1 1 1 1 0 0 1 0 0 0 1 1 0 0 0 1 1 0 1
1 0 0 1 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 1 0 1 1 0 1 1 0 1 0 1 1 0 0 0 0 1 1 0 0 0 1 0 1
1 0 0 0 1 1 1 1 1 1 0 0 1 1 0 1 0 1 1 1 1 1 1 0 0 1 0 0 0 1 0 1 1 0 1 0 1 0 1 1 1 0 0 1 1 1 1
0 0 0 1 0 0 1 0 1 0 1 1 1 0 1 0 0 0 0 1 1 0 0 1 1 1 1 1 1 0 1 1 0 0 1 0 0 1 0 0 1 1 0 1 0 1 1 0
0 0 1 0 1 0 1 1 0 1 1 1 1 1 1 1 0 1 1 1 0 0 0 0 1 0 1 0 0 0 1 0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 1
1 0 0 0 1 1 1 0 0 0 0 1 1 0 1 1 1 0 1

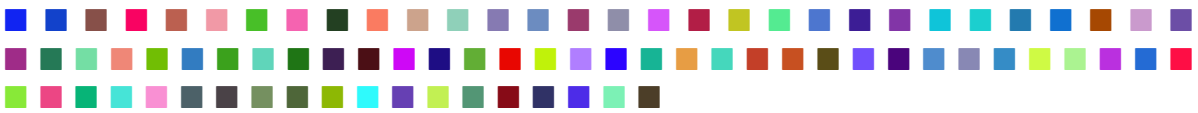
Aus 5 einzelnen Bits kann man Zufallsbuchstaben von A bis Z erzeugen. Da es bei 5 Bit 32 Möglichkeiten gibt und das Alphabet nur 26 Buchstaben hat, wurden die fehlenden Zuordnungen mit einem (?) gekennzeichnet. Die Binärzahlen von der letzen Seite ergeben die folgenden 400 Buchstaben:

R A J E P J I I L ? B B V E F ? D Q Y W L Q B K R P G N K E ? X I J
? H G Y O E A S I U ? ? F M M ? I Z Y H C ? Z V B V H Z S N M E Q V J ? Q N P
U D T K L X K ? X M ? B D F Y F W I I V V H S N S ? ? M ? U D V U A L T T ?
B E O W X R H ? Z D R ? ? K I A O Q W J R E B I Z ? M T Z G H Z U ? E L Q Y
S E P W C ? ? N S ? ? H ? ? C H ? S A S B ? C ? ? E U ? A Y K N ? ? D V L F ? T
P M K L ? D K B H D B W X H ? A C K M O N N Q ? D E A A W ? V A Y ? P ? H
L I Q ? ? C U N F P ? O S I F ? V Z ? B ? H I Z R B V Q I L N ? F C X H R ? K C
B Y X H R R N G C R I ? W G M U R ? M ? T I L ? ? D J ? C G ? G J W G K ? ?
O I R Q Y U D H M X R I Y D Q W X T R I ? L H ? Q ? U Z U Q B N K S Q O U ?
B S A T T M W ? U R Y F B ? C ? T ? G D Q G L B D ? T ? U M Z ? ? Q L Y F A
D Z Y M N C L Q O ? F ? V F T ? D U E D

Aus 8 einzelnen Bits (1 Byte) kann man dezimale Zufallszahlen von 0-255 erzeugen. Die Binärzahlen von der letzen Seite ergeben die folgenden 250 Zahlen:

17, 36, 242, 18, 66, 203, 135, 80, 73, 249, 3, 98, 187, 96, 80, 241, 153, 166, 72, 191, 40, 245, 99, 176, 35, 64, 34, 250, 123, 97, 204, 163, 140, 143, 208, 185, 134, 122, 178, 108, 140, 192, 154, 58, 108, 143, 142, 169, 214, 85, 250, 178, 30, 70, 193, 197, 34, 84, 235, 145, 77, 118, 207, 60, 29, 149, 130, 53, 167, 15, 196, 217, 27, 207, 207, 35, 122, 175, 16, 112, 208, 166, 72, 2, 202, 154, 205, 108, 78, 166, 159, 44, 136, 37, 121, 86, 116, 222, 164, 239, 135, 119, 113, 190, 4, 50, 124, 193, 59, 161, 28, 96, 213, 186, 31, 117, 21, 61, 31, 83, 75, 15, 21, 206, 8, 246, 30, 13, 132, 98, 174, 53, 232, 7, 1, 192, 242, 10, 176, 126, 255, 44, 4, 255, 23, 180, 149, 231, 157, 68, 69, 215, 188, 195, 63, 40, 199, 80, 33, 90, 77, 23, 113, 79, 252, 74, 4, 124, 79, 140, 205, 136, 136, 180, 53, 140, 198, 207, 250, 68, 171, 243, 145, 186, 48, 223, 36, 107, 212, 254, 14, 69, 136, 233, 56, 236, 70, 132, 7, 180, 119, 70, 228, 215, 249, 144, 211, 76, 97, 104, 74, 66, 71, 117, 144, 96, 78, 102, 57, 141, 184, 4, 47, 250, 252, 102, 64, 179, 194, 240, 83, 83, 150, 117, 135, 11, 23, 48, 50, 102, 77, 44, 232, 124, 241, 181, 76, 62, 40, 25,

Aus 24 einzelnen Bits (3 Byte) kann man 16,8 Millionen verschiedene Zufallsfarben erzeugen. Die Binärzahlen von der ersten Seite ergeben die folgenden 83 Farben:



Analyse der aufgenommenen Quantenzufallszahl

19. Juni 2009

In diesem Dokument wurden für Max Mustermann die erzeugten Quantenzuufallszahlen analysiert und mit zwei computergenerierten Pseudozufallszahlen verglichen. Die erste Pseudozufallszahl enstand durch einen einfachen linearen Kongruenzgenerator (LCG). Die zweite Pseudozufallszahl entstand durch die Kombination mehrerer LCG. Um die Güte einer Zufallszahl zu testen kann man auf eine sehr große Anzahl verschiedener Testverfahren zurückgreifen. In diesem Dokument werden fünf Testverfahren vorgestellt. Um im Vergleich mit einer Peudozufallszahl wirklich eindeutige Testergebnisse zu bekommen, benötigt man einen Datensatz von mind. 80 MBits. Beim Experiment im Quantenoptiklabor wurden jedoch nur 993.097 binäre Zufallszahlen aufgenommen.

1 Zufallszahlen mit 8-Bit

Durch Umwandlung der binären Zahlen in 8-Bit Zahlen reduzierte sich die Datenmenge von 993.097 Binärzahlen auf 124.137 Dezimalzahlen im Bereich von 0-255. Der Mittelwert und die Entropie für 8-Bit Zufallszahlen kann man aus Tabelle 1 entnehmen. In Bild 1 kann die Häufigkeit der einzelnen Quantenzufallszahlen betrachtet werden. Durch den von Neumann Algorithmus kann das Strahlteilerverhältnis verbessert werden. In Bild efBild:Haeufigkeit255Neum wurden die Häufigkeiten der Zahlen für die von Neumann Zahl dargestellt. In Bild 3 und 4 sind die Häufigkeiten der Pseudozufallszahlen dargestellt.

Zufallszahl	Mittelwert	Entropie
Quantenzufallszahl	127,0313	7,9983
Quantenzufall Neumann	128,2216	7,9948
Pseudozufallszahl 1	127,5050	8,0000
Pseudozufallszahl 2	127,5158	7,9985

Tabelle 1: Mittelwert und Entropie

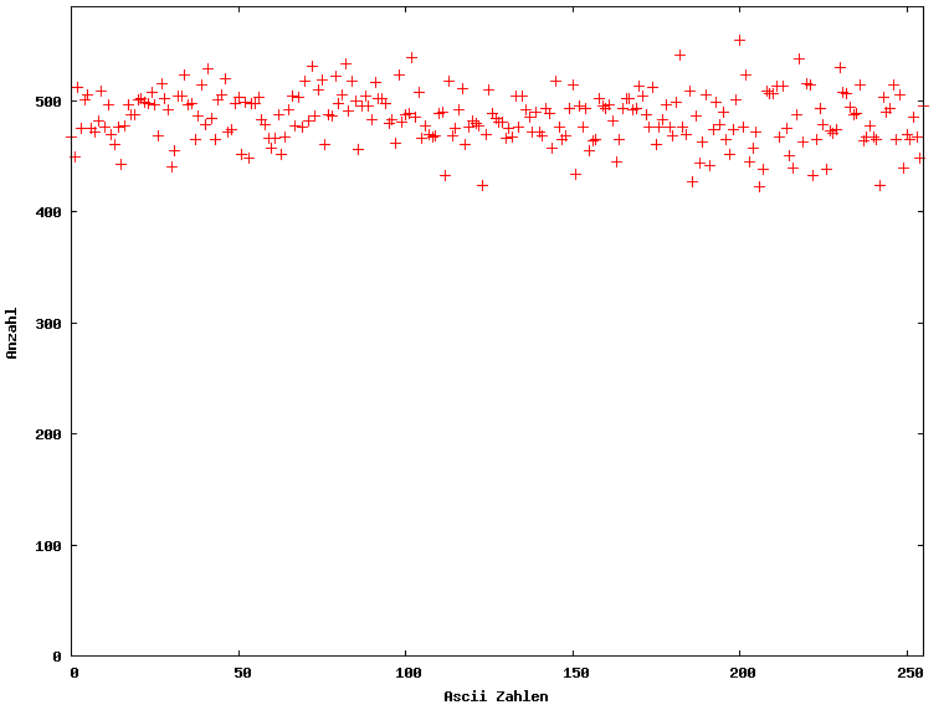


Abbildung 1: Häufigkeit der Zahlen 0-255 Quantenzufallszahl

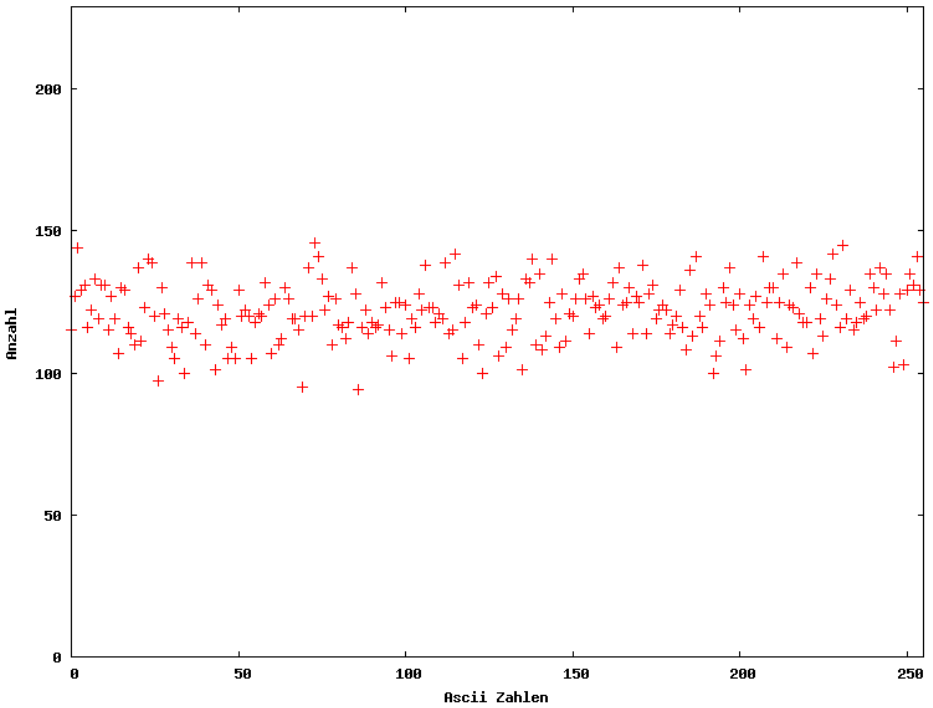


Abbildung 2: Häufigkeit der Zahlen 0-255 Quantenzufallszahl Neumann

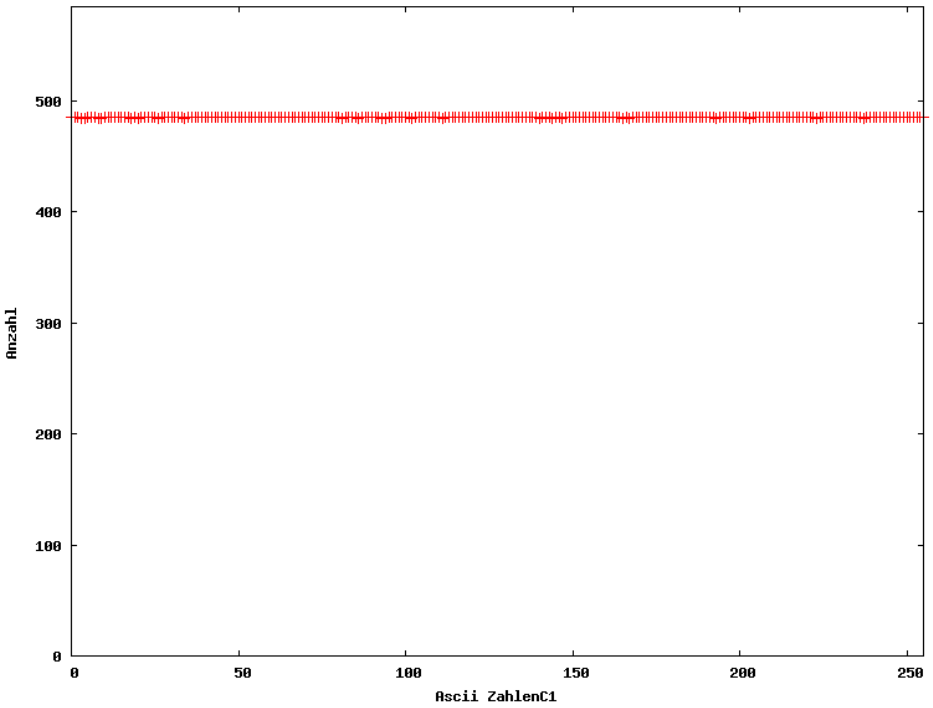


Abbildung 3: Häufigkeit der Zahlen 0-255 Pseudozufallszahl 1

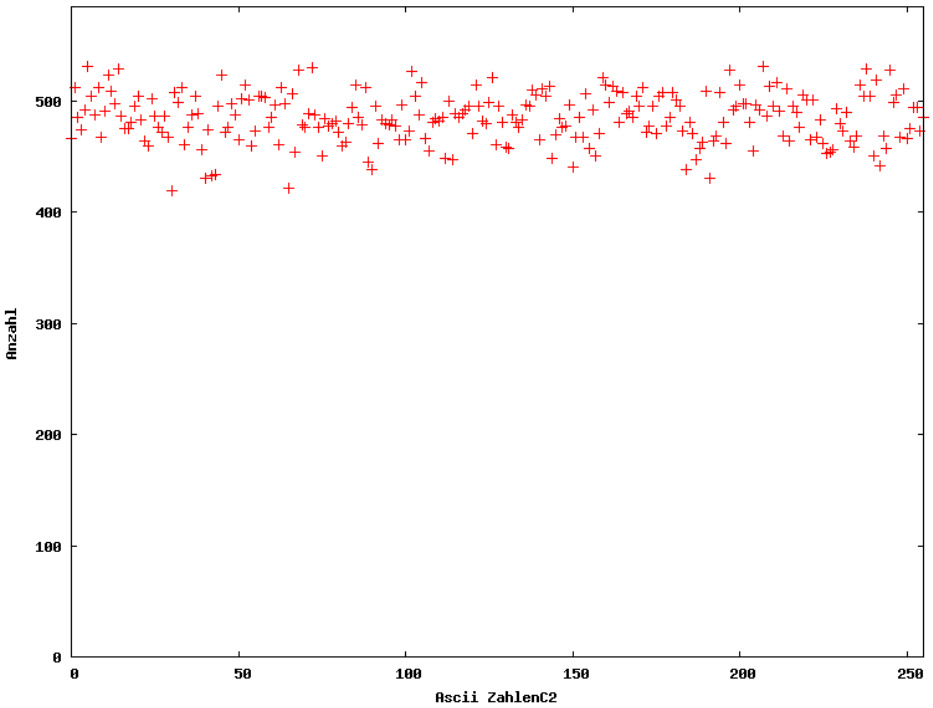


Abbildung 4: Häufigkeit der Zahlen 0-255 Pseudozufallszahl 2

2 Zufallszahlen und Kreiszahl π

Über die Monte-Carlo-Methode (Abbildung 5) kann man die Kreiszahl π berechnen. Zur Bestimmung von π wurden pro Koordinate 2*13 Bit verwendet. Es gab dadurch 38.196 mögliche Koordinaten. Die berechneten Werte und Abweichungen von π kann man Tabelle 2 entnehmen.

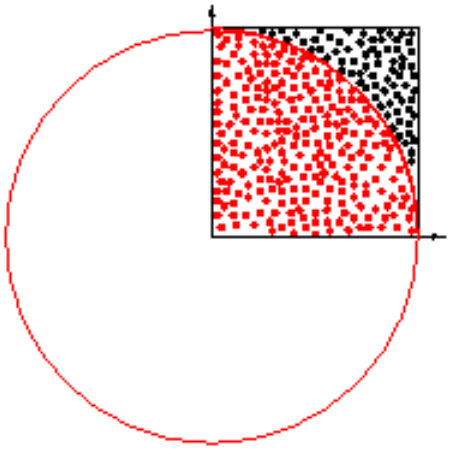


Abbildung 5: Monte-Carlo Methode zur Bestimmung von π über Zufallszahlen

Zufallszahl	Wert für π	Abweichung [%]
Exakter Wert	3,1416	-
Quantenzufallszahl	3,1675	0,8231
Quantenzufall Neumann	3,1351	0,2059
Pseudozufallszahl 1	3,3384	6,2633
Pseudozufallszahl 2	3,1453	0,1164

Tabelle 2: Zahl π

3 Strahlteilerverhältnis

Bei den binären Quantenzufallszahlen kommt die 1 in 49,85% der Fälle vor. Bei einem exakten Strahlteiler sollte das Verhältnis bei dieser Anzahl zwischen 50,15% und 49,85% (Sigma Binominalverteilung) liegen. Um ein ideales Strahlteilerverhältnis zu bekommen wurden die Daten mit dem von Neumann Algorithmus bearbeitet. Hierzu musste jedoch die Datenmenge um 74,85% auf 249.775 Bits reduziert werden. In den neuen Binärzahlen kommt die 1 in 50,0879% der Fälle vor. Bei einem exakten Strahlteiler sollte das Verhältnis bei dieser Anzahl zwischen 50,30% und 49,70% liegen. Die Häufigkeit der einzelnen Kombinationen der Binärzahl ist in Tabelle 3 für die rohen und bearbeiteten Daten dargestellt. Das Strahlteilerverhältnis kann sich während der Messung verändern. Dies liegt z. B. an der Dejustierung oder an der Effizienzänderung der Detektoren aufgrund der eigenen Erwärmung. Die zeitliche Änderung des Verhältnisses bei den Rohdaten ist in Abbildung 6 dargestellt. Die zeitliche Änderung des Verhältnisses mit den von Neumann Zahlen ist in 7 dargestllt. Die Blockgröße beträgt bei den Rohdaten 9930 Bits und bei den von Neumann-Daten 12488 Bits.

Kombination	Häufigkeit Rohdaten [%]	Häufigkeit Neumann [%]
1	49,85	50,09
00	25,00	24,93
01	25,11	25,02
10	25,20	24,95
11	24,70	25,10

Tabelle 3: Wahrscheinlichkeiten für Ereignisse.

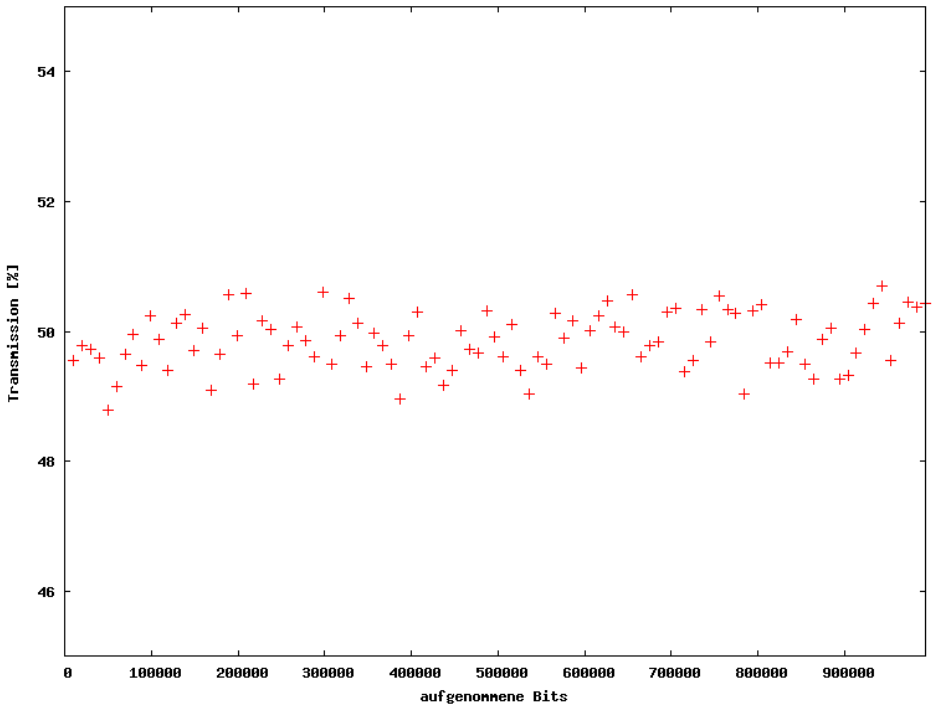


Abbildung 6: Veränderung des Strahlteilerverhältnisses über die Zeit mit Rohdaten

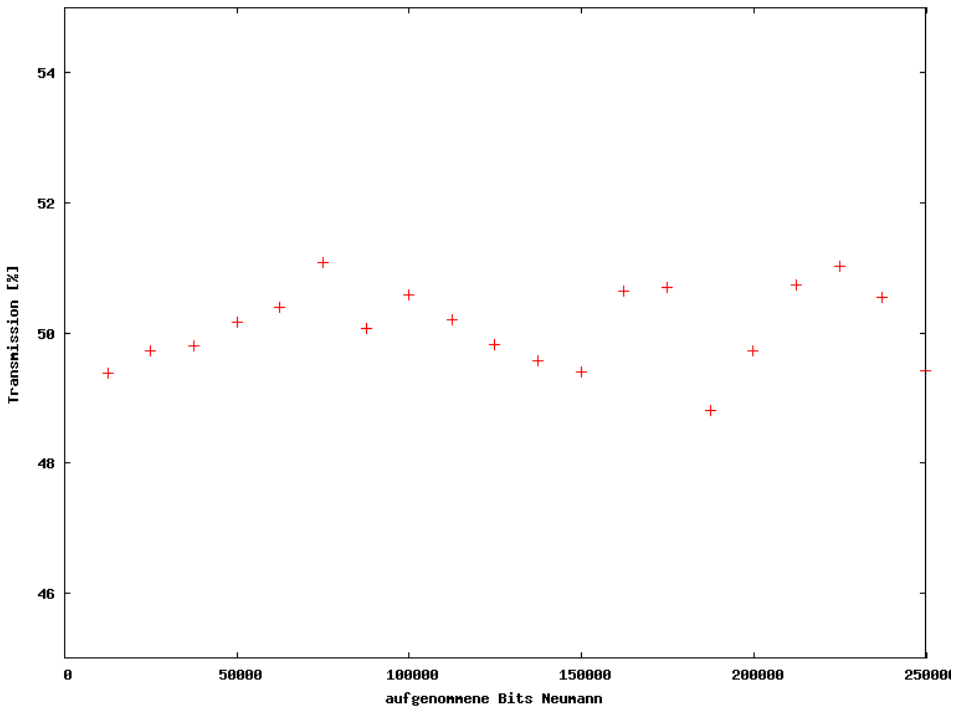


Abbildung 7: Veränderung des Strahlteilerverhältnisses über die Zeit mit Neumann-Zahlen

4 Wahrscheinlichkeit für gleich folgende Zahl

Um etwas über die Güte einer binären Zufallszahl zu sagen kann man schauen, wie oft die binäre 1 hintereinander kommt. Betrachtet man z.B. nur zwei Bits, so ist die Wahrscheinlichkeit um die Kombination 11 vorzufinden 1/4. Bei n-Bits ist die Wahrscheinlichkeit 2^{-n}. Trägt man diese Wahrscheinlichkeit logarithmisch auf, so sollte dies im Idealfall eine Gerade ergeben. Die kann man für die Rohdaten an Abbildung 8 und für die von Neumann Daten an Abbildung 9 erkennen.

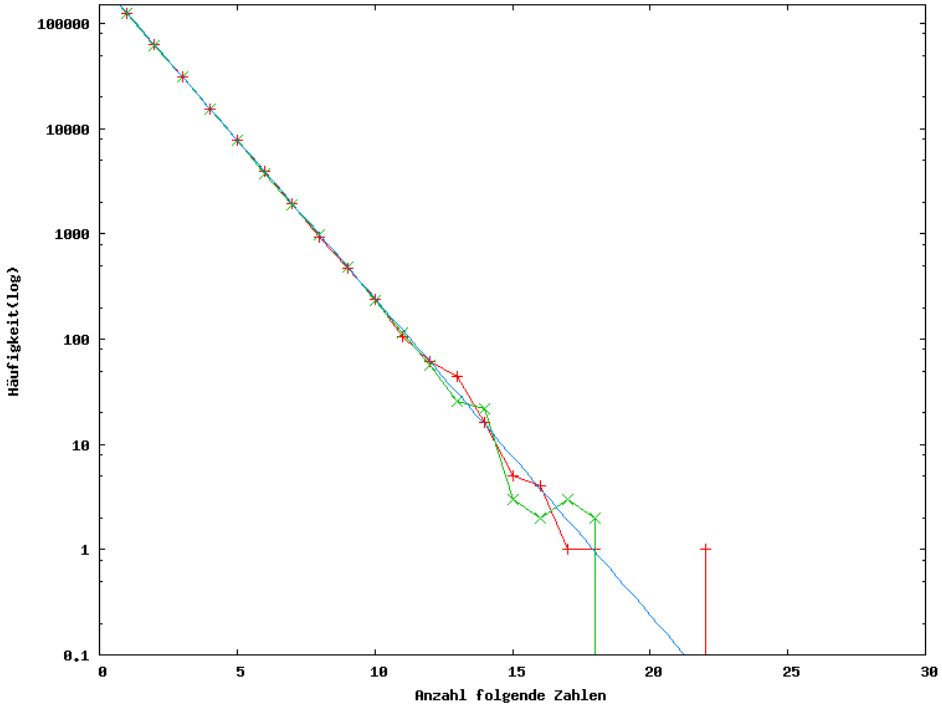


Abbildung 8: Wie oft kommt in Rohdaten die Binärzahlen hintereinander vor? Binär 1: rot, Binär 0: grün, Theorie: blau

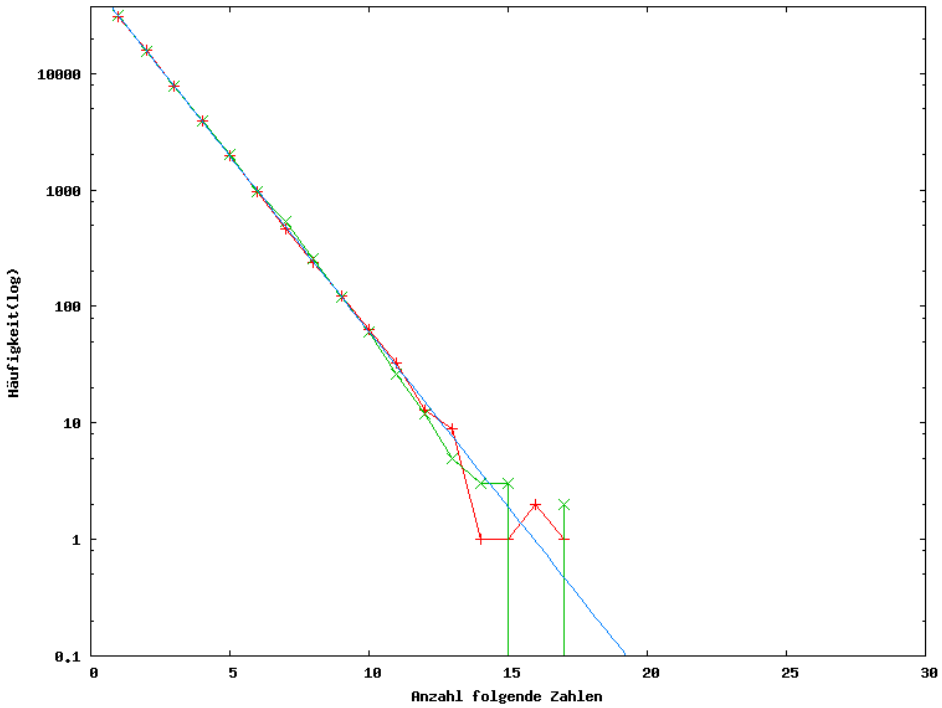


Abbildung 9: Wie oft kommt in Neumann-Zahlen die Binärzahl hintereinander vor? Binär 1: rot, Binär 0: grün, Theorie: blau

5 Aufeinanderfolgende Zahlen

Um etwas über die Güte einer Zufallszahl auszusagen, kann der Spektral-Test verwendet werden. Hier wird geschaut, ob bei drei nachfolgenden Ziffern ein bestimmtes Muster auftritt. Graphisch kann man dies durch eine 3D Darstellung veranschaulichen. Hierbei bilden jeweils drei folgende Zufallszahlen einen Raumpunkt. Je besser die Zufallszahl, desto gleichmäßiger sind die Raumpunkte verteilt. Die Verteilung der Quantenzufallszahl kann man in Abbildung 10 erkennen. Die Verteilung der Pseudozufallszahlen kann man in Abbildung 11 und 12 erkennen.

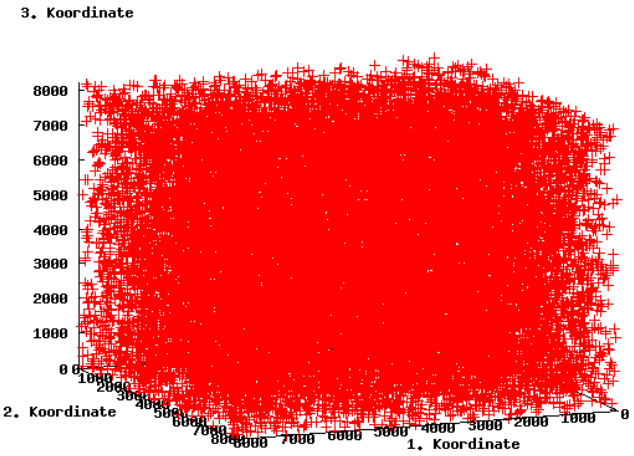


Abbildung 10: Verteilung von drei folgenden Zufallszahlen

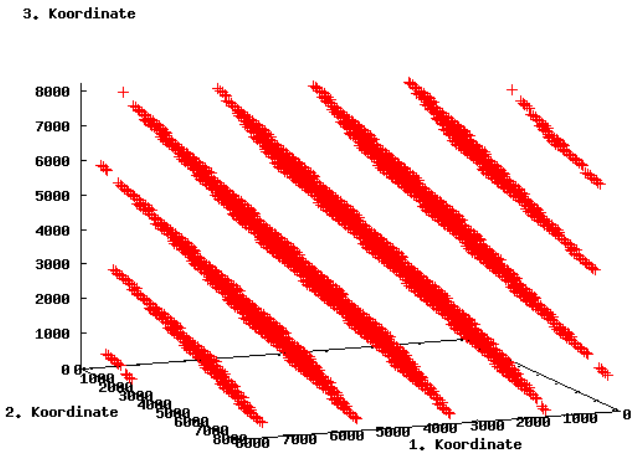


Abbildung 11: Verteilung von drei folgenden Zufallszahlen bei Pseudozufallszahl 1

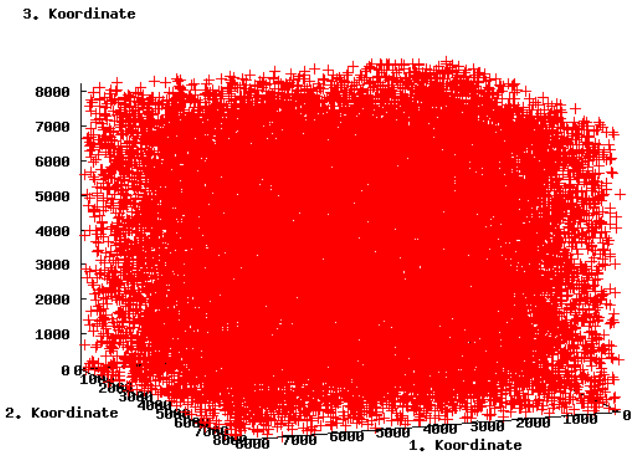


Abbildung 12: Verteilung von drei folgenden Zufallszahlen bei Pseudozufallszahl 2