Dokumentation zur IHK-Abschlussprüfung Sommer 2020

Entwicklung eines Softwaresystems

**Geschrieben von: Felix Warschewski**

**Prüflingsnummer 101 20580**

**Tag der Einreichung: 26.06.2020**

**Programmiersprache: C#**

Inhaltsverzeichnis

[1 Eigenhändigkeitserklärung 3](#_Toc44058643)

[2 Änderungen zu Tag 1 4](#_Toc44058644)

[3 Einleitung 4](#_Toc44058645)

[4 Benutzeranleitung zur Ausführung 4](#_Toc44058646)

[4.1 Laufzeitumgebung 4](#_Toc44058647)

[4.2 Installation und Aufrufen 5](#_Toc44058648)

[4.3 Dateiformat 5](#_Toc44058649)

[4.4 Aufrufbefehle 6](#_Toc44058650)

[5 Beschreibung der Klassenbibliothek 6](#_Toc44058651)

[6 Beschreibung der Zufallszahlengeneratoren und Verfahren 12](#_Toc44058652)

[7 Diskussion der Güte-Testverfahren und der Parameter für den LCG 13](#_Toc44058653)

[8 Diskussion der Testbeispiele 14](#_Toc44058654)

[9 Vergleich und Interpretation der Ergebnisse 16](#_Toc44058655)

[10 Zusammenfassung und Ausblick 18](#_Toc44058656)

[11 Programmcode im Anhang 20](#_Toc44058657)

# Eigenhändigkeitserklärung



# Änderungen zu Tag 1

Sämtliche Variablen und Eigenschaften mit dem Datentyp long wurden in double umgeändert. Dies betreffen vor allem die Einstellparameter, sowie Rechnungen und hat den Vorteil, dass sämtliche mathematische Funktionen nicht umgewandelt werden müssen.

Zur Speicherung der Beispiel-LCGs wird eine Konstanten-Klasse verwendet. In dieser werden die Beispielparameter für die LCGs als statische Eigenschaften festgelegt.

Darüber hinaus wurde anstatt einer einfachen Verteilungsklasse eine Verteilungsschnittstelle implementiert. An diese Schnittstelle wurden zwei Unterklassen angebunden (Gleichverteilung, Standardnormalverteilung). Diese Klassen implementieren die Funktion ‚transformiere‘, welche eine gleichverteilte Zufallsvariable in eine nach der entsprechenden Verteilung transformierte Zufallsvariable umwandelt. Im Falle der Standardnormalverteilung geschieht dies bspw. über die Polarmethode.

Die Polar-Klasse wird gestrichen und die Funktionalität der Polar-Methode wird in der Funktion „transformiere(x)“ der Standardnormalverteilungsklasse implementiert. Dies hat den Vorteil, dass die Funktion direkt an der richtigen Stelle ist und nicht erst noch über eine Hilfsklasse aufgerufen werden muss.

# Einleitung

Die erstellte Arbeit handelt von der Implementierung von Zufallszahlengeneratoren und das Testen der Güte mit den passenden Testverfahren. Es wurde eine Klassenbibliothek erstellt mit der man Zufallszahlen generieren kann und einen Zufallszahlengenerator, je nach eingestellter Verteilung, auf seine Güte mit einem entsprechenden Güte-Testverfahren prüfen kann. Des Weiteren wurde eine Konsolenanwendung implementiert, welche eine Eingabe-Datei mit Testparameter einliest und dynamisch nach den Eingaben die Berechnungen durchführt. Genauere Informationen befinden sich in der Benutzeranleitung.

# Benutzeranleitung zur Ausführung

## Laufzeitumgebung

Das verwendete Betriebssystem ist Windows 10 64-bit Version. Die Programmiersprache ist C# (Version C# 7.3) und es wurde in der Entwicklungsumgebung Visual Studio 2017 Enterprise Edition geschrieben. Das Zielframework der Klassenbibliothek ist .NET Standard 2.0 und das Zielframework der Konsolenapplikation ist das .NET Framework 4.7. Ursprünglich sollte die Konsolenanwendung in .NET Core programmiert werden, da dieses Framework auf einer breiteren Anzahl an Geräten läuft. Dies wurde aufgrund der Tatsache verworfen, dass der Compiler für die Core-Anwendung keine direkt ausführbare Datei generiert, sondern nur eine dll, die separat installiert werden muss.

## Installation und Aufrufen

Die Installation erfolgt über das Extrahieren der abgegebenen zip-Datei. In dieser zip-Datei wird es eine Ordnerstruktur geben. In dem bin-Ordner befindet sich die .exe einer Konsolenanwendung, eine batch-Datei, sowie zwei Ordner „Tests“ und „Ergebnisse“. Es wird empfohlen das Programm über die Batch-Datei zu starten. Hierbei werden die Testfälle, welche in den Interpretationen aufgegriffen werden, neu berechnet und in den Ordner „Ergebnisse“ abgelegt.

Auf der ersten Ebene gibt es einen zweiten Ordner mit dem Namen „Programmcode“. In diesem Ordner befindet sich die Projektmappe zu der Klassenbibliothek und der Konsolenanwendung.

Darüber hinaus sind in dem zip-Ordner eine Dokumentation und eine Entwicklerdokumentation vorhanden.

## Dateiformat

Mithilfe des args-Parameter in der Main-Methode kann ein Dateipfad übergeben werden. Dieser Pfad sollte auf eine Textdatei zeigen, in der Daten zur Bedienung der Konsolenanwendung stehen. Die batch-Datei kann ohne jegliche Vorkonfiguration gestartet werden.

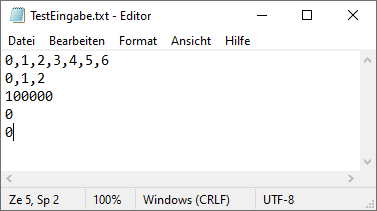


Abbildung , Eingabe-Datei

Die erste Zeile beschreibt die Zufallszahlengeneratoren, welche überprüft werden sollen. Falls mehrere Generatoren miteinander verglichen werden sollen, können diese hintereinander, mit einem Komma getrennt, aufgelistet werden. Das gleiche gilt für die Angabe der Testverfahren. In Kapitel 3.5 gibt es eine Auflistung an Möglichkeiten für die Eingabe. Die zweite Zeile beschreibt die Güte-Testverfahren, die angewendet werden sollen. Die dritte Zeile legt fest, wie hoch die Sequenzlänge ist, also wie viele Zufallszahlen für die Prüfungen erstellt werden. Die vierte Zeile legt ein k fest. Bei der seriellen Autokorrelation ist das k die Ordnung der Autokorrelation und steht für den Abstand der verglichenen Paare. Bei dem Sequenz-Up-Down-Test bestimmt das k die Länge einer bestimmten Bitfolge. Gibt man 0 für k an, erstellt die serielle Autokorrelation einen zufälligen Abstand k und bei dem Sequenztest wird über alle k iteriert und letztlich die Differenz ausgegeben. Bei dem Sequenz-Up-Down-Test ist k die Kettenlänge, welche verglichen werden soll. Die letzte Zeile gibt die Art der Verteilung der Zufallszahlen an. Man kann unterscheiden zwischen standardnormalverteilten Zufallszahlen und gleichverteilten Zufallszahlen. Hierbei sind gleichverteilte Zufallszahlen der Standard.

## Aufrufbefehle

Innerhalb der aufzurufenden Textdatei:

Zeile 1 – Generatoren:

1. Ansi-C
2. Minimal Standard
3. RANDU
4. SIMSCRIPT
5. NAG’s LCG
6. Maple’s LCG
7. Datumsbasiert(eigener)

Zeile 2 – Güte-Testverfahren

1. Serielle Autokorrelation
2. Sequenz-Up-Down-Test
3. Eigener Güte-Test

Zeile 3 – Sequenzlänge

Zeile 4 – k

Wenn k = 0 dann werden die allgemeinen Bedingungen übernommen. Siehe 6.4 Dateiformat. Wenn k <> 0 dann wird die k-te Ordnung des Verfahrens berechnet und zurückgegeben.

Zeile 5 – Verteilung

1. Gleichverteilung
2. Standardnormalverteilung

# Beschreibung der Klassenbibliothek

Der Aufbau der Klassenbibliothek und der zugehörigen Konsolenanwendung kann der Abbildung 2, Klassendiagram entnommen werden. Die drei Hauptbestandteile der Klassenbibliothek sind die Schnittstellen. Es gibt eine Schnittstelle für die Zufallszahlengeneratoren (Zufallsbibliothek), eine Schnittstelle für die Güte-Testverfahren (GüteTests) und eine für die Verteilungen (Verteilung).

Die beiden Zufallszahlengeneratoren LCG und Datumsbasiert implementieren die Zufallsbibliothek-Schnittstelle. Diese beiden Generatoren haben nun die Funktionalität Zufallszahlen zu generieren. Darüber hinaus hängt die Generierung von Zufallszahlen auch von der verwendeten Verteilung ab. Je nach Verteilung werden anders verteilte Zufallszahlen ausgegeben.

Mögliche Verteilungen sind die Gleichverteilung und die Standardnormalverteilung.

Mögliche Güte-Testverfahren sind die serielle Autokorrelation, der Sequenz-Up-Down-Test und das eigene Güte-Testverfahren.

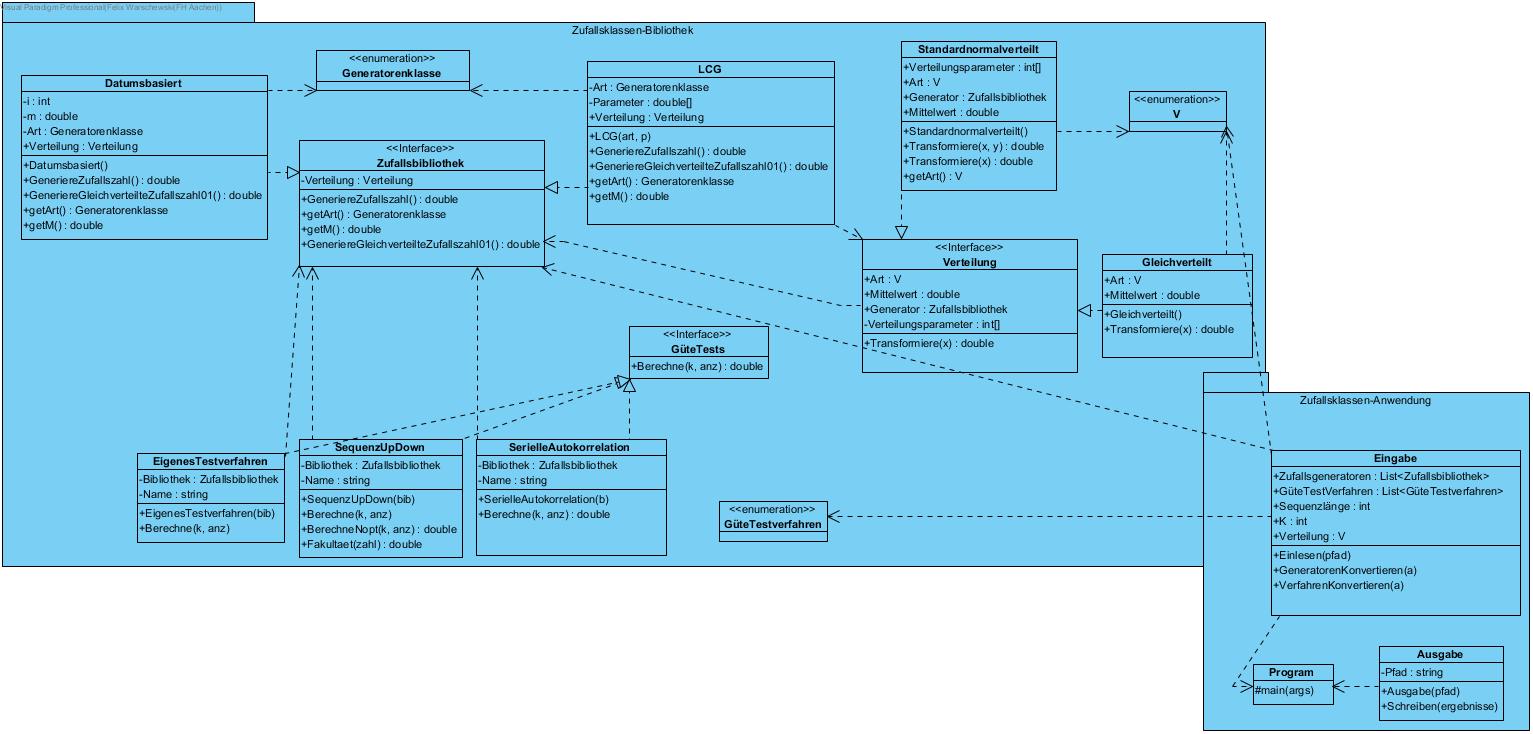
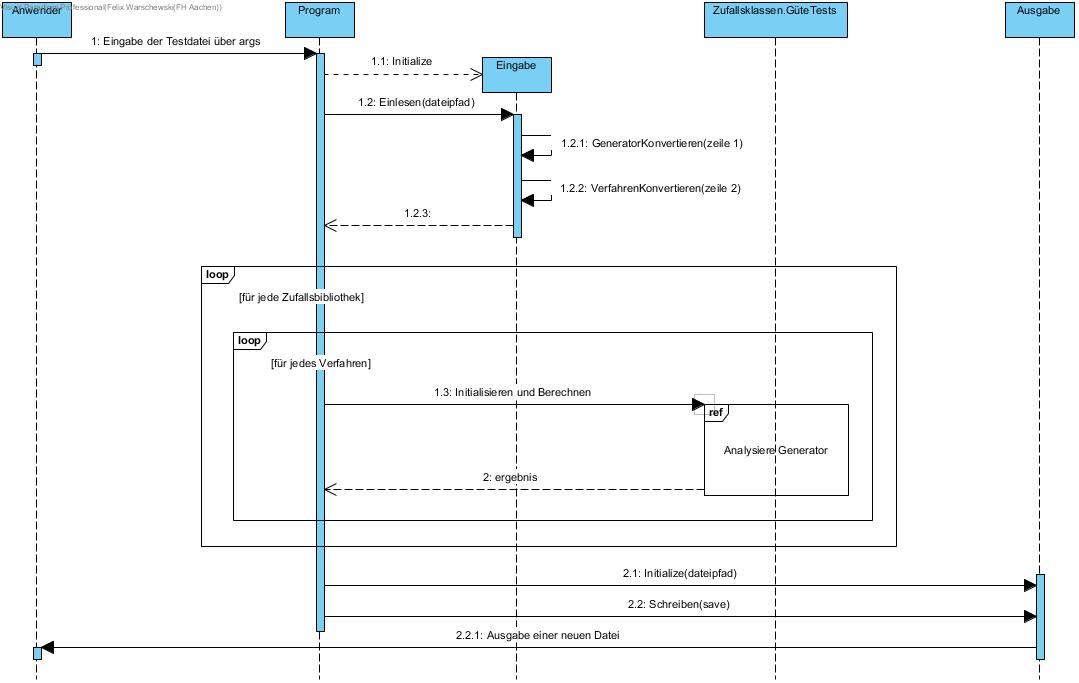
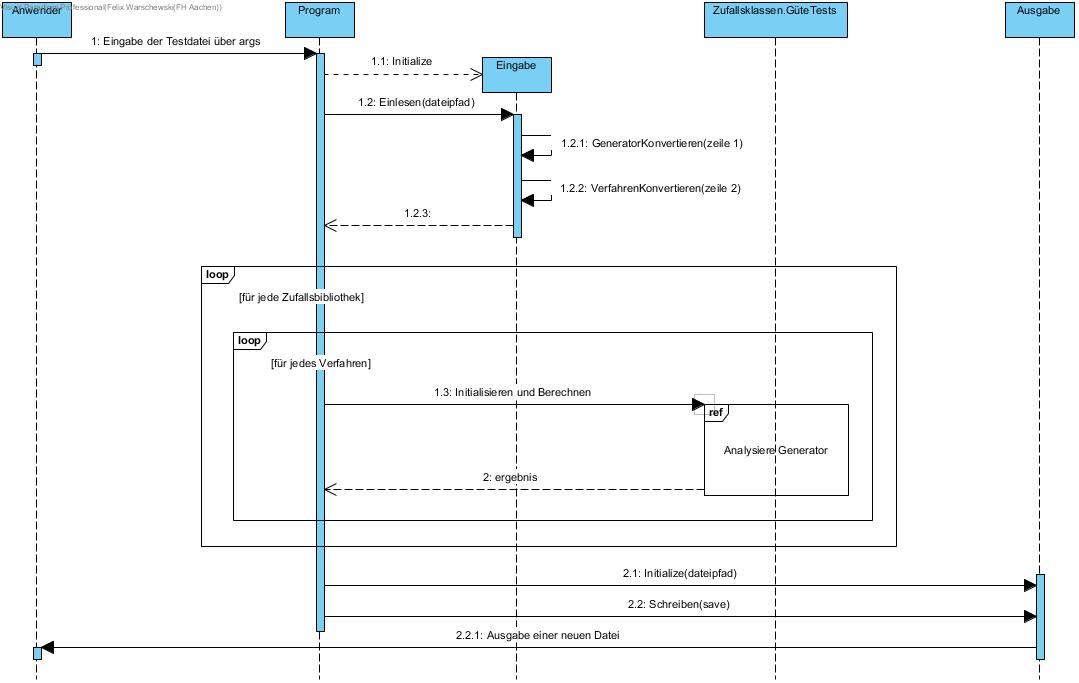


Abbildung , Klassendiagram

Der Programmablauf kann in dem Sequenzdiagramm in Abbildung 3, Testdurchlauf nachempfunden werden. Es wird die Konsolenanwendung mit einem Dateipfad aufgerufen. Dann wird die Textdatei unter dem mitgegebenen Dateipfad eingelesen. Je nachdem, wie viele Generatoren und Verfahren erzeugt werden sollen, iteriert das Programm durch die Verfahren. Am Ende werden die Ergebnisse in eine Ausgabedatei geschrieben. Der genauere Ablauf der Programmlogik wird in Abbildung 4, Analyse Generator dargestellt.

Abbildung , Testdurchlauf

In Abbildung 4, Analyse Generator ist die Initialisierung eines Zufallsgenerators dargestellt, (Im Detail Abbildung 5, Initialisiere Generator). Im Anschluss wird der Generator dem jeweiligen Testverfahren übergeben. Dann werden je nach Güte Test verschiedene Operationen ausgeführt. Diese kann man in der **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.** sehen.

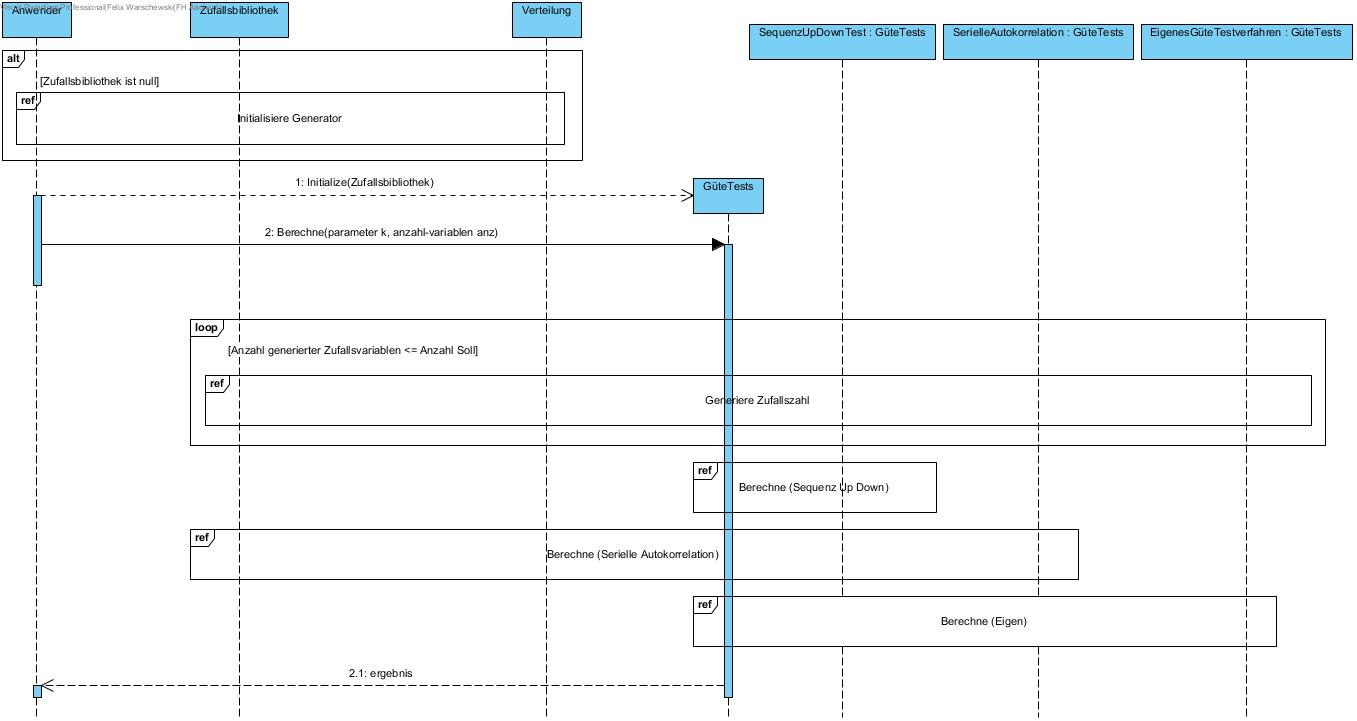


Abbildung , Analyse Generator

In der Abbildung 5, Initialisiere Generator steht beschrieben, dass die erstellte Instanz eines Zufallszahlengenerators seine Einstellparameter und ein Enum zugewiesen bekommt. Des Weiteren wird ihm eine Verteilung zugewiesen. Aufgrund dieser werden dann die Zufallszahlen generiert.

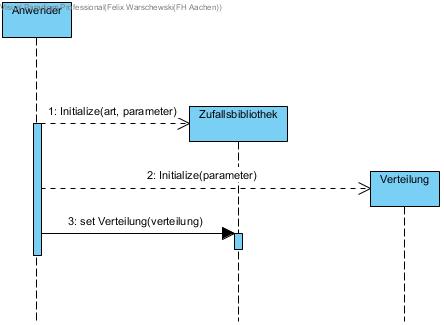


Abbildung , Initialisiere Generator

Es folgen die Hauptalgorithmen des Programmes in Form von Aktivitätsdiagrammen.

In der Abbildung 6, Generiere Zufallszahl (LCG) ist die Generierung einer Zufallszahl beschrieben. Es werden die Parameter gesetzt und mithilfe der LCG-Formel Zahlen in einem Zahlenraum von 0 bis m erzeugt. Dies ändert sich indem durch das Modul geteilt wird. Nun ergibt sich ein Zahlenraum von 0 bis 1. Je nach Verteilung werden die Zahlen erneut auf einen anderen Zahlenraum transformiert. Dies ist aber verteilungsabhängig. Letztlich wird eine Zufallszahl ausgegeben in Abhängigkeit der angegebenen Verteilung des Zufallszahlengenerators.

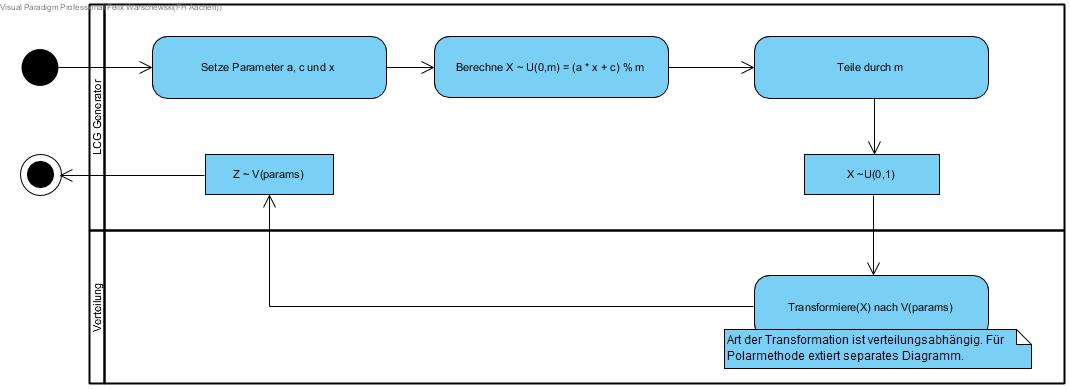


Abbildung , Generiere Zufallszahl (LCG)

In Abbildung 7, Generiere Zufallszahl Datumsbasiert ist die Logik des eigenen datumsbasierten Zufallszahlengenerators beschrieben. Es wird die aktuelle Zeit und Systemlaufzeit des Programmes aufsummiert und durch ein gegebenes Modul Modulo gerechnet und geteilt. Dies erzeugt eine Zufallszahl in einem Zahlenraum von 0 bis 1. Anschließend wird ggfls. transformiert, wenn nicht die Gleichverteilung als Verteilung angegeben ist, da alle generierten Zufallszahlen zu Beginn gleichverteilt sind.

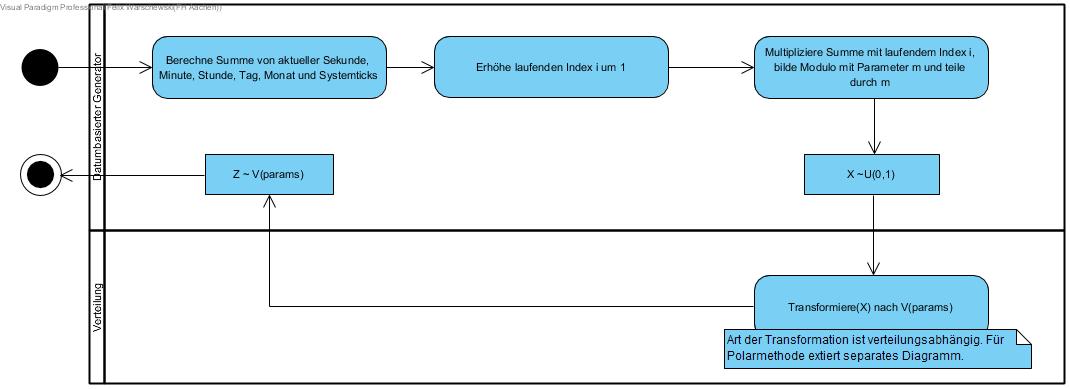


Abbildung , Generiere Zufallszahl Datumsbasiert

Die Abbildung 8, Polar-Methode (Normaltransformation) beschreibt die Polar-Methode, welche immer dann angewandt wird, wenn standardnormalverteilte Zufallszahlen generiert werden sollen. Hierfür wird ein gegebenes x verwendet und das auf den Zahlenraum -1 bis 1 transformiert. Anschließend wird ein y zufällig generiert und für die Polarmethode verwendet, falls x und y gemeinsam im Punkt im Einheitskreis liegen. Ansonsten wird solange ein y generiert bis diese Bedingung erfüllt ist. Durch die letzte Berechnung gibt die Methode eine Standardnormalverteilte Zufallszahl in dem Zahlenraum 0 bis 1 wieder.

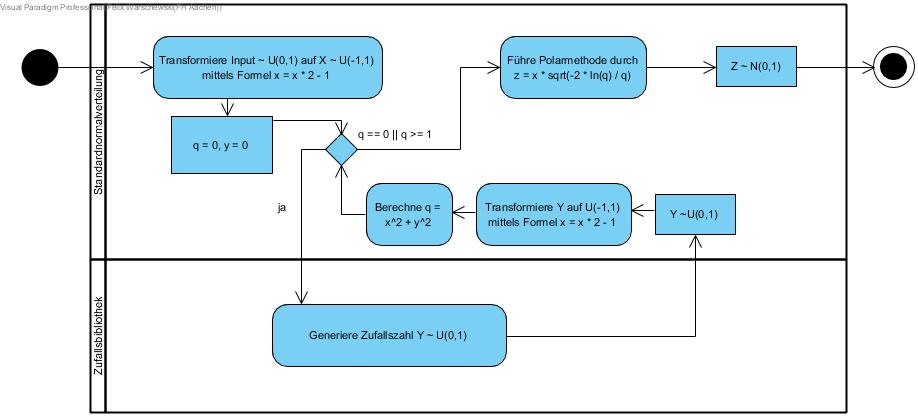


Abbildung , Polar-Methode (Normaltransformation)

In der Abbildung 9, Serielle Autokorrelation steht das Güte-Testverfahren der seriellen Autokorrelation beschrieben. Zuerst wird eine Testmenge mit einer bestimmten Größe erstellt. Anschließend wird die Abhängigkeit aller Zufallszahlenpaare mit einem gegebenen Abstand geprüft. Dies ergibt dann den Korrelationsfaktor, welcher zurückgegeben wird.

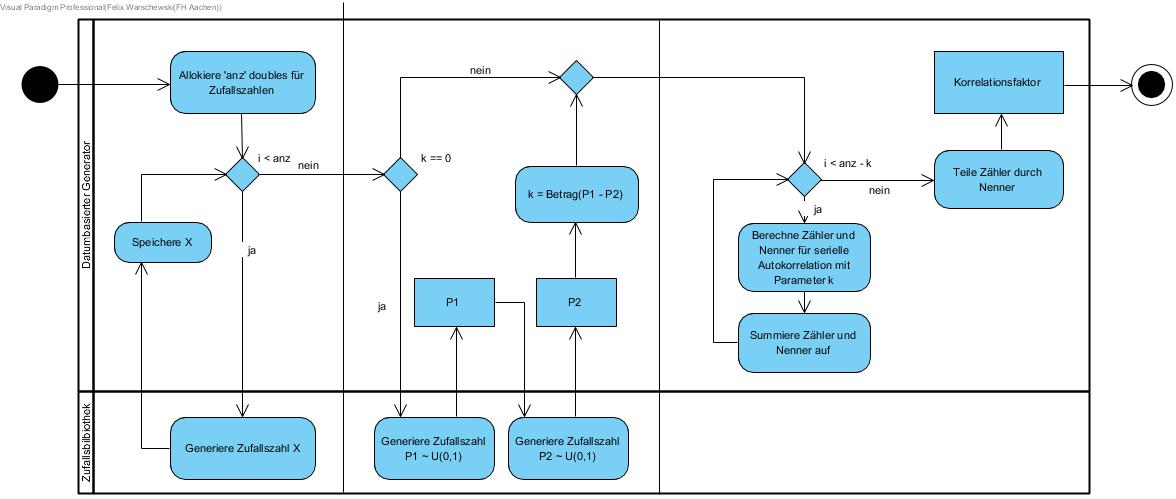


Abbildung , Serielle Autokorrelation

Die Abbildung 10, Sequenz-Up-Down-Test zeigt die Funktionsweise des Sequenz-Up-Down-Testverfahrens. Es wird eine Testmenge mit einer bestimmten Länge erzeugt und daraufhin eine Bit Maske erstellt. In der Bit Maske steht eine 1 dafür, dass das vorherige Element kleiner war als das jetzige und eine 0 für den anderen Fall. Anschließend wird zu jeder Kettenlänge die Häufigkeit ihrer Vorkommen in der Testmenge gespeichert. Falls ein k<>0 angegeben war, wird die Abweichung der Häufigkeit für die Kettenlänge mit Länge k mit der optimalen Häufigkeit zurückgegeben. Ansonsten wird die Gesamtdifferenz über alle Häufigkeiten aller Kettenlängen mit der optimalen Verteilung zurückgegeben.

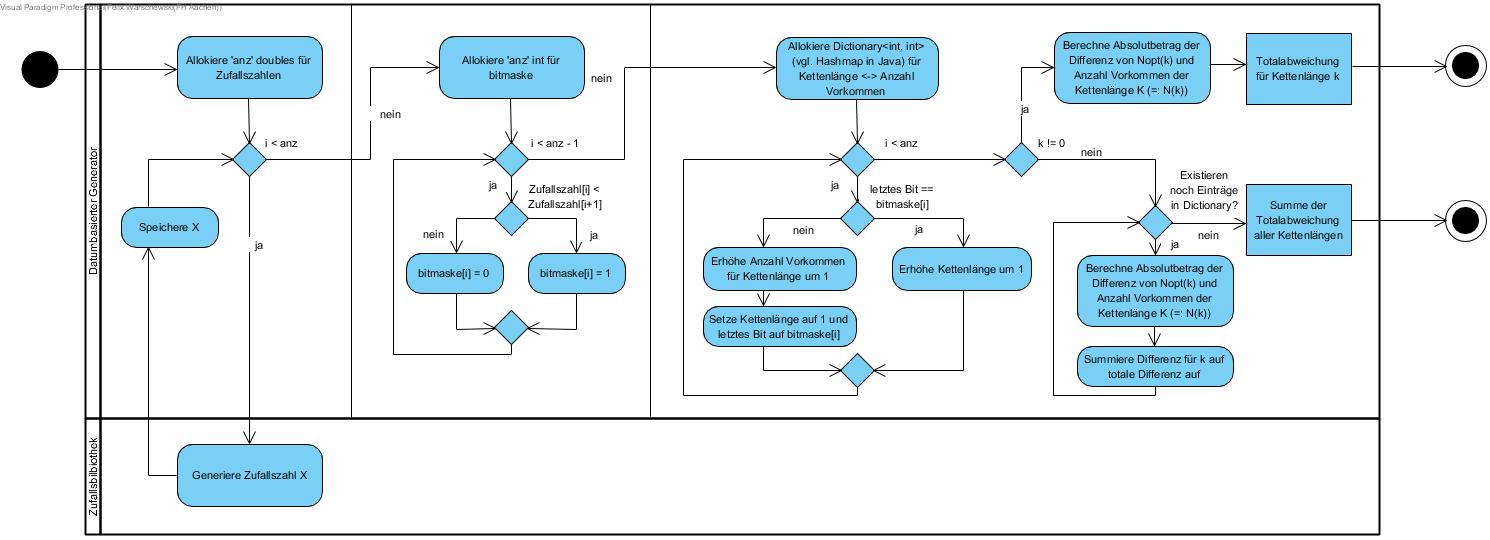


Abbildung , Sequenz-Up-Down-Test

In der Abbildung 11, Eigenes Güte-Testverfahren wird die Funktionalität des eigen entworfenen Güte-Testverfahren beschrieben. Dieses erstellt sich zuerst eine Testmenge und daraufhin eine Bit Maske exakt wie im vorherigen Güte-Testverfahren in Abbildung 10, Sequenz-Up-Down-Test. Daraufhin wird ein Mittelwert für alle Zustandswechsel in der Bit Maske generiert und zurückgegeben.

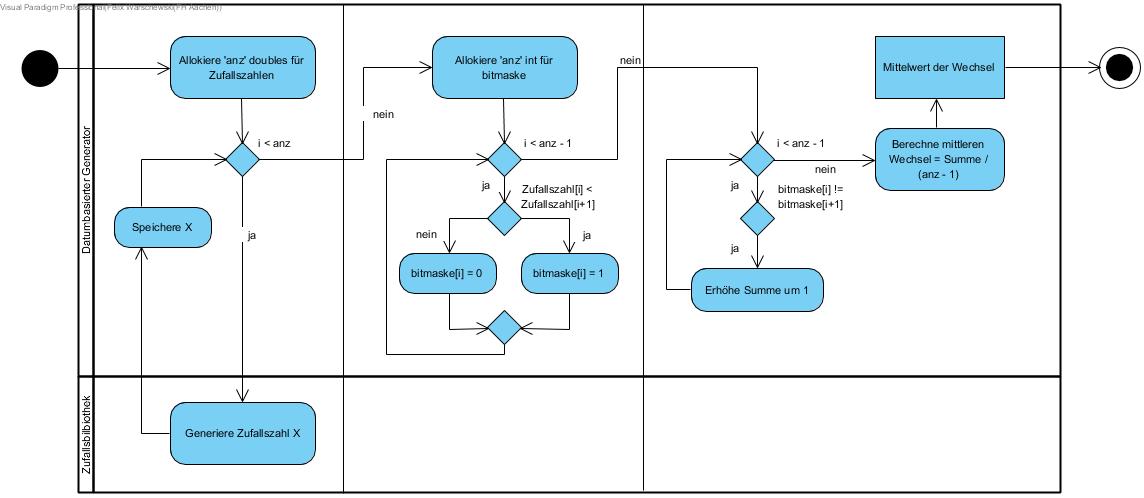


Abbildung , Eigenes Güte-Testverfahren

# Beschreibung der Zufallszahlengeneratoren und Verfahren

Zu implementieren waren folgende Generatoren und Testverfahren:

* Linearer Kongruenz-Generator mit 6 verschiedenen Einstellungsmöglichkeiten
* Umwandlung gleichverteilter in normalverteilte Zufallszahlen mithilfe der Polar-Methode
* Eigener Zufallszahlengenerator (Datumsbasiert)
* Güte-Testverfahren Serielle Autokorrelation
* Güte-Testverfahren Sequenz-Up-Down-Test
* Eigenes Güte-Testverfahren

Der Lineare Kongruenz-Generator (LCG) errechnet Zufallszahlen auf Basis der Kongruenzrechnung. Hierfür sind 4 Eingabeparameter wichtig. Das Modul m, der Multiplikator a, das Inkrement c und der Startwert x0. Des Weiteren sind 6 zu implementierende Verfahren für den LCG in Tabellenform gegeben. Diese Verfahren unterscheiden sich in der Wahl ihrer Einstellungsparameter. Der LCG funktioniert auf Grundlage einer Folge, wobei die Elemente der Folge schnell sehr groß werden und willkürlich erscheinen.

Der LCG erzeugt hauptsächlich gleichverteilte Zufallszahlen. Daher sollte eine Methode zur Transformierung von gleichverteilte in normalverteilte Zufallszahlen implementiert werden. Die Methode, welche im Programm angewendet wird, ist die Polar-Methode. Hierbei werden euklidische Koordinaten, die von den verschiedenen Zufallsverfahren generiert werden, in Polarkoordinaten umgewandelt. Wenn beide Koordinaten als Punkt im Einheitskreis liegen, werden sie zu zwei unabhängigen standardnormalverteilten Zufallszahlen transformiert. Dieses Prinzip der Verteilungstransformation kann auf jedes Verfahren des Linearen Kongruenz-Generators angewendet werden.

Der eigene Zufallszahlengenerator funktioniert auf Basis der Zeit und Laufzeit des Programms. Es werden die Sekunden, Minuten, Stunden, Tage, Monate als Integer aufsummiert, sowie die aktuelle Laufzeit des Programmes in Millisekunden. Darüber hinaus wird gespeichert, wie viele Zufallszahlen bereits mit einer Instanz des Generators erzeugt wurden. Die Summe wird mit der Anzahl der bereits erzeugten Zufallszahlen multipliziert. Das Ergebnis wird anschließend mit Modulo 1000 gerechnet und durch das Modul geteilt. So ergibt sich eine Zufallszahl zwischen 0 und 1 mit 3 Nachkommastellen. Die erhaltene Zufallszahl kann bis 1000 hochskaliert werden ohne ungenau zu werden. Will man höher skalieren benötigt man ein höheres Modul.

Das Güte-Testverfahren mithilfe der seriellen Autokorrelation misst die Abhängigkeit einer Folge von Zahlen. Die Zufallszahlen sollen paarweise möglichst unabhängig sein und im Optimalfall eine Korrelation von p=0 aufweisen. Das Verfahren verwendet eine Sequenz von Zufallszahlen, einen von der Verteilung abhängigen Mittelwert von 0,5 in der Gleichverteilung und 0 in der Normalverteilung, sowie die Ordnung k. Je nachdem wie hoch die Ordnung ist, prüft man auf weiter entfernte oder näher aneinander liegende Paare in der Sequenz. Die Wahl von k kann das Ergebnis des Güte-Tests stark beeinflussen. Daher sollte man zum Testen von bestimmten Generatoren die Verfahren mehrmals mit unterschiedlichen Ordnungen durchlaufen lassen. Wenn man in einer Textdatei kein k angibt (k=0), wird dieses zufällig generiert. Dieser Vorgang ist nur für das gegebene Programm wichtig.

Ein weiteres Güte-Testverfahren ist der Sequenz-Up-Down-Test. Dieser prüft wie viele Folgen bestimmter Länge von stetig größer oder kleiner werdenden Zahlen in einer Zufallszahlensequenz vorhanden sind. Es wird eine Bit Maske erstellt mit den Werten 0 und 1. Der Wert 0 wird in die Maske eingefügt sobald ein folgender Wert kleiner ist als der jetzige. Wenn der folgende Wert hingegen größer als der derzeitige ist, wird eine 1 in die Bit Maske eingefügt. Das Ergebnis des Verfahrens gibt einen Aufschluss darüber, wie viele Folgen es mit einer bestimmten Länge gab. Je höher die Zahl bei niedrigen Werten für k (Kettenlänge) ist, desto besser funktioniert der Zufallszahlengenerator, da die Werte öfter hin und her springen und sich nicht stetig aufbauen.

Das eigene Güte-Testverfahren erstellt auch eine Bit Maske. Hier werden alle Werte gleich dem Sequenz-Up-Down-Verfahren in die Bit Maske geschrieben. Anschließend wird die Bit Maske aufsummiert und durch die Anzahl der vorhandenen Bits der Bit Maske dividiert. Dies gibt Aufschluss über den Mittelwert der Wechsel der Zahlenfolgen. Wenn der Mittelwert deutlich unter 0,5 liegt, ist das ein Zeichen für sehr wenige Wechsel und die Entstehung längeren Folgen. Das bedeutet die Güte des Generators wäre schlechter, als wenn der Mittelwert über 0.5 liegt. Je höher desto öfter wechselt er innerhalb der Zufallszahlensequenz eine Reihenfolge und desto zufälliger werden die Zahlen generiert.

# Diskussion der Güte-Testverfahren und der Parameter für den LCG

Es werden sechs verschiedene Verfahren für den Linearen Kongruenz-Generator vorgestellt. Diese unterscheiden sich teils stark und haben deswegen auch eine andere Abfolge zur Erzeugung von Zufallszahlen.

Der Ansi-C LCG besitzt vergleichsweise große Parameter zu dem Rest der Verfahren. Schon im zweiten Schritt wird das Modul häufig übersprungen. Da das Verfahren so große Parameter besitzt, bekommt es für längere Zahlenfolgen auch immer gleichere Muster heraus und wird bei einer hohen Sequenzlänge (z.B. 10.000) schlechter abschneiden als Verfahren mit kleineren Multiplikatoren. Das Ansi-C Verfahren weist auch ein Muster von geraden und ungeraden Zufallszahlen im dauerhaften Wechsel auf. Dies liegt daran, dass das Modul eine gerade Zahl ist und der Multiplikator ungerade. Durch das ungerade Inkrement springen die Zufallszahlen immer von geraden Zahlen zu ungeraden Zahlen und umgekehrt.

Für das Minimal Standard-Verfahren wird ein ungeraderes Modul verwendet und ein deutlich kleinerer Multiplikator als bei den meisten anderen Verfahren. Der kleinere Multiplikator sorgt dafür, dass die Zahlen in den ersten Schritten nicht so häufig über das Modul herauskommen. Nichtsdestotrotz sollte durch die exponentiell ansteigende Zahl, vor Abzug des Modulo, das Modul schnell erreicht werden.

Das RANDU -Verfahren fängt mit dem Startwert 1 an und wird mit einem ungeraden Multiplikator multipliziert. Da das Modul gerade ist, bekommen wir nur ungerade Zahlen heraus. Das bedeutet die mögliche Zahlenmenge des RANDU -Verfahren ist halbiert. Des Weiteren weisen die ersten zehn generierten Zufallszahlen eine steigende Abfolge auf, obwohl das Modulo mehrmals überschritten wird. Dies sollte sehr schlechte Güte-Ergebnisse für kleine Sequenzlängen bis 10 zu Folge haben.

SIMSCRIPT besitzt als einziges Verfahren einen geraden Multiplikator und ein ungerades Modul. Das Verfahren ist von der Höhe der Parameter im Vergleich zu den anderen am meisten ausgeglichen. Daher kann die Vermutung aufgestellt werden, dass die generierten Zufallszahlen über alle Sequenzlängen am besten verteilt ist.

NAG‘s LCG generiert ausschließlich ungerade Zahlen, wobei der zur Verfügung gestellte Zahlenraum mit 2 hoch 59 deutlich über dem der anderen Verfahren liegt. Das gibt eine breitere Streuung der generierten Zufallszahlen, wenn man von der Differenz zu einem Mittelwert ausgeht. Dies könnte ein Nachteil für das Güte-Testverfahren der seriellen Autokorrelation darstellen. Des Weiteren ist der Startwert relativ hoch und das Verfahren hat früh eine gewisse Länge der Zufallszahlen erreicht. Das bedeutet das Verfahren funktioniert für eine geringe Sequenzlänge schon willkürlich, im Gegensatz zum RANDU-Verfahren.

Bei dem Maple’s LCG wird als Modul ein in Relation niedriges Modul gewählt in Kombination mit einem sehr hohen Multiplikator. Dies führt dazu, dass das Modul oft übertroffen wird. Da der Multiplikator beinahe so groß wie das Modul ist, werden vor allem Zahlen generiert, welche das Modul beinahe annähern. Daher haben diese auch im Verhältnis zueinander keine allzu großen Abweichungen und sind relativ konstant. Das kann zur Folge haben, dass das Verfahren eine relativ konstant gute Güte über diverse Sequenzlängen aufzeigt.

Um zwei Beispielverfahren aus der Menge der sechs gegebenen Verfahren zu wählen, verwende ich den Ansi-C LCG und den RANDU LCG. Beide haben ein Modul von 231. Des Weiteren haben beide Verfahren für das Modul einen geraden Wert und für den Multiplikator einen ungeraden Wert. Ohne das ungerade Inkrement des Ansi-C Verfahrens würde dieser auch ausschließlich ungerade Zahlen generieren. Durch das Inkrement werden aber gerade und ungerade Zufallszahlen im Wechsel generiert. Der Ansi-C Generator hat einen deutlich höheren Multiplikator von 1.103.515.245 im Vergleich zu dem RANDU-Multiplikator von 65.539. Das Inkrement und der Startwert bei dem Ansi-C ist auch höher. Allein dies gibt eine Aussage darüber, wie schnell der Algorithmus den Wert des Moduls erreicht und übertrifft. Wenn er den Wert des Moduls übertrifft, fängt dieser wieder bei 0 an und zählt nach oben. Ansi-C erreicht das Modul deutlich schneller und besitzt einen Wechsel von größeren und kleineren Zahlen. Der RANDU LCG hingegen braucht länger und besitzt mehr Folgen von aufeinander größer werdenden Zufallszahlen. In den folgenden Testfällen muss geprüft werden, ob dies eine Auswirkung auf die Güte des Generators hat. Sobald aber der Parameter x eine gewisse Größe erreicht hat, werden die Sprünge immer größer und das Ergebnis überschreitet öfter das Modul. Dies bedeutet, dass die Werte öfter variieren und die Folgen von aufeinanderfolgenden größer werdenden Zufallszahlen deutlich kleiner werden. Daher sollte man die beiden Zufallszahlengeneratoren mit mehreren beliebig großen Sequenzlängen testen.

# Diskussion der Testbeispiele

Die Testbeispiele geben Aufschluss über die Güte der Zufallszahlengeneratoren. Deswegen muss hier differenziert werden und es kann nicht nur ein Testverfahren mit einer bestimmten Sequenzlänge und einer bestimmten Ordnung verwendet werden. Es müssen mehrere unterschiedliche Testvorgänge durchgeführt werden.

Aus dem Kapitel 7 kann angenommen werden, dass sich die Güte der Testverfahren je nach Sequenzlänge ändern kann. Genauso können Rückschlüsse über einen Zufallszahlengenerator gewonnen werden, indem man die Abstände der verglichenen Zufallszahlen beziehungsweise die Kettenlängen der überprüften Folgen ändert. Die Änderungen kann man anhand der Variablen „k“ bestimmen, welche in der Eingabe-Datei gesetzt werden kann.

Zum Vergleich werden folgende Testfälle betrachtet. Alle Testfälle können mit ihren Werten in dem Auslieferungsordner unter „TestsZurDoku“ gefunden werden.

**Fall 1:**

Alle LCG-Verfahren mit serieller Autokorrelation für eine Sequenzlänge von 10

**Fall 2:**

Alle LCG-Verfahren mit serieller Autokorrelation für eine Sequenzlänge von 1000

**Fall 3:**

Alle LCG-Verfahren mit serieller Autokorrelation für eine Sequenzlänge von 100000

**Fall 4:**

Alle LCG-Verfahren mit Sequenz-Up-Down-Test für eine Sequenzlänge von 10

**Fall 5:**

Alle LCG-Verfahren mit Sequenz-Up-Down-Test für eine Sequenzlänge von 1000

**Fall 6:**

Alle LCG-Verfahren mit Sequenz-Up-Down-Test für eine Sequenzlänge von 100000

**Fall 7:**

Alle LCG-Verfahren mit Sequenzlänge 100000 und einem k von 1

**Fall 8:**

Alle LCG-Verfahren mit Sequenzlänge 100000 und einem k von 10000

**Fall 9:**

Alle LCG-Verfahren mit beiden vorgegebenen Testverfahren und einer Länge von 100000 und Standardnormalverteilung

**Fall 10:**

Eigener Datumsbasierter Zufallszahlengenerator für eine Sequenzlänge von 1000

**Fall 11:**

Alle LCG-Verfahren auf den eigenen Güte-Test für eine Sequenzlänge von 100000

# Vergleich und Interpretation der Ergebnisse

Um die Ergebnisse der Testfälle besser einordnen zu können, folgt eine Beschreibung ihrer Aussagekraft. Das Güte-Testverfahren der seriellen Autokorrelation fällt besser aus je näher das Ergebnis an null liegt. Wenn das Ergebnis sich signifikant von null unterscheidet, wird der Zufallsgenerator abgelehnt. In dem Fall ist dieser nicht brauchbar, da er Muster aufzeigt und voneinander abhängige Zufallszahlen bildet. Eine signifikante Unterscheidung von 0 wäre bei der seriellen Autokorrelation schon ein Wert größer 0,2 oder kleiner -0,2.

Der Sequenz-Up-Down-Test gibt einen Wert für die Gesamtdifferenz zu dem optimalen Wert aller Kettenlängen zurück. So kann gesagt werden, wie stark ein Verfahren von der optimalen Verteilung abweicht. Wenn der Wert deutlich zu den anderen gewonnen Werten ausschlägt, ist die Verteilung der Folgen von verschiedenen Kettenlängen besonders und nicht optimal. Es gibt dann Ausreißer für verschiedene Kettenlängen und dies ist ein Zeichen dafür, dass Muster gebildet werden.

Der Vergleich der Testergebnisse, sowie der Vergleich folgt zuerst in Reihenfolge der Testfälle. Es wird auf jeden Testfall eingegangen und direkte Zusammenhänge interpretiert. Die Zusammenfassung über alle Generatoren und Verfahren folgt im Kapitel 8 „Zusammenfassung und Ausblick“.

**Fall 1: Alle LCG-Verfahren mit serieller Autokorrelation für eine Sequenzlänge von 10**

Die Folge, die am schlechtesten abschneidet, ist das RANDU-Verfahren. Es wird ein Wert von 1 zurückgegeben. Dies ist der schlechtmöglichste Wert, der erreicht werden kann. Dies liegt daran, dass die Werte für RANDU in dem Intervall 1-10 stetig größer werden. Die generierten Zahlen sehen nicht aus wie Zufallszahlen, sondern wie eine immer größer werdende Folge. Das beste Ergebnis für eine derartig kleine Sequenzlänge liefert das Minimal Standard-Verfahren mit -0,2. Ein negatives Ergebnis kommt zustande, wenn mehr Zufallszahlen unter dem Stichprobenmittelwert von 0,5 liegen als darüber. Das Ergebnis ist das beste von allen sechs Generatoren. Dennoch ist der Wert keineswegs optimal. Dies liegt vor allem daran, dass alle Verfahren auf dem Linearen Kongruenz-Generator basieren und dieser wie eine Folge mit spezifischen Eingabeparametern funktioniert. Der LCG braucht eine bestimmte Menge an Durchläufen, bis er zuverlässige Zufallszahlen ausgibt. In den nächsten Testschritten wird geprüft, wie lange die verschiedenen Verfahren brauchen, um eine gute Güte zu erreichen.

**Fall 2: Alle LCG-Verfahren mit serieller Autokorrelation für eine Sequenzlänge von 1000**

Die Werte für die Güte der Verfahren hat sich deutlich gebessert. Der einzige Zufallszahlengenerator, welcher eine unbrauchbare Güte aufweist, ist der NAG’s LCG mit einer Güte von -0,42. Dieser Generator besitzt das größte Modul. Durch die extreme Breite des Zahlenraums, der mithilfe des gewählten Moduls zur Verfügung gestellt wird, treten auch stärkere Abweichungen von einem Mittelwert auf. In den folgenden Testfällen ist zu prüfen, ob sich mit einer größeren Sequenzmenge die Güte des Verfahrens verbessert.

Sehr gute Werte liefern die Generatoren Minimal Standard (0,0006) und Maple’s LCG (-0,0003). Das Maple’s Verfahren nähert, wie in Kapitel 6 beschrieben, das Modul an und liefert Zufallszahlen in einem recht konstanten Bereich. Dies reflektiert das starke Güte-Testergebnis mit der seriellen Autokorrelation bei einer Sequenzlänge von 1.000. Bei dem Minimal Standard-Verfahren wird genau das gegenteilige Prinzip angewandt. Hier ist der Multiplikator in Relation niedrig und das Modul größer als beim Maple’s LCG. Dies sorgt dafür, dass sich die Zahlen relativ schnell ausgleichen und nicht allzu weit voneinander entfernt liegen.

**Fall 3: Alle LCG-Verfahren mit serieller Autokorrelation für eine Sequenzlänge von 100000**

Für den dritten Testfall bleibt das NAG’s Verfahren das mit der schlechtesten Güte. Diese hat sich sogar mit zunehmender Sequenzlänge nochmal verschlechtert (-0,5). Dies wird vor allem durch den großen Zahlenraum, welcher durch das große Modul bereitgestellt wird, hervorgerufen. Die Werte können sich hier deutlicher unterscheiden als bei kleineren Zahlenräumen.

Die Werte für die Güte der anderen Generatoren haben sich nicht sonderlich verändert. Die besten Gütewerte haben die Verfahren RANDU (0,0018), SIMSCRIPT (-0,0013) und Maple’s (-0,0024).

Das Minimal Standard-Verfahren, welches im vorherigen Testfall die beste Güte aufzeigte, hat sich auf eine Güte von 0,01 verschlechtert. Dies kann bedeuten, dass der Minimal Standard bis 1.000 Zufallszahlen eine relativ geringe Abweichung aufweist und danach wieder mehr streut. Also wird es bei diesem Verfahren Schübe geben, in denen die Folge besser zufällig generiert werden bzw. schlechter.

Für das Güte-Testverfahren der seriellen Autokorrelation ist besonders der RANDU-Generator hervorzuheben. Bei einer sehr geringen Sequenzlänge hat dieser noch die schlechtmöglichste Güte und je größer die Zahlen werden, desto besser wird seine Güte. Darüber hinaus kann man über den NAG’s LCG sagen, dass der große Zahlenraum die Werte deutlich weiter streuen lässt und die Differenzen der einzelnen Zahlen zum Mittelwert sehr verschieden ausfallen können, was den Generator nach dem Prinzip der seriellen Autokorrelation schlecht macht.

**Fall 4: Alle LCG-Verfahren mit Sequenz-Up-Down-Test für eine Sequenzlänge von 10**

Bei dem Sequenz-Up-Down-Test schneidet der Maple’s Generator am schlechtesten ab (3,35). Es wird die Differenz für die Häufigkeit sämtlicher Kettenlängen mit der Häufigkeit im angenäherten Optimalfall gebildet. Wenn eine hohe Zahl als Güte ausgegeben wird, bedeutet dies, dass der Generator über den ganzen Verlauf der optimalen Häufigkeit verschiedener Kettenlängen relativ schlecht war. Das beste Ergebnis erzielte RANDU mit einer Güte von 0,999. Da man pro Kettenlänge die absolute Differenz auf die Gesamtgüte aufsummiert, besagt das Ergebnis wie sehr die Kurve der Optimal Verteilung approximiert wird. Für eine derartig niedrige Sequenzlänge sind die Ergebnisse nicht wirklich aussagekräftig. Dennoch kann beobachtet werden, dass der RANDU LCG am besten abschneidet, wobei das RANDU-Verfahren bei der seriellen Autokorrelation am schlechtesten bei niedrigen Sequenzlängen abgeschnitten hat. Dies zeigt, dass sich die Verfahren in der Erfassung der Güte deutlich unterscheiden.

**Fall 5: Alle LCG-Verfahren mit Sequenz-Up-Down-Test für eine Sequenzlänge von 1000**

Für diesen Testfall schneidet der NAG’s LCG am schlechtesten ab (150,15). Am besten verläuft das Testverfahren für den SIMSCRIPT-Generator mit 23,47.

Das NAG’s-Verfahren hat stärkere Ausreißer für die Anzahl mancher Kettenlängen. Also gibt es Stellen, an denen das Verfahren besonders häufig oder selten auf oder absteigende Zahlenfolgen erstellt, die an den Stellen der optimalen Verteilung liegen.

Der SIMSCRIPT hingegen hat eine relativ ähnliche Verteilung, wie die optimale Verteilung.

**Fall 6: Alle LCG-Verfahren mit Sequenz-Up-Down-Test für eine Sequenzlänge von 100000**

Das Maple’s LCG-Verfahren approximiert am besten die optimale Verteilung mit einer Gesamtdifferenz von 242,9. Der NAG’s LCG sticht deutlich mit einer schlechten Approximation hervor. Die Gesamtdifferenz liegt bei 15.000. Durch den immensen Zahlenraum und den hohen Startwert, sowie den großen Multiplikator werden die Zufallszahlen vor allem in der zweiten Hälfte des Zahlenraums generiert. Nun muss geprüft werden, ob die extremen Differenzen für kleine Zeichenketten(k) oder für große Zeichenketten(k) auftreten. Dies geschieht in den folgenden Testfällen.

**Fall 7 & 8: Alle LCG-Verfahren mit Sequenzlänge 100.000 und einem k von 1 und 10.000**

Der NAG’s LCG weist eine absolute Differenz von über 8.000 für k = 1 aufweist. Diese Differenz entsteht dadurch, dass es in dem NAG-Verfahren mehr Zeichenkettenfolgen mit der Länge 1 gibt. Der richtige Differenzwert zwischen optimaler Verteilung und NAG liegt bei -8.000. Dies bedeutet, dass es kaum immer größer werdende oder kleiner werdende Folgen gibt, sondern die Muster durch das Springen der Zufallszahlen entstehen. Es muss ein Muster vorhanden sein, sonst wäre der Wert bei der seriellen Autokorrelation nicht derartig schlecht.

Ansonsten sind keine großen Auffälligkeiten bei der Betrachtung verschiedener k mit gleicher Sequenzlänge zu sehen.

**Fall 9 & 10 & 11:**

Diese Testfälle zeigen die Funktionsweise der Polar-Methode, des eigenen Zufallszahlengenerators und der eigenen Güte-Funktion.

Bei der Anwendung der Standardnormalverteilung auf alle Zufallszahlen ist zu erkennen, dass die Werte relativ ähnlich bleiben. Es werden nur die Zahlenräume verschoben und die Gesamtzusammenhänge der Güte-Ergebnisse ändern sich nicht. Die Zufallszahlen wurden alle mit dem gleichen Verfahren von einem gleichverteilten Intervall [0,1] auf eine Standardnormalverteilung mit dem Intervall [-1,1] verschoben.

Der eigene Zufallszahlengenerator, welcher Datumsbasiert Zahlen generiert, besitzt eine nicht optimale Güte (-0,43 und 598 bei einer Sequenzlänge von 1.000). Dies könnte aber durch die Erweiterung des Moduls verbessert werden oder durch die Erweiterung der Datumsparameter.

Das eigene Güte-Testverfahren liefert den Mittelwert der Wechsel der Zahlenfolgen, d.h. wie häufig eine Folge mit stetigen Zahlen unterbrochen wird. Je höher dieser Wert ist, desto besser. In dem Testfall 11 lieferte der NAG’s LCG die besten Werte, da diese am höchsten waren mit ungefähr 0,75. Dies bedeutet, dass es kaum große Zahlenfolgen gibt, die sich stetig aufbauen.

# Zusammenfassung und Ausblick

Alle Generatoren, außer dem NAG’s LCG, weisen ab einer bestimmten Länge eine starke Güte auf.

Der NAG’s LCG liefert stetige Wechsel. Dies wurde erfasst aus dem eigenen Güte-Testverfahren und Sequenz-Up-Down. Da der Zahlenraum extrem groß ist, unterscheiden sich die Differenzen zum Mittelwert stark und es resultiert eine schlechte Güte. Der NAG’s LCG ist also kein schlechter Generator, welcher nur Muster liefert, sondern die Testverfahren waren eher auf die anderen Generatoren angepasst und nicht auf den LCG.

Ein besonderer Generator ist der RANDU LCG, welcher nur ungerade Zahlen liefert. Er ist anfangs für kleine Sequenzlängen sehr schwach, aber je größer die Sequenzlänge wird, desto besser wird seine Güte.

Alle Generatoren, ausgenommen dem NAG LCG, können aufgrund der Testergebnisse angenommen werden. Denn ab einer bestimmten Sequenzlänge funktionieren alle Verfahren sehr gut und können verwendet werden. Für alle Generatoren sollte es eine Mindestsequenzlänge größer 10 geben, da die Ergebnisse für das Güte-Testverfahren kleiner 10 zu schlecht ausgefallen sind. Die Generatoren werden somit für Sequenzlängen kleiner 10 abgelehnt.

Aufgrund der zufälligen Generierung der Testmenge kann es vorkommen, dass für manche Güte-Testverfahren ein untypisches Ergebnis herauskommt. Um dies zu verhindern, könnte eine Erweiterungsmethode geschrieben werden, die mehrmals über ein Testverfahren geht und den Mittelwert aller Ergebnisse zurückgibt. Dadurch würden nur stabile Ergebnisse zurückgeliefert werden und die Ergebnisse würden sich kaum noch unterscheiden.

Um die Funktionalität des NAG’s LCG nachzuprüfen, müsste ein weiteres Verfahren benutzt werden, was einen differenzierten Blick auf die Güte wirft. Das bedeutet, dass nicht nur die paarweisen Abhängigkeiten oder die generierten Kettenlängen verglichen werden, sondern auch andere Eigenschaften, welche zu Mustern führen könnten. Diese Güte-Testverfahren könnten dann bessere Ergebnisse für den NAG LCG erzielen.

In weiteren Schritten der Programmierung könnte man die Klassenbibliothek um weitere LCG-Schemas erweitern. Damit stellt man eine breitere Funktionalität des LCG-Verfahrens bereit. Darüber hinaus kann man mehr Verteilungen an die Verteilungs-Schnittstelle anbinden. Dies ermöglicht die Transformation von Koordinaten oder Zahlen in andere Verteilungen. Dafür müsste man lediglich eine neue Klasse anlegen mit der dazugehörigen „Transformiere()“-Methode der Verteilungsschnittstelle. Zusätzlich kann man bestehende Verteilungen um Parameter erweitern zum Beispiel Varianz und Mittelwert der Normalverteilung oder Intervallgrenzen bei der Gleichverteilung.

Des Weiteren kann man Klassen an die Güte-Tests-Schnittstelle an klemmen. Man kann mehr Testverfahren benutzen um die Güte der verschiedenen Generatoren, welche erzeugt wurden, zu bestimmen. Dies kann man alles mit beliebigen Parametern für die Anzahl der zufallsgenerierten Elemente (Sequenzlänge) und die Ordnung k der Funktion ausführen, indem die Berechne()-Methode aus dem Interface „GüteTests“ verwendet wird. Die drei Schnittstellen sind Hauptbestandteile um diverse Funktionalitäten zu erweitern, neue Tests einzuführen, in andere Verteilungen umzuwandeln oder komplett andere Zufallszahlen zu erstellen.

# Programmcode im Anhang



