## Einleitung

Der Zufall ist in der Vortragsreihe der Willms-Neuhaus-Stiftung schon aus vielfältiger Perspektive beleuchtet worden. Dennoch können wir weiter darüber wissenschaftlich diskutieren und wo das nicht weiterhilft, trefflich spekulieren. Ich werde in meinem Vortrag den wissenschaftlichen Ansatz verfolgen aber auch die Grenzen deutlich machen hinter denen die Spekulation beginnt. Der Zufall wird sie daher im weiteren Verlauf meiner Ausführungen immer wieder überraschen. Mein Vortrag allerdings soll alles andere als zufällig sein, kann aber durchaus eine instabile Wendung nehmen, wenn Fragen der Zuhörer die Ausgangsbedingungen auch nur ein wenig verändern. Natürlich habe ich auch meinen persönlichen Erfahrungshintergrund benutzt, der für Zuhörer eher zufällig erscheinen mag und ich habe Fragen an Browser formuliert und Antworten erhalten, die auf meinen persönlichen Präferenzen und denen anderer mit ähnlichen Fragestellungen beruhen.

Meinen Schwerpunkt lege ich auf Algorithmen und werde zeigen, dass Algorithmen Zufall und Chaos anschaulich machen können und dass der Zufall sich auch in Algorithmen selbst wiederfinden kann.

Für das Verständnis chaotischer Systeme werfe ich mit Ihnen einen Blick auf ein Problem, das Mathematiker und Physiker über Jahrhunderte in den Wahnsinn getrieben hat – das n-Körper-Problem. Die preisgekrönte aber leider falsche Lösung durch Henri Poincaré hat die Grundlagen der qualitativen Theorie dynamischer Systeme, der Chaos-Theorie, geschaffen. Mit einem Algorithmus zur Berechnung der Mandelbrot-Menge machen wir eine kurze Reise in das Apfelmännchen.

Die Grundlagen für Algorithmen als Computerprogramme wurden in der Welt der Automaten gelegt - als Beispiel soll uns ein Pfefferminzautomat dienen, dessen Verallgemeinerung zur Theorie endlicher Automaten führt, mit der Informatikstudenten gequält werden. Diese Theorie führt direkt zu Computern, die nichts anderes als endliche Automaten sind.

Zuletzt zeige ich Ihnen am Beispiel von Zufallszahlengeneratoren und der künstlichen Intelligenz wie der Zufall programmiert werden kann.

Die Erkenntnis, dass die Gerichtetheit der Zeit in chaotischen Systemen eine Rolle spielt, führte zu neuen Ansätzen dem Zufall wissenschaftlich zu Leibe zu rücken – der Thermodynamik und der Quantentheorie. Ich bin zuversichtlich, dass beide in der Fortsetzung der Vortragsreihe noch eine Rolle spielen werden.

## 1. Die Begriffe Zufall, Algorithmus und Chaos

### 1.1 Zufall

„Ein Zufall ist das Fehlen einer Kausalität für ein Ereignis. Es gibt kein allgemeines Gesetz und keine Absicht einer handelnden Person die das Ereignis erklärt.“

In dieser Definition stecken eine naturwissenschaftliche Perspektive (allgemeine Gesetze) und eine anthropische Perspektive (Absicht). Mit wissenschaftlichen Methoden versuchen wir Gesetzmäßigkeiten zu finden und zu beweisen, die jedes Ereignis erklären. Dafür stehen das Eindringen in immer kleinere Dimensionen und die Bemühungen eine Weltformel zu finden, in der alle physikalischen Kräfte und Teilchen konsistent zusammenpassen. Dabei stoßen wir allerdings auf die Grenzen der Berechenbarkeit, und auf Teilchen, die gleichzeitig verschiedenen Zustände annehmen und gleichzeitig an verschiedenen Orten sein können. Die naturwissenschaftliche Perspektive nähert sich dem Zufall ohne den Menschen als Akteur, obwohl natürlich auch die Wissenschaftler Menschen sind und nur deswegen überhaupt über den Zufall nachdenken können. Die anthropische Sicht schließt den Menschen als Akteur ein. Die Absicht eines Menschen ist der Grund für ein Ereignis. Philosophisch wird auch die Frage diskutiert, ob der Zufall ohne den Menschen überhaupt eine Bedeutung haben kann, denn schließlich setzt jeder Zufall ein wahrnehmendes Wesen voraus, dass in der Lage ist Kausalitäten herzustellen und ein Ereignis als zufällig zuerkennen.

## 1.2 Algorithmus

„Der Algorithmus beschreibt einen Berechnungsprozess in einzelnen Schritten, die zum Ergebnis führen".

In dieser allgemeinen Definition ist der Algorithmus universell und begegnet uns schon bei der Addition ganzer Zahlen. Das Wort Algorithmus selbst ist eine Verballhornung des Namens von Mathematiker Muhammaed Al-Khwarizmi. In der lateinischen Übersetzung seines Werkes über das hinduistische Dezimalsystem heißt es „Liber Algorismi de Numero Indorum". Der Algorithmus wird zur Steuerung von Automaten eingesetzt die mit Eingangsdaten unter Berücksichtigung des momentanen Zustands des Automaten Ausgangsdaten erzeugen. Heutzutage sind diese Automaten in der Regel Computer.

Algorithmen müssen folgende Anforderungen erfüllen, wenn sie als Computerprogramm eingesetzt werden:

- Ausführbarkeit – es muss einen Automaten geben, der jeden Schritt des Algorithmus ausführen kann
- Eindeutigkeit – nach jedem Schritt muss eindeutig klar sein, welcher Schritt als nächstes folgt
- Endlichkeit – der Algorithmus darf nur endliche viele Schritte umfassen
- Speicherbarkeit – für jeden Schritt darf nur ein endlich großer Arbeitsspeicher eingesetzt werden
- Allgemeinheit – der Algorithmus löst nicht nur einen Spezialfall, sondern eine Klasse von Problemen
- Terminiertheit – der Algorithmus soll nach endlich vielen Schritten stoppen

Es gibt allerdings Algorithmen, die nur durch äußere Einflüsse stoppen. Das sind zum Beispiel Echtzeitsysteme, die in einer Endlosschleife auf Nachrichten von Anwendern oder Sensoren warten und dann entsprechende Pfade des Algorithmus ausführen. Ein allgemeines Beispiel eines solchen Algorithmus ist das Betriebssystem eines Computers.

## 1.3 Chaos

„Das Chaos ist die Verhaltensweise deterministischer, nicht linearer dynamischer Systeme, bei der irreguläre, aperiodische Zeitpfade der Systemvariablen erzeugt werden".

Etymologisch aus dem Altgriechischen stammend, ist das Chaos ein Zustand vollkommener Unordnung und damit der Antipode des Kosmos als Weltordnung (Kosmos). Das weist eher auf die Entropie des Universums, einem Begriff aus der Thermodynamik, hin. Die Mathematiker haben dem Begriff einen besser beherrschbaren Inhalt gegeben.

Deterministisch ist ein System, wenn es durch lösbare Gleichungen beschrieben ist. Als nicht lineares dynamisches System kann man sich z.B. unser Sonnensystem vorstellen. Irreguläre Zeitpfade der Systemvariablen entstehen hier durch die Kollision von Massen.

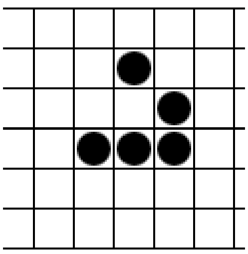
Die Chaos-Theorie untersucht genau solche Prozesse bei denen kleinste Störungen zu exponentiell anwachsenden Fehlern führen und bei denen daher der Zustand zu einem bestimmten Zeitpunkt nicht vorhersagbar ist. Sie grenzt sich ab von regulären Prozessen bei denen Störungen höchstens linear wachsende Fehler erzeugen und auf der anderen Seite stochastischen Prozessen, die nur durch Wahrscheinlichkeitsverteilungen zu beschreiben sind.

## 1.4 Die Grenzen der Berechenbarkeit

Die Wissenschaft hat besonders im Zeitalter der Aufklärung versucht Zufälle auszuschließen und für alle Ereignisse Kausalitäten zu finden – alles ist messbar. Pierre-Simon Laplace behauptete 1776, dass man den Zustand des Universums für künftige Jahrhunderte genau bestimmen könne, wenn man nur den augenblicklichen Zustand genau bestimmen könne. Es gäbe eben nur zu wenig Wissen um die derzeitigen exakten Ausgangsbedingungen. Gleichwohl könne man sich ein Wesen denken, dass über all das fehlende Wissen verfüge und damit in der Lage wäre die Vorhersage zu treffen. Dieses Wesen ist als der Laplace'sche Dämon in die Wissenschaftsgeschichte eingegangen.

Abgesehen von dem unendlichen Aufwand den es bedeuten würde mit der nötigen unendlichen Genauigkeit zu rechnen, hat Henri Poincaré 1903 bewiesen, dass eine Klasse von Funktionen bei der kleinsten Veränderung der Ausgangsbedingungen gänzlich unterschiedliche Ergebnisse produziert und damit unberechenbar wird.

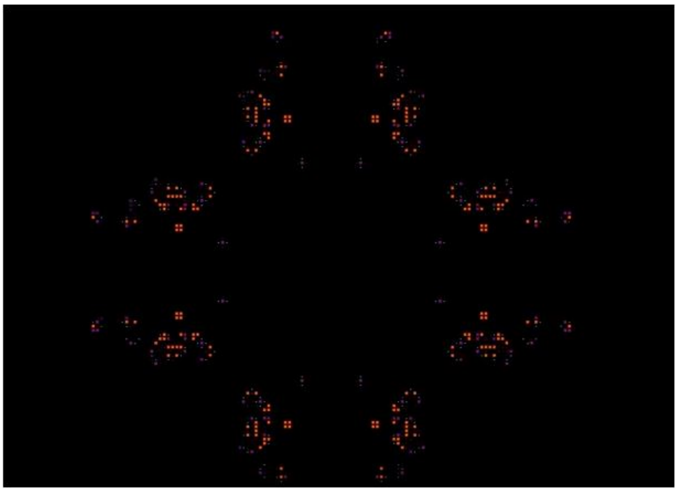
Mit den Grenzen der Berechenbarkeit eng verbunden ist das Problem der Entscheidbarkeit, das mit der Forderung ein Algorithmus solle nach endlich vielen Schritte terminieren elegant umgangen wird. Ein anschauliches Beispiel für ein nicht entscheidbares Problem ist John Conways game of life.



Eine Population von Zellen lebt in einer zweidimensionalen Matrix. Sie können entweder tot oder lebendig sein. Drei einfache Regeln bestimmen, ob eine Zelle tot oder lebendig ist:

- Eine Zelle wird lebendig, wenn 3 ihrer 8 Nachbarn leben
- Eine Zelle stirbt wegen Überbevölkerung, wenn 4 ihrer Nachbarn leben
- Eine Zelle stirbt wegen Vereinsamung, wenn höchstens ein Nachbar lebt

Die Frage ist, ob die Population unsterblich ist für eine beliebige Ausgangspopulation. Ein Algorithmus, den man dazu leicht beschreiben kann, terminiert, wenn die Population ausstirbt. Überlebt sie aber, befindet er sich in einer Endlosschleife.



QR-Code einscannen,
um die Animation zu öffnen

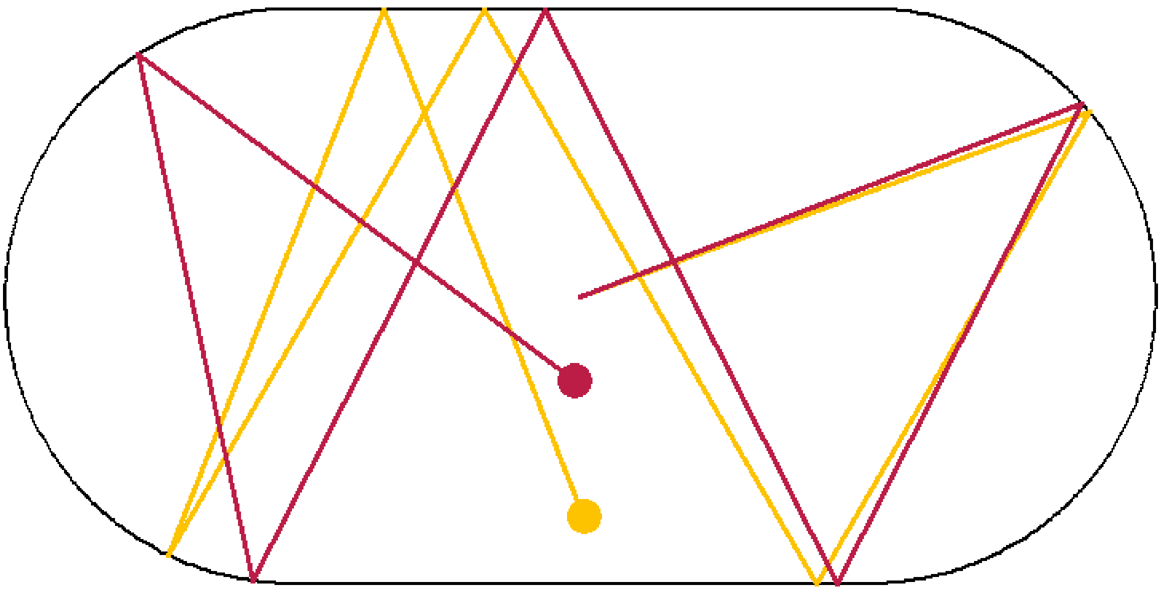
# 2. Algorithmen und Chaos-Theorie

## 2.1 Abgrenzung

Wie schon gesagt, beschränkt sich die Chaos-Theorie auf deterministische dynamische Systeme die durch lösbare Gleichungen beschrieben werden. Dabei werden Systeme ausgegrenzt die

- stochastisch sind und mit Wahrscheinlichkeitsverteilungen beschrieben werden
- linear sind und damit reproduzierbare Ergebnisse liefern
- periodisch sind
- nicht dynamisch sind

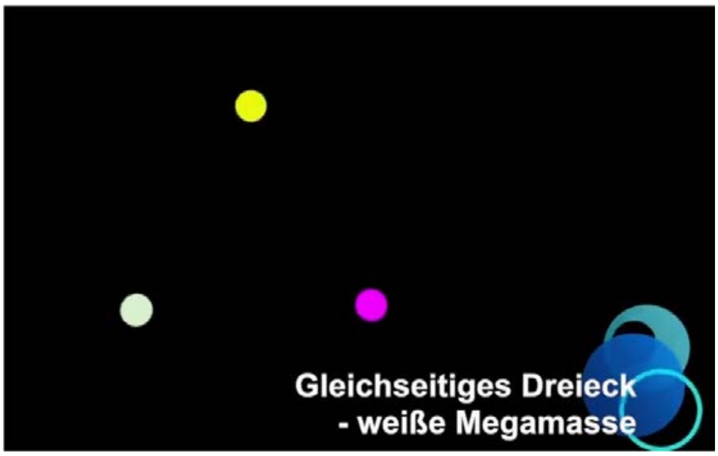
Die entscheidende Eigenschaft chaotischer Systeme ist, dass kleinste Fehler sich exponentiell verstärken. Das Beispiel einer Billardkugel kann die Eigenschaft veranschaulichen:



Angenommen, die Kugel könnte ohne Energieverlust rollen, würden sich dennoch kleinste Fehler bei jedem Anstoß der Bande verstärken. Schon nach kurzer Zeit könnte die Position der Kugel nicht mehr vorhergesagt werden. Eine Vorhersage würde wieder den allwissenden Laplace'schen Dämon erfordern der in der Lage wäre z. B. auch noch die kleinste Bewegung unter dem Eis des Jupitermondes Europa mit zu berücksichtigen.

## 2.2 n-Körper-Problem

Ich gehe kurz ein auf das unter Mathematikern wohlbekannte 3-Körper-Problem das Jahrhunderte lang kluge Köpfe zu rauchen gebracht hat. Es verallgemeinert die Lösung, die Isaac Newton für die Zustandsentwicklung eines Systems mit 2 Körpern, z.B. ein Doppelsternsystem ohne Planeten, gefunden hat. Für ein solches System ist analytisch mit Differentialgleichungen die Bewegung und die Position der Sterne zu jedem Zeitpunkt (Vergangenheit oder Zukunft) bestimmbar. Sobald aber mindestens ein dritter Körper hinzukommt, versagt der Lösungsansatz. Die Frage war: Lässt sich die Bewegung von n Massepunkten, deren Positionen und Geschwindigkeiten zu einem Zeitpunkt bekannt sind für alle Zukunft vorhersagen?




Von Mar Schneider - Eigenes Werk

QR-Code einscannen,
um die Animation zu öffnen

König Oscar II. von Schweden und Norwegen hatte einen Preis auf die Lösung des Problems ausgesetzt. Es wurden aber keine vollständige Lösung eingereicht. Dennoch wurde der Preis an Henri Poincaré vergeben, der seine fehlerhafte Lösung anschließend noch heftig korrigieren und schließlich auf seine Kosten erneut veröffentlichen musste. Heute wird auch sein Beweis nicht anerkannt denn eigentlich hatte er nur bewiesen, dass ein spezielles Verfahren zur Lösung scheitern muss.
Die besondere Schwierigkeit liegt darin, dass die beteiligten Massen kollidieren können und dass dadurch jede mögliche Konvergenz unmöglich wird. Massen können dadurch sogar in endlicher Zeit ins Unendliche verschwinden.
Eine Lösung des Problems gibt es aber tatsächlich – Das 3-Körper-Problem wurde gelöst von Karl Sundman 1990 und Wang Qiu-Dong verallgemeinerte es für das n-Körper Problem.

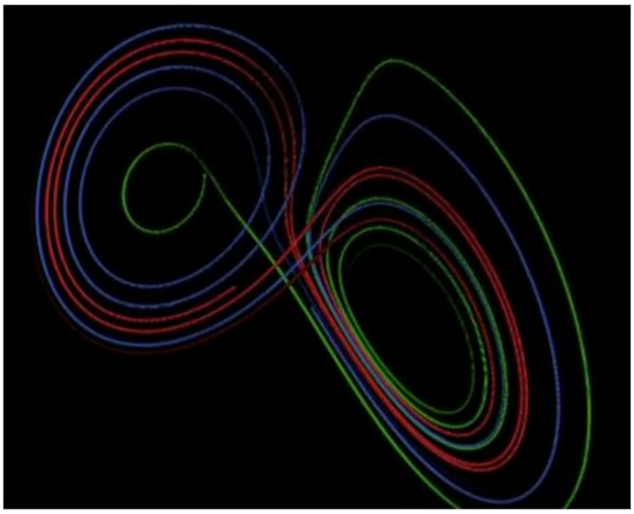
## 2.3 Eigenschaften chaotischer Systeme

Obwohl die Entwicklung chaotischer Systeme nicht vorhersagbar (zufällig) ist, sind doch bestimmte Verhaltensmuster erkennbar. Diese Muster lassen sich in chaotischen Systemen aus gänzlich unterschiedlichen Bereichen z.B. Turbulenzen, Vibrationen, Wettergeschehen nachweisen. Sie sind von universeller Bedeutung. Um das deutlich zu machen wird der Zustand eines Systems zu jedem Zeitpunkt durch einen Punkt in einem Raum dargestellt. Die Dynamik lässt sich damit als die Bahn des Punktes im Raum interpretieren.

In manchen Fällen streben Systeme mit verschiedenen Anfangsbedingungen zu demselben Verhalten; die Punktbahnen im Raum konvergieren dann zu einer bestimmten Bahn, dem Attraktor. Es gibt punktförmige Attraktoren oder Kurven.

Systemeigenschaften

1. Attraktoren



QR-Code einscannen,
um die Animation zu öffnen

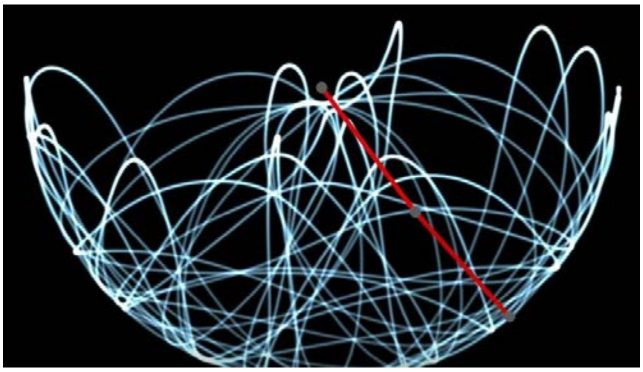
Die Punkte haben zunächst nahezu identische Bahnen und zeigen dann chaotisches Verhalten mit deutlichem Attraktor.

Neben den Attraktoren sind weitere Eigenschaften chaotischer Systeme entdeckt worden. Dafür benutzte der Meteorologe Edward Lorenz Gleichungssysteme, die Merkmale des Wettergeschehens abbildeten. Er entdeckte

- die Quasiperiodizität, das Wettergeschehen verläuft zyklisch aber nie gleich
- die Sensitivität, kleinste Veränderungen haben langfristig großen Einfluss (Schmetterlingseffekt)

Systemeigenschaften

1. Attraktoren
2. Quasiperiodizität
3. Sensitivität



QR-Code einscannen,
um die Animation zu öffnen

Als Beispiel dient ein Doppelpendel bei dem an einem Pendel ein weiteres Pendel gelagert wird (rote Linie). Der Bahnverlauf (weiße Linie) ist chaotisch, sensitiv gegenüber Anfangsbedingungen und äußeren Einflüssen, erfolgt aber ähnlich.

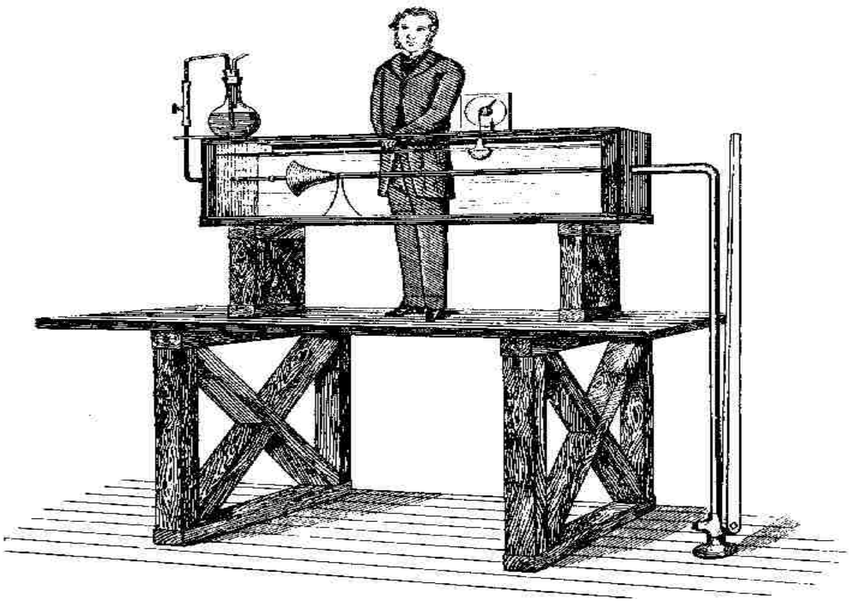
Osborne Reynolds untersuchte Turbulenzen an einem Hindernis in fließenden Flüssigkeiten. Er entdeckte, dass die Entstehung von Turbulenzen von den Faktoren

- Fließgeschwindigkeit
- Zähigkeit der Flüssigkeit (Viskosität)
- Trägheitskräfte (z.B. Reibung)

abhängt. Er bewies, dass der Übergang von regulärem zu turbulentem Verhalten Gesetzmäßigkeiten folgt und beschrieb diese in der Reynoldszahl (Verhältnis von Trägheits- zu Zähigkeitskräften) die für gegebene Verhältnisse empirisch bestimmbar ist.

Systemeigenschaften

1. Attraktoren
2. Quasiperiodizität
3. Sensitivität
4. **Reynoldszahl**

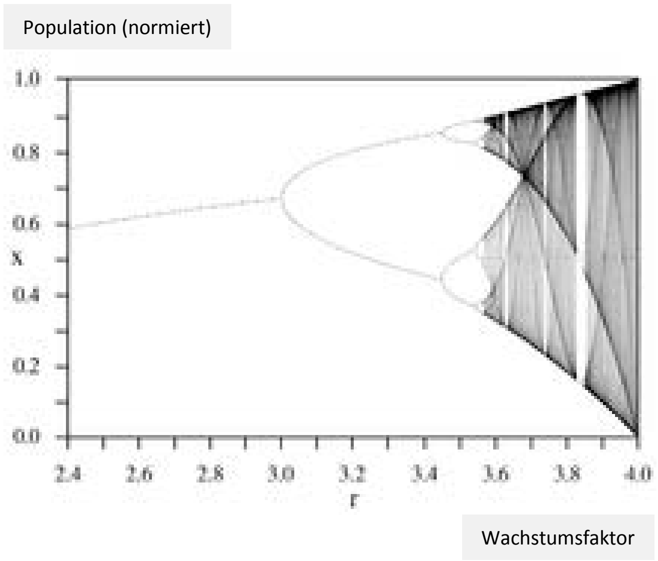


Osbourne Reynolds mit seinem Versuchsaufbau

Der Biologe Robert May untersuchte die Entwicklung von biologischen Populationen (z.B. Kaninchen) mit einer nichtlinearen iterativen Gleichung, die Geburt- und Sterberate mit Nahrungsangebot und Feinden rückkoppelt. Er stellte dabei fest, dass das System zunächst einem Attraktor zustrebt, sich dann aber aufspaltet und ein zweiter Attraktor erscheint, genannt Bifurkation.

Systemeigenschaften

1. Attraktoren
2. Quasiperiodizität
3. Sensitivität
4. Reynoldszahl
5. **Bifurkation**
6. **Feigenbaum-Konstante**



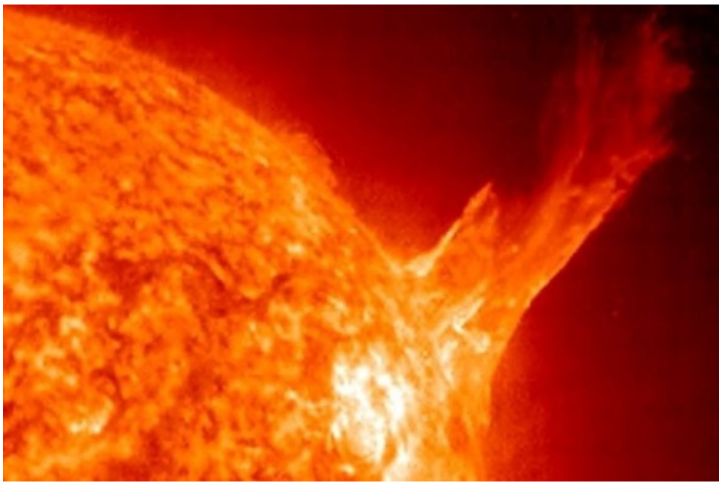
Die Population folgt einem Attraktor bis zum Wachstumsfaktor 3. Bei größeren Faktoren erscheinen weitere Attraktoren.

Mitchell Feigenbaum setzte die Forschung fort und konnte schließlich nachweisen, dass in solchen Systemen die Bifurkationen immer schneller aufeinander folgen bis hin zu unvorhersehbar großen Schwankungen von Generation zu Generation. Er leitete daraus eine Konstante, die Feigenbaum-Konstante ab.

Robert May fand noch weitere Organisationsmuster im Chaos. Er stellte fest, dass in der Entwicklung der Population nach Zuständen mit Bifurkationen in jeder neuen Generation auch kurzzeitig wieder stabile Verhältnisse entstehen können die berechenbar und vorhersagbar sind und nannte diese Intermittenzen. Sie treten z.B. beim Sonnenwind, einem von der Sonne ausgehenden Partikelstrom, auf.

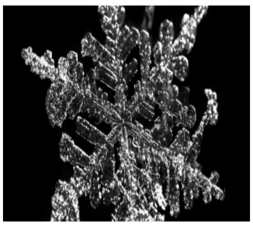
**Systemeigenschaften**

1. Attraktoren
2. Quasiperiodizität
3. Sensitivität
4. Reynoldszahl
5. Bifurkation
6. Feigenbaum-Konstante
7. **Intermittenzen**



Benoit Mandelbrot entdeckte, dass sich die Gesetzmäßigkeiten des Chaos in der Natur wiederfinden. Er veröffentlichte in seinem Buch „Die fraktale Geometrie der Natur" seine Erkenntnis, dass es in der Natur keine gradlinige Geometrie gibt. Er konnte zeigen, dass die Natur einem grundlegenden Bauprinzip folgt das in jedem Maßstab wiederholt wird.

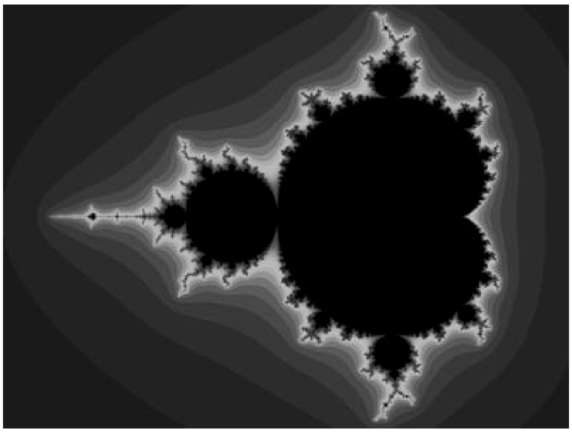




Mandelbrot nannte diese selbstähnlichen immer kleiner werdenden Strukturen Fraktale (von lat. frangere - zerbrechen) und machte diese anschaulich mit der Mandelbrot-Menge die sich aus der Iteration der Gleichung $z = z^2 + C$ ergibt. In der Darstellung als Punktebahn ergibt sich daraus das berühmte Apfelmännchen. Fraktale haben die Eigenschaft der Selbstähnlichkeit und besitzen mathematisch gesehen keine ganzzahlige Dimension.

Systemeigenschaften

1. Attraktoren
2. Quasiperiodizität
3. Sensitivität
4. Reynoldszahl
5. Bifurkation
6. Feigenbaum-Konstante
7. Intermittenzen
8. **Fraktale, Selbstähnlichkeit**



QR-Code einscannen,
um die Animation zu öffnen

Die Erkenntnisse aus der Chaos-Theorie werden in Simulations- und Prognosesystemen in den verschiedensten Fachgebieten benutzt. Dazu gehören neben den Meteorologen auch Historiker Volkswirte und Psychologen.

## 3. Algorithmen und Automaten

Unser heutiges Wissen um die Macht und die Grenzen von Algorithmen wurde wesentlich geprägt durch das in den 60er Jahren des letzten Jahrhunderts entwickelte Konzept endlicher Automaten. Noch heute ist es der Ausgangspunkt der theoretischen Informatik und ist stets Thema im ersten Semester theoretische Informatik. Die Frage war, wie abstrakte Automaten unabhängig von ihren physikalischen Bauteilen dargestellt werden können. Später kam die Erkenntnis hinzu, dass die Komplexität der Automaten nur beherrschbar wird durch die Verwendung weniger einfacher Bauteile und deren Kombination. Das Konzept endlicher Automaten ist eingegangen in die Entwicklung digitaler Schaltungen und generell in die Softwaretechnik.

### 3.1 Der Pfefferminzautomat

Am Beispiel des einfachen Pfefferminzautomaten wird der Abstraktionsschritt sichtbar.


Zunächst betrachtet man die Einflüsse, die auf den Automaten einwirken können (Gewalt, Witterung, Verschleiß einmal ausgenommen). Es sind nur wenige:

- M = Münze einwerfen
- R = Geldrückgabeknopf drücken
- W = Warenausgabe wählen

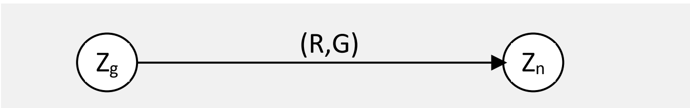
Ebenso ist die Anzahl der Reaktionen des Automaten begrenzt:

- G = Münze auswerfen
- A = Ware auswerfen
- K = keine Reaktion

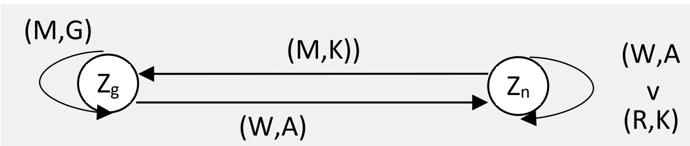
Zusätzlich kann der Automat verschieden innere Zustände besitzen in deren Abhängigkeit verschieden Reaktionen auf einen Eingangsreiz möglich sind:

- $Z_n$ = neutraler Zustand
- $Z_g$ = geladener Zustand nach Einwurf einer Münze

Der Zustand des Automaten kann durch ein passendes Eingangssignal verändert werden. Zum Beispiel geht der Automat aus dem Zustand „geladen“ in den Zustand „neutral“ über, wenn der Rückgabeknopf gedrückt wird. Dabei wird außerdem die Reaktion Münze auswerfen erzeugt. Man beschreibt diesen Sachverhalt in einem Zustandsdiagramm:




Die vollständige Beschreibung des Pfefferminzautomaten sieht dann so aus:




und vereinfacht für beliebige Reiz- und Reaktionsmengen und beliebige Automaten

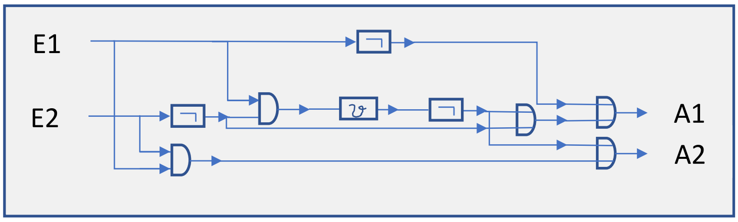

Mit drei weiteren Abstraktionsschritten nähern wir uns der digitalen Rechnerwelt.

- Alan Turing erdachte 1936 einen einfachen Automaten, der eine Zeichenkette Schritt für Schritt verarbeitet und stoppt, sobald eine Lösung gefunden wurde – die Turingmaschine. Mit ihr konnte er beweisen, dass jedes vorstellbare mathematische Problem zu lösen ist, sofern dieses auch durch einen Algorithmus gelöst werden kann.
- Die Realisierung eines Algorithmen verarbeitenden Automaten mit wenigen Bausteintypen die für sich genommen einfachste endliche Automaten sind, nämlich

- Und (∧, )
- Oder (∨, )
- Negation (¬, )
- Verzögerung (ν, ) speichert einen Zustand

- Jetzt müssen wir nur noch die Eingangs- und Ausgangssignale codieren. Für die 3 Ein- und Ausgänge des Pfefferminzautomaten reichen jeweils 2 Leitungen, wenn man sie dual codiert:
  - M = Münze einwerfen (1,0)
  - R = Geldrückgabeknopf drücken (0,1)
  - W = Warenausgabehebel drehen (1,1)
  - G = Münze auswerfen (1,0)
  - A = Ware auswerfen (0,1)
  - K = keine Reaktion (1,1)

  Der Pfefferminzautomat ist nun ein elektronischer Schaltkreis:




Das Verzögerungsglied stellt dabei den Zustand des Automaten dar. Alle Möglichkeiten dieser Schaltung zeigt die Automatentafel

| Zustand ν | Eingang | (1,0) | (0,1) | (1,1) |
|---|---|---|---|---|
| | 0 | 1,(1,1) | 0,(1,1) | 0,(1,1) |
| | 1 | 1,(1,0) | 0,(1,0) | 0,(0,1) |

In Wirklichkeit ist der Pfefferminzautomat natürlich widrigen Bedingungen ausgesetzt. Die Witterung, der Verschleiß von Bauteilen, die Unregelmäßigkeiten der Ware, unzufriedene Kinder, betrügerische Münzen – um nur einige zu nennen. Auf solche eher zufälligen Einflüsse haben die Theoretiker reagiert und Wahrscheinlichkeiten für einzelne Zustände eingeführt. Für unseren Automaten führen wir zur Veranschaulichung einen weiteren Zustand „Defekt“ und ein weiteres Eingangssignal „Faustschlag“ ein. Im geladenen Zustand macht dann z.B. der Automat nach einem Faustschlag in 80% der Fälle nichts und bleibt geladen, in 10% gibt er Geld zurück und geht in den neutralen Zustand über und in 10% geht er in den Zustand defekt und gibt nichts aus. Verallgemeinert ist das ein stochastischer Automat.

## 3.2 Algorithmen und Software

Der Pfefferminzautomat hat gezeigt, wie Algorithmen implementiert werden können und wie codierte Eingangssignale zu entsprechenden Ausgangssignalen werden. Damit ist der wesentliche Schritt zu Softwareprogrammen die Algorithmen umsetzen getan. Der Rest beschäftigt seitdem die

Informatiker, ist aber schnell erzählt. Zunächst wurde aus der dualen Maschinensprache, die sich aus der Automatentafel ergibt, ein Satz von Abläufen erstellt der oktal oder hexadezimal dargestellt wird weil es dual sehr unübersichtlich wird.

| Dez | Hex | Okt | Dual |
|---|---|---|---|
| 0 | 00 | 0 | 000000 |
| 1 | 01 | 1 | 000001 |
| 2 | 02 | 2 | 000010 |
| 3 | 03 | 3 | 000011 |
| 4 | 04 | 4 | 000100 |
| 5 | 05 | 5 | 000101 |
| 6 | 06 | 6 | 000110 |
| 7 | 07 | 7 | 000111 |
| 8 | 08 | 10 | 001000 |
| 9 | 09 | 11 | 001001 |
| 10 | 0A | 12 | 001010 |
| 11 | 0B | 13 | 001011 |
| 12 | 0C | 14 | 001100 |
| 13 | 0D | 15 | 001101 |
| 14 | 0E | 16 | 001110 |
| 15 | 0F | 17 | 001111 |
| 16 | 10 | 20 | 010000 |

Umrechnungstabelle Dezimal – Hexadezimal – Oktal - Dual

Die ausführenden Automaten (Computer) werden nun gerade so konstruiert, dass sie diese Instruktionen direkt ausführen können. Damit kann man dann Abfolgen aus Instruktionen programmieren und damit Anwendungen entwickeln. Der hohe Grad der Komplexität solcher Instruktionsfolgen und die daraus folgende Fehleranfälligkeit führte zu klugen Ideen für höhere Programmiersprachen, der Trennung von Daten und Verarbeitung, und der Objektorientierung. Heute gibt es eine große Anzahl von Programmiersprachen mit dem Ziel die Komplexität zu beherrschen.

## 4. Algorithmen und Zufall

Ein Algorithmus, der bei gleichen Eingabedaten ein zufälliges Ergebnis produziert, wäre nichtdeterministisch. Er würde verschiedene unterschiedlich lange Pfade enthalten, die zu unterschiedlichen Ausgabedaten führen würden. Es gibt aus heutiger Sicht keinen Rechner (auch Quantencomputer nicht), auf dem ein solcher Algorithmus ausführbar wäre, denn alle Rechner sind deterministisch. Der nichtdeterministische Algorithmus ist daher nur ein theoretisches Modell. Damit kann ausgeschlossen werden, dass ein Algorithmus, der programmiert wird und auf einem Rechner läuft, im engeren Sinne zufällig ist. Wohl aber kann man einen Algorithmus bauen, der Zufallszahlen erzeugt und mit diesen Zahlen einen anderen Algorithmus steuern. Bestimmte Pfade werden dann in

Abhängigkeit der Zufallszahl ausgeführt. Für den Anwender ergibt sich daraus ein scheinbar zufälliges Ergebnis.

Im Prinzip ist das nichts anderes als unser stochastischer Pfefferminzautomat.

## 4.1 Zufallszahlengeneratoren

Je nach den Anforderungen an die zufällige Zahl stehen Generatoren aus drei verschiedenen Klassen zur Verfügung: deterministische Generatoren, nichtdeterministische Generatoren und hybride Generatoren. Der Aufwand für nichtdeterministische Generatoren ist besonders hoch, weil dafür physikalische Prozesse eingebunden werden müssen.

### 4.1.1 Deterministische Generatoren

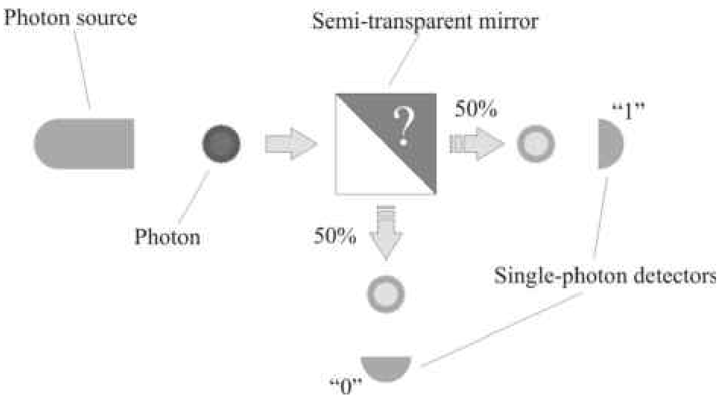
Diese Klasse der Generatoren erzeugt eine scheinbar zufällige Zahlenfolge mit einem (deterministischen) Algorithmus. Sie ist daher bei gleichen Eingangswerten reproduzierbar. Als Ausgangswerte werden hier gerne Werte benutzt, die in die Hardware bereits eingebaute Funktionen liefern. Diese Werte werden dann mit einem Algorithmus benutzt um als Zufallszahlen am Ende eine möglichst gleichverteilte Menge zu liefern. Ein Beispiel dafür ist der Mersenne-Twister 19937, der auf bestimmten Primzahlen beruht. Andere Beispiele sind der „Linear Kongruenz Generator (LKG)“ oder der „Multiplikative Rekursive Generator (MRG“). All diese Generatoren liefern sehr gut gleichverteilte Ergebnisse, können aber bei einer großen Anzahl von erzeugten Zufallszahlen periodisch werden.

Die Zufälligkeit der generierten Zahlen kann man empirisch testen und damit ein Maß für die Qualität der Zahlen erhalten. Es wird z.B. überprüft ob alle Zahlen gleich oft vorkommen (Frequenztest), ob bestimmte Paare von Zahlen gleich oft vorkommen (Serieller Test). Es gibt viele weitere Tests und in der Praxis hat sich bewährt nie nur einen Test durchzuführen.

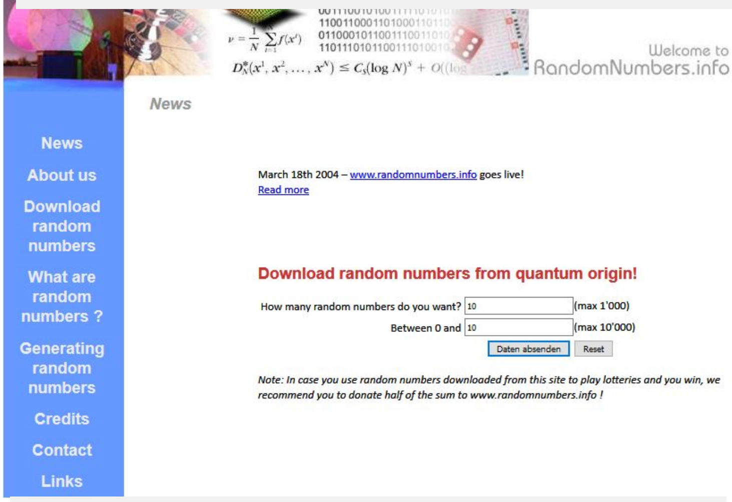
### 4.1.2 Nichtdeterministische Zufallszahlengeneratoren

Für einen solchen Generator misst z.B. ein Geigerzähler die Zahl der radioaktiven Zerfälle in einer bestimmten Zeitspanne. Man nutzt die Tatsache, dass radioaktive Isotope nach einer rein zufälligen Zeitspanne in das Tochterelement bzw. -isotop zerfallen. Die Zeitspanne hat aber beim gleichen Isotop immer den gleichen Mittelwert (die sogenannte Halbwertszeit). Da der radioaktive Zerfall unabhängig von Umgebungsbedingungen abläuft, kann dieser Vorgang Zufallszahlen hoher Güte liefern. Um Fehler der Messgeräte auszuschließen werden mehrere der Generatoren benutzt. Aus den Ergebnissen aller Generatoren benutzt man dann vielleicht nur das letzte Bit und bildet damit eine Modulo-2-Summe. Man erhält dann echte Zufallszahlen.

Es gibt Webpages, die echte Zufallszahlen anbieten. Als Beispiel sei eine Seite der Uni Genf (www.randomnumbers.info) genannt, die Zahlen auf der Basis eines quantenoptischen Effekts liefert.




Prinzipieller Aufbau eines quantenoptischen Generators




Webseite der Uni Genf

QR-Code einscannen,
um die Seite zu öffnen

## 4.2 Zufall und künstliche Intelligenz

Die künstliche Intelligenz (KI) hat die Labore verlassen und ist im Begriff unseren Alltag zu beeinflussen. Daher ist die Frage von Bedeutung in welchem Maße Zufälle in der KI eine Rolle spielen.

Der entscheidende Ansatz in der KI ist die Dynamisierung der Algorithmen. Das bedeutet, dass sich der Algorithmus selbst verändern kann. Dafür werden Erfahrungen aus der Anwendung des Algorithmus gespeichert und Veränderungen am Algorithmus ausprobiert mit dem Ziel, bessere Ergebnisse zu erzielen. Die Veränderung hängt also von der Verwertung von Erfahrungen ab. Dabei können ganz unterschiedliche zufällig erscheinende Ergebnisse zustande kommen.

Ganz ähnlich funktioniert unser Gehirn. Wenn es nicht schafft ein Problem zufriedenstellend zu lösen wird Vorgehensweise oder Verhalten so lange geändert, bis das Problem lösbar ist. Der gefundene Lösungsweg wird dann immer wieder benutzt.

Die Auseinandersetzung mit der Funktionsweise des Gehirns und die Forschung der Informatik an semantischen Netzen hat weiter dazu geführt algorithmisch Neuronen nachzubilden und damit ein neuronales Netz aufzubauen.

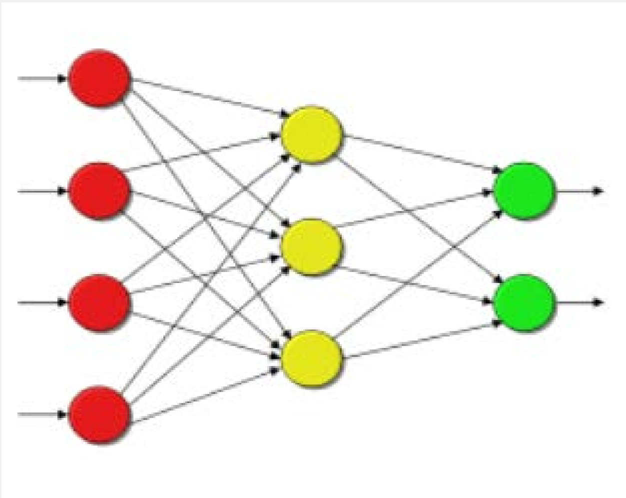
### 6.2.1 Der Aufbau eines neuronalen Netzes

Es werden drei verschiedene Typen von Neuronen, auch Units genannt, verwendet:

**Input-Units:** Nehmen das Eingangs-Signal entgegen. Im Falle der Bilderkennung wird dort die digitale Signatur (Eingangs Vector) des Bildes angelegt.

**Hidden-Units:** Sind beliebig viele Schichten von Neuronen zwischen dem Input- und den Output-Neuronen. Die Informationen die dort liegen, sind von außen nicht sichtbar.

**Output-Units:** Sie liegen außen und repräsentieren das Endergebnis, welches nach außen getragen wird. (Ausgangs Vector)

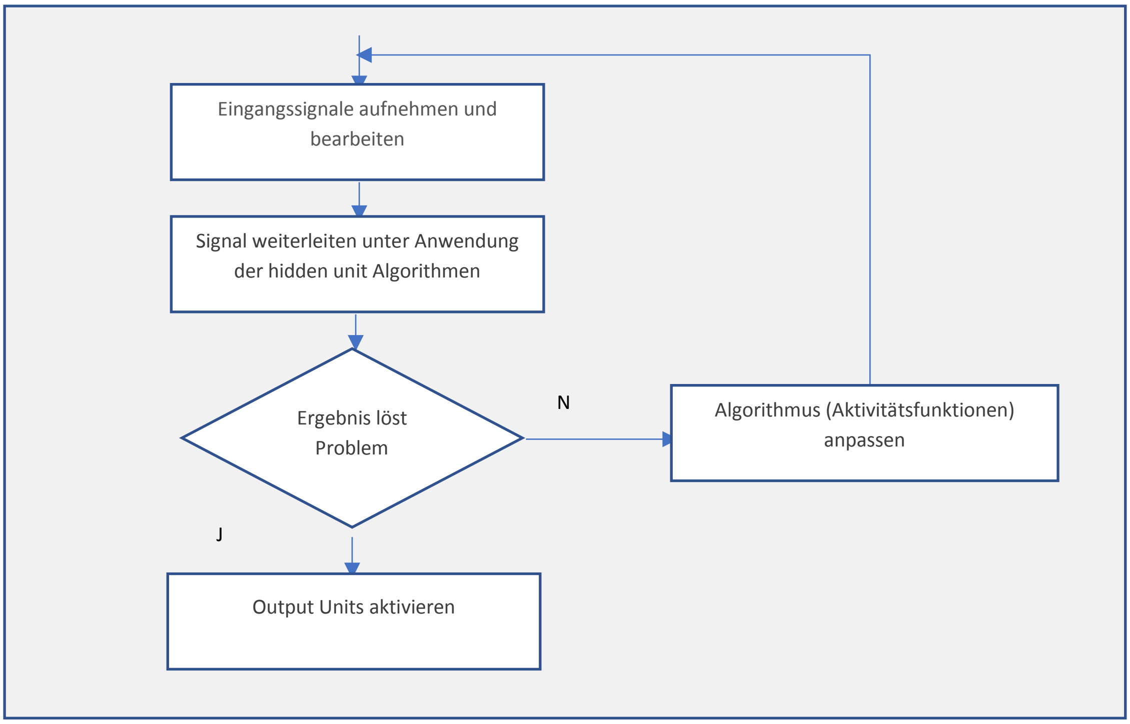


Michael Graf

Die Hidden-Units können beliebig komplex vernetzt sein; die Verbindungen tragen die eigentliche Information. Jedes dieser Neuronen wird durch eine Aktivitätsfunktion beschrieben nach der das Neuron feuert. Die Regeln sind einfach:

- Positive Eingangswerte verstärken den Aktivitätslevel bis das Neuron feuert und ein Signal an die Nachbarn weitergibt
- Negative Eingangswerte schwächen das Potential
- Neutrale Eingangswerte beeinflussen das Signal nicht (es besteht keine Verbindung zwischen den Neuronen)

Ein neuronales Netzwerk muss trainiert werden um die Aktivitätsfunktionen des Netzes für die Lösung einer Klasse von Problemen zu kalibrieren. Nach dieser Phase kann das Netzwerk Probleme nach dem folgenden Blockdiagramm lösen:




Mehrere spektakuläre Ergebnisse hat die KI-Sparte von Alphabet bereits geliefert darunter:

- zwei neuronale Netze, die miteinander ein Verschlüsselungssystem entwickelt haben um abhörsicher miteinander zu kommunizieren. Dabei ist nicht klar, wie sie es gemacht haben.
- Ein neuronales Netz, das nach der Trainingsphase neuronale Netze trainieren kann und zwar besser als die menschlichen Experten.

Der programmierte Zufall ist in diesen Beispielen anschaulich nachzuvollziehen.

## Quellenverzeichnis

| | |
|---|---|
| Dr. Stefan Frerichs | Grundlagen der Chaostheorie |
| Benoit Mandelbrot | Die fraktale Geometrie der Natur |
| John Briggs /Peat David | Die Entdeckung des Chaos |
| Alfred Schmitt | Automaten, Algorithmen, Gehirne |
| Florian Aigner | Der Zufall, das Universum und du |
| Dr. Nicolaus Wirth | Algorithmen und Datenstrukturen |
| Klaus Mainzer | Künstliche Intelligenz |
| Michael Graf | ki-robotik.de |

Diverse Quellen aus Wikipedia und Youtube