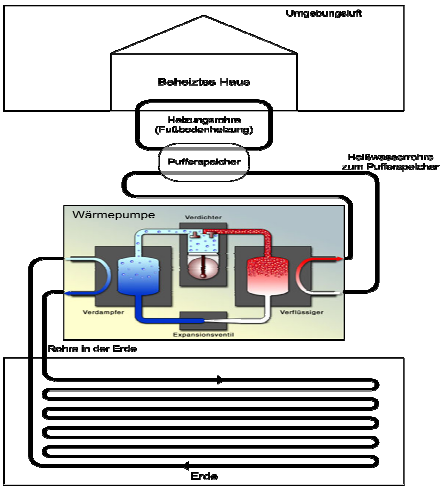
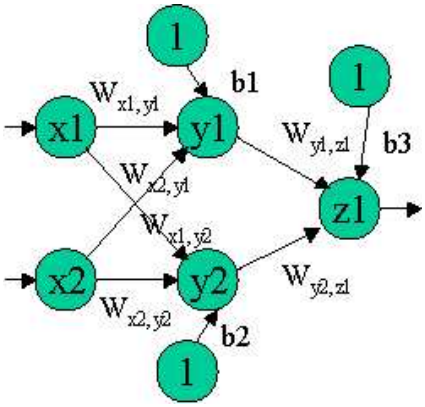
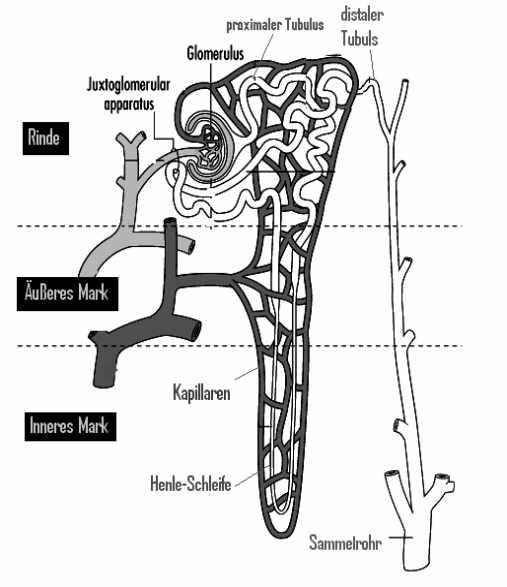
WOCHE DER MODELLIERUNG MIT MATHEMATIK

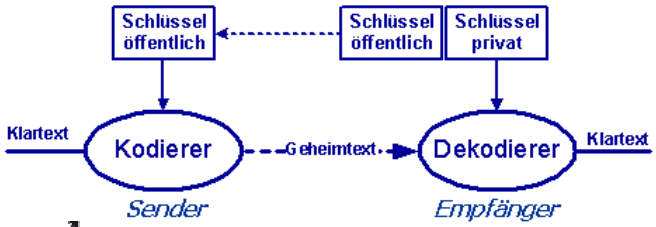
Dokumentationsbroschüre

14. – 20. Jänner 2007









Das Land Steiermark

LSR Stmk

Bank Austria Creditanstalt

UNI GRAZ

Woche der Modellierung mit Mathematik

Schloss Seggau, 14.01. – 20.01.2007

Weitere Informationen:
http://math.uni-graz.at/modellwoche/2007/

LSR Stmk

Bank Austria Creditanstalt

UNI GRAZ

Vorwort

Die Idee zu der in der Steiermark durchgeführten „Modellierungswoche“ für Schüler der 7. und 8. Klasse der AHS wurde schon längere Zeit am Institut für Mathematik und Wissenschaftliches Rechnen der Universität Graz diskutiert. Vorbild waren ähnliche Vorhaben, die bereits in Kaiserslautern, in Bozen und auch in Linz durchgeführt wurden. Mitglieder des Institutes haben bereits Erfahrungen mit ähnlichen Veranstaltungen für Studierende und angehende Wissenschafter. Im Jahre 2005 wurde vom Institut für Mathematik und Wissenschaftliches Rechnen der Karl-Franzens-Universität erstmals eine Modellierungswoche durchgeführt, die bei allen teilnehmenden SchülerInnen großen Anklang gefunden hat. Ermutigt durch diesen durchschlagenden Erfolg haben wir auch im Jahre 2006 wieder eine Modellierungswoche angeboten. Hauptziel der Modellierungswoche war es, Schüler mit einem Aspekt der Mathematik zu befassen, der unserer Meinung nach im Unterricht an den AHS unterrepräsentiert ist: Die Rolle der Mathematik als Werkzeug zum Verständnis der Welt, die uns in Alltag und Wissenschaft umgibt. Während ihrer gesamten Geschichte stand die Mathematik immer in Wechselwirkung mit angewandten Bereichen. Viele mathematische Theorien entstanden in Reaktion auf Anforderungen aus den verschiedensten Anwendungsbereichen. Die Verfügbarkeit immer leistungsfähigerer Computer hat neue Möglichkeiten für die mathematische Behandlung verschiedenster komplexer Probleme eröffnet. Quantitative Resultate statt qualitativer Aussagen sind immer wichtiger und erfordern zu ihrer Bewältigung die mathematische Modellierung komplexer Systeme in interdisziplinärer Zusammenarbeit.

Den an der Modellierungswoche teilnehmenden SchülerInnen sollte an Hand sorgfältig ausgewählter Projektaufgaben Gelegenheit gegeben werden, den angewandten Aspekt der Mathematik durch Teamarbeit in Projektgruppen zu erleben. Es wurde versucht, den Teilnehmenden die wesentlichen Phasen eines Modellierungsprozesses nahe zu bringen: Einarbeiten in das Anwendungsgebiet, Wahl der Modellstruktur in Hinblick auf die Aufgabenstellung, Einsatz numerischer Methoden, Interpretation der Ergebnisse, Präsentation der Resultate.

Treibende Kraft für die Realisierung der Modellierungswoche war Dr. Stephen Keeling, dem hier für seinen großen Einsatz gedankt sei. Besonderer Dank gebührt dem Landesschulrat für Steiermark, und hier insbesondere Frau Landesschulinspektor Hofrat Mag. Marlies Liebscher. Sie hat die Idee einer gemeinsamen Veranstaltung sofort sehr positiv aufgenommen und tatkräftig unterstützt. Ohne den großen Einsatz der direkten Projektbetreuer, Dr. Sigrid Thaller – Institut für Sportwissenschaft, Dr. Günther Lettl, Dr. Stephen Keeling, Dr. Alfio Borzì – alle Institut für Mathematik und Wissenschaftliches Rechnen, und der Betreuerin aus dem Kreis der Lehrerschaft, Mag. Melanie Wogrin, die auch die Gestaltung dieses Berichtes übernommen hat, wäre die Modellierungswoche nicht durchführbar gewesen. Eine wesentliche Rolle im Organisationsteam der Modellierungswoche spielten Gerlinde Krois und Dr. Georg Probst vom Institut für Mathematik und Wissenschaftliches Rechnen. Der Bank Austria – Creditanstalt sei für eine nicht unbeträchtliche Subvention gedankt. Die Abteilung für Wissenschaft & Forschung der Landesregierung Steiermark und das Programm für Begabungs- und Begabtenförderung des Zukunftsfonds Steiermark haben Subventionen in Aussicht gestellt.

Für ihre Unterstützung sei Vizerektor Martin Polaschek, Vizerektor Ralph Zettl und Dekan Georg Hoinkes der Universität Graz gedankt.

Schloss Seggau, am 20. 1. 2007

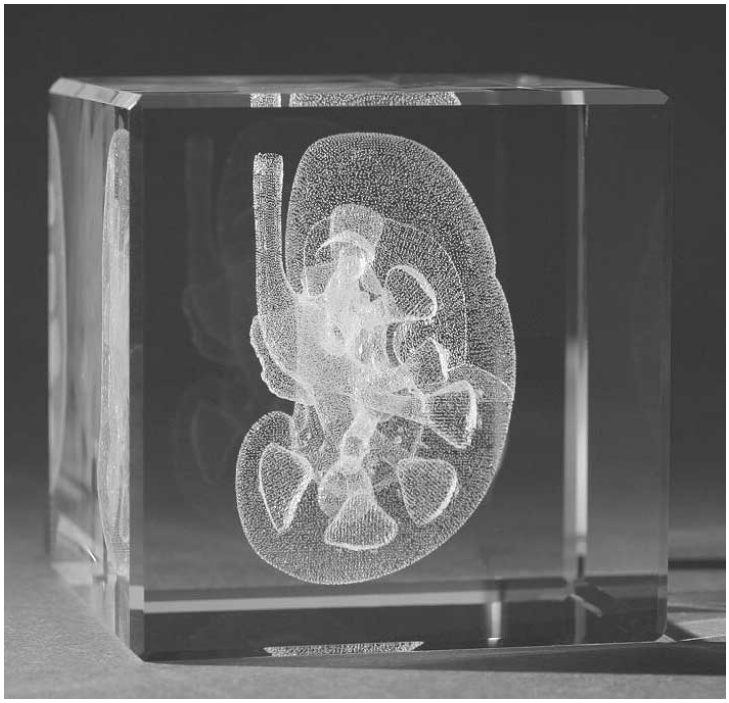
F. Kappel
(Leiter des Institutes für Mathematik und
Wissenschaftliches Rechnen)

Der Gegenstrommechanismus der Niere

<u>Dankwort</u>

Bevor wir Ihnen unser Projekt erläutern, möchten wir uns auf das Herzlichste bei unserem Tutor, Univ. Prof. Dr. Franz Kappel, der uns nicht nur in die komplexe Materie der Niere sondern auch in den Modellierungsprozess einführte, bedanken. Trotz zahlreicher anderer Verpflichtungen ist es ihm gelungen uns tatkräftig zu unterstützen und große Begeisterung in uns zu wecken.

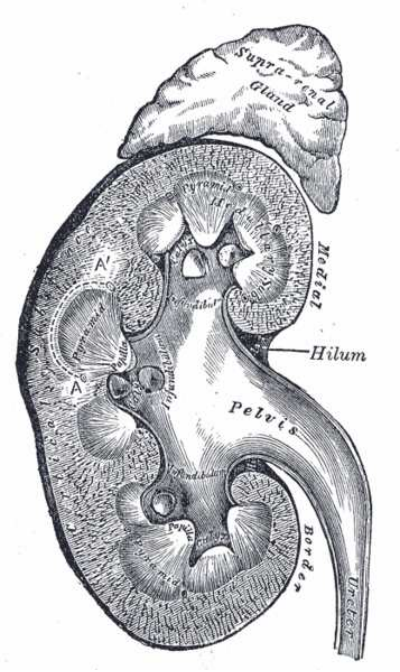
Vielen Dank!



1. Einführung in die Problematik

Physiologie der Niere

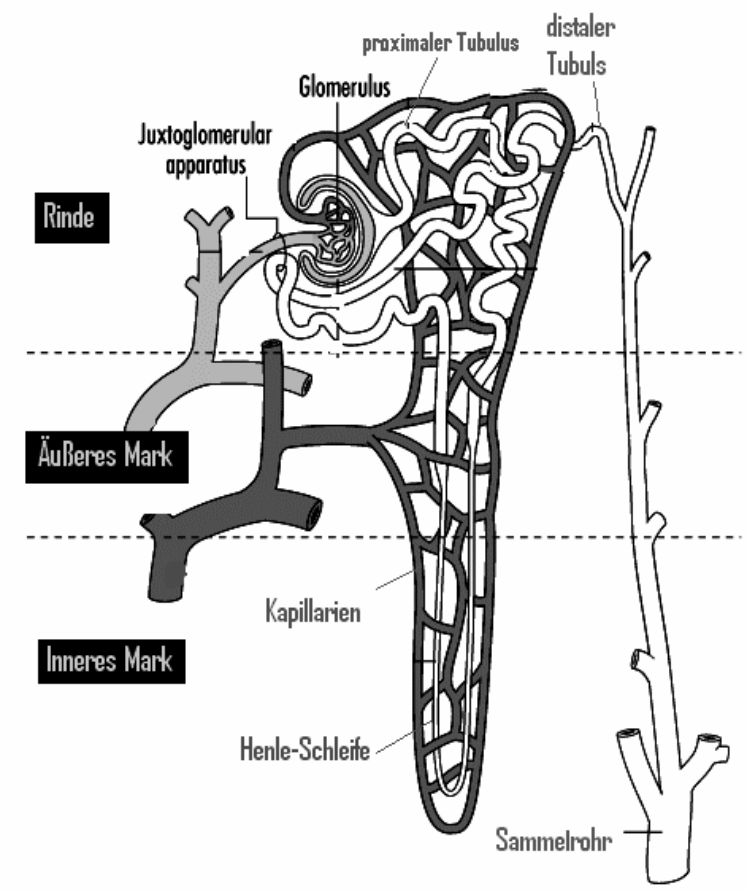
Die Aufgabe unserer Niere besteht neben der Regelung des Säure-Basen Haushalts, des Blutdrucks und des Wasserhaushalts darin, überflüssige Stoffe durch Bildung des Harns aus dem Körper auszuscheiden.



Sie regelt deren Konzentration und somit die Zusammensetzung des Blutplasmas.

Im Laufe dieser Woche beschäftigten wir uns mit dem Aufbau der Niere im Allgemeinen und der Konzentration positiv geladener **Natrium-Ionen** im Blutplasma im Besonderen.

Die menschliche Niere besteht aus etwa 10^6 **Nephronen**, die unter der Nierenrinde zu finden sind, wobei man oberflächliche und tiefe Nephronen unterscheidet, die beide über ein Verbindungsstück in das Nierenbecken münden. Nierenkörperchen („**Glomerulus**“) und die Nierenkanälchen der Henle-Schleife („**Tubuli**“) , während deren Verlauf die Natriumkonzentration geregelt wird, sind deren Hauptteile.



Man unterteilt Nephronen in 3 Teile: die Rinde, das äußere Mark und das innere Mark

Die Tubuli sind von einem Gefäßsystem aus **Kapillarien** umgeben, die Wasser und Na^+, welches von diesen ausgeschieden wird, aufnehmen. Deswegen nimmt die Konzentration in dieser Außenwelt von oben nach unten zu. Beim Übergang der beiden Äste ist sie am höchsten.

An die Henle-Schleife schließt an deren Ende der distale Tubulus und das Sammelrohr an.

Alle diese Strukturen mit ihrer engen räumlichen Beziehung bilden zusammen das **Gegenstromsystem**, das der Harnkonzentrierung dient.

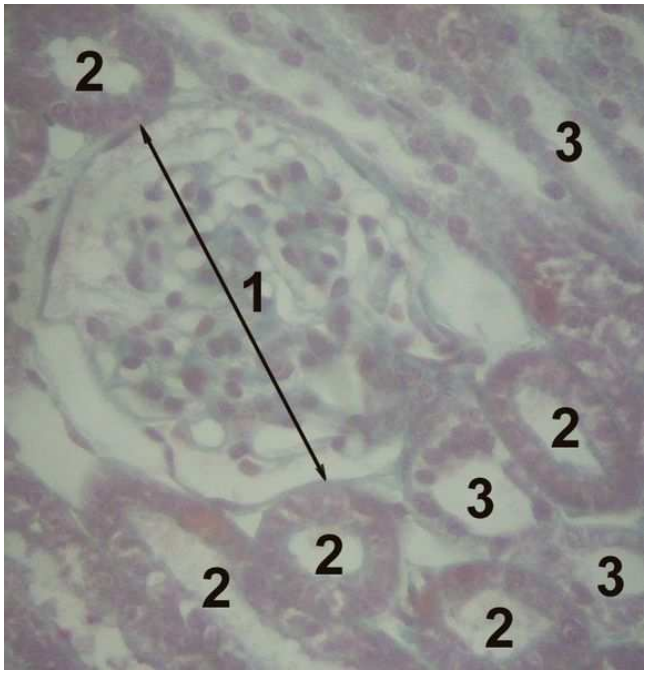
Am Anfang dieses komplexen Systems findet sich der Juxtoglomerulärer Apparat, der zusammen mit dem Glomerulus den Grad der Filtration der in die Tubuli eintretenden Flüssigkeit durch das Hormon Renin, das im Blut zu **Angiotensin** umgewandelt wird, regelt.

Dieses Hormon bewirkt, dass der Durchmesser der Kapillarien verringert bzw. vergrößert wird. Im Fall der Verengung der Gefäße wird der Fluss geringer und daher auch die Filtration. Es wird weniger Salz herausgefiltert. Im Falle der Erweiterung tritt das Gegenteil auf.

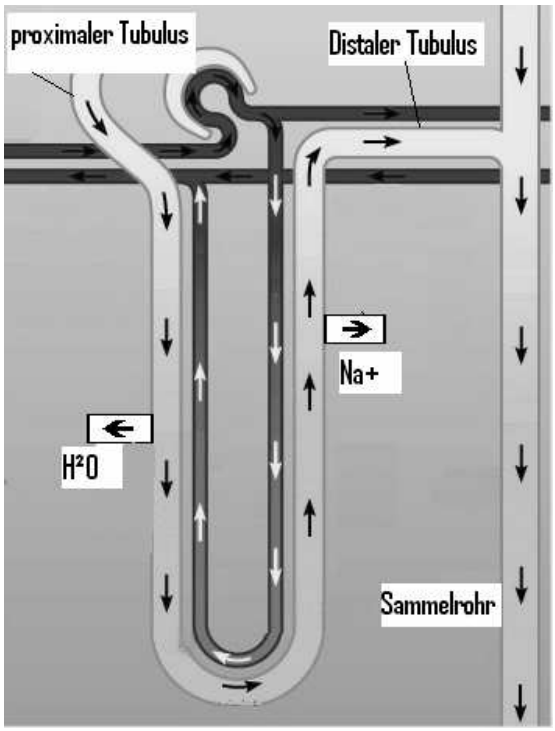
Durch den proximalen Tubulus gelangt das Filtrat in die Henle-Schleife, welche aus absteigendem und aufsteigendem Ast besteht , wobei bei ersterem die Wände durchlässig für Wasser und bei letzteren für Na+ sind.

- Im absteigenden Tubulus der Henle-Schleife versucht das Wasser den herrschenden Druckunterschied zwischen der Natriumkonzentration innerhalb und außerhalb (in den Kapillarien) des Tubulus auszugleichen. Es herrscht osmotischer Druck.

- Im aufsteigenden Tubulus wird Energie aufgewandt um Natrium-Ionen zurück in das Blutplasma zu befördern.



Lichtmikroskopische Aufnahme der Nierenrinde
1 Nierenkörperchen, 2 Hauptstück, 3 Mittelstück



Das entwendete Wasser bzw. Natrium wird jeweils von den umliegenden Kapillargefäßen aufgenommen und zurück in die Blutbahn transportiert.

Zwei Hormone können auch noch nach dem Austritt des Filtrats aus den Tubuli die Zusammensetzung von Blutplasma und Urin nicht unbeträchtlich beeinflussen.

- Im Distalen Tubulus kann **Aldosteron** einen Austausch von Na+ gegen Kalium hervorrufen. Dies senkt die Natriumkonzentration im auszuscheidenden Urin.

- Die Hirnanhangdrüse ist in der Lage das Hormon **ADH** (= antidiuretisches Hormon) zu produzieren (im Falle von zu viel Salz im Körper)
  Dies bewirkt eine größere Durchlässigkeit der Wände des Sammelrohrs und des distalen Tubulus gegenüber Wasser. Dem Urin wird dies entzogen und seine Konzentration somit größer, als im Blutplasma, das Volumen daher geringer.

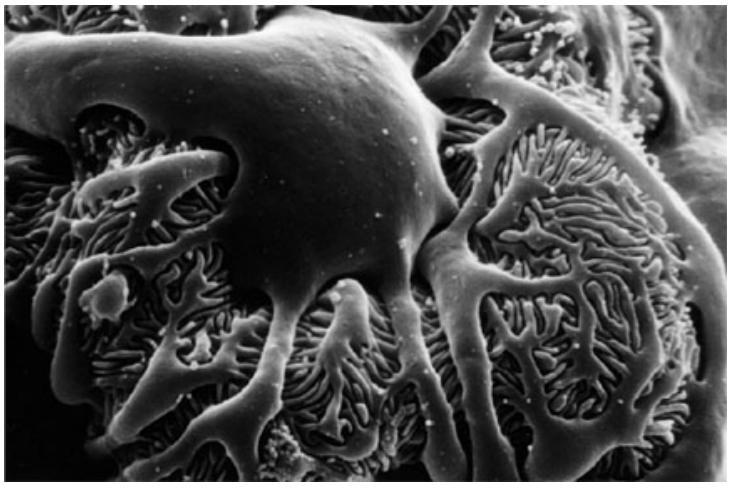
  Diesen Vorgang nennt man **Diurese**.

  Wenn kein ADH vorhanden ist sind die Wände undurchlässig und Volumen und Konzentration bleiben bestehen.

  Man spricht von **Antidiurese**

Nach der Passierung des Sammelrohrs gelangt der Urin durch ein Verbindungsstück in das Nierenbecken, in welches alle Nephronen schließlich einmünden, um dann über den Harnleiter ausgeschieden zu werden.

Unsere Problemstellung



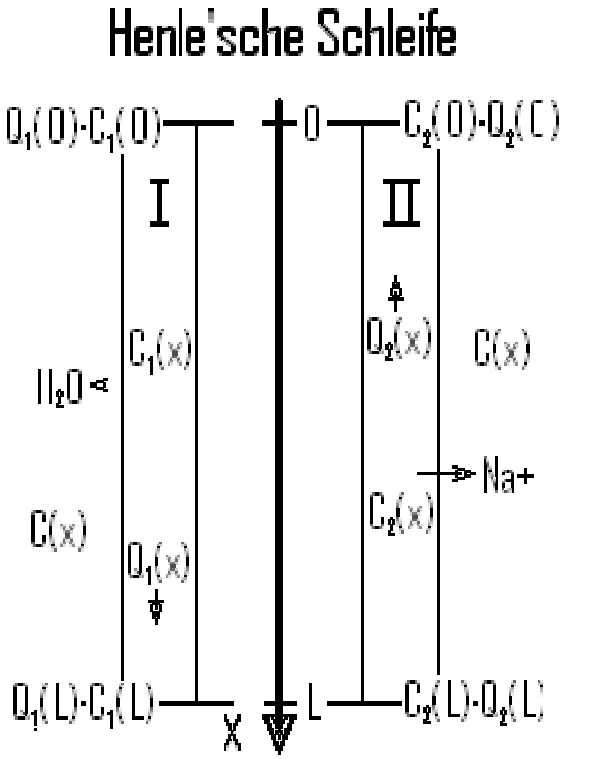
Glomerulus

Eine der Hauptaufgaben der Niere besteht in der Regelung der Zusammensetzung des Blutplasmas und so auch des Natriumhaushalts des Körpers.
Im Laufe der vergangenen Woche untersuchten wir welche Mechanismen von der Niere genutzt werden um Schwankungen dieses Natriumsspiegels auszugleichen, z.B. bei der Aufnahme von stark salzhaltigen Speisen und umgekehrt. Nimmt man eine große Menge an Salz zu sich, hat dies zur Folge, dass der ausgeschiedene Urin eine höhere Na-Konzentration als im Blutplasma vorhanden ist, vorzuweisen hat. Wird wenig Salz aufgenommen, bzw. viel Wasser weist der ausgeschiedene Urin demnach eine geringere Konzentration auf.

Im Zuge dieser Problematik stellten wir einige Überlegungen an um diese Vorgänge des Körpers mathematisch darzustellen und nachzuvollziehen.

2. Modellierungsprozess

Nach der Einführung in die biologischen Abläufe und zusammenhängenden Kontrollmechanismen beschäftigten wir uns mit den allgemeinen Eigenschaften von Rohrsystemen und über unseren Bildungslevel reichende mathematische Methoden. Nach dieser Einführung betrachteten wir ein Nephron und begannen die Henle-Schleife mathematisch zu beschreiben.



Nach gründlichen Überlegungen versuchten wir nur das Wesentliche herauszufiltern, wobei wir das als nebensächlich Eingeschätzte vereinfachten. So nahmen wir an, dass der Übergang vom ab- zum aufsteigenden Tubulus der Henle-Schleife nahtlos verläuft, weshalb

$$Q_1(L)=-Q_2(L)$$

$$C_1(L)=C_2(L)$$

ist. Zur Erläuterung, Q ist der Fluss, C die Na-Ionen-Konzentration, die tiefgestellten Zahlen $_1$ & $_2$ zeigen die Zugehörigkeit zu dem absteigenden, bzw. dem aufsteigenden Tubulus. Der Buchstabe L beschreibt die Position am inneren Ende der Henle-Schleife an der die Werte angelegt sind.

Weiters setzten wir die Permeabilität des absteigenden Tubulus gegenüber H_2O als unendlich fest, woraus folgt, dass

$$C(x)=C_1(x)$$

ist. Die Folge des osmotischen Drucks ist, dass die außerhalb der Tubuli herrschende Konzentration gleich der innerhalb des absteigenden Tubulus herrschenden ist.

Q=Fluss C=Kons. Na+
L=Ende d. Schleife
$Q_3(0)=Q_3(x)=Q_3(L)$
$C_3(0)=C_3(x)=C_3(L)$

Nach Überlegungen stellten wir zudem fest, dass der Fluss im aufsteigenden Tubulus konstant ist.

$$Q_2(0)=Q_2(X)=Q_2(L)$$

Anschließend betrachteten wir den Ausfluss von Na^+-Ionen im aufsteigenden Tubulus, wegen nicht vorhandener Messdaten nahmen wir diesen als konstant an und verbanden die außerhalb der Tubuli herrschende Na^+-Konzentration, den H_2O- und Na^+-Ausfluss, worauf sich folgende Formel ergab:

$$f_{Na+}=C(x)\ f_{H_2O}$$

Aus der logischen Schlussfolgerung, dass nicht mehr ausfließen kann als vorhanden ist und diese mit der zuvorkommenden gekoppelt erhält man:

$$Q_1'(x)+f_{H_2O}'(x)=0$$

$$Q_1'(x)+\frac{f_{Na+}}{C(x)}=0$$

Zu beachten ist auch, dass das Verhältnis der Konzentration und dem Fluss im absteigenden Tubulus an jeder beliebigen Stelle gleich ist.

$$C_1(x) * Q_1(x) \equiv \text{const.} \quad \Rightarrow \quad (C(x) * Q_1(x))' = 0$$

Durch Kombinieren der oberen und der dieser vorhergehenden Formel ergab sich:

$$C(x) = e^{\left(\frac{f_{Na^+}}{C(x) * Q_1(x)}\right) * x} * C(0)$$

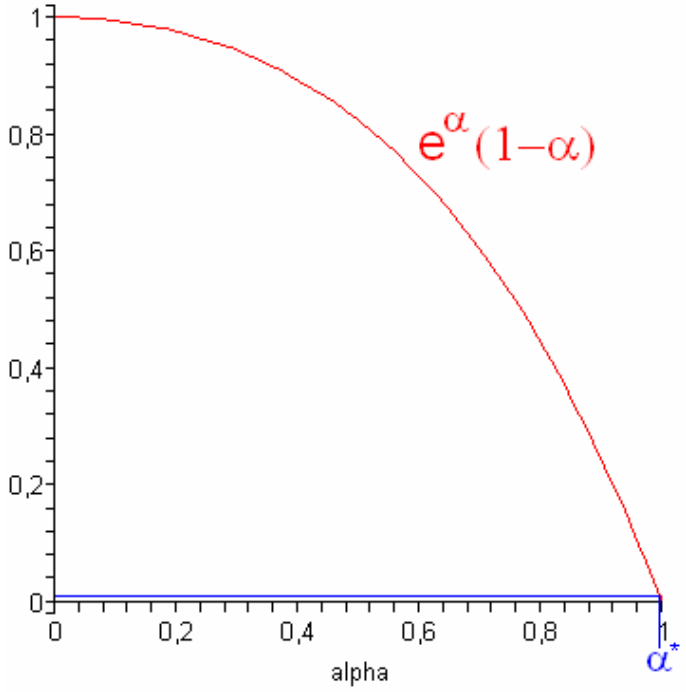
Diese Formel von der Konzentration am Ende des absteigenden Tubulus ergibt den Anfangswert vom aufsteigenden Tubulus und nachdem wir α, die Eintrittrate der Na^+-Ionen am Anfang der Henle-Schleife, definiert haben konnten wir auch die Konzentration am Ende der Henle-Schleife definieren.

$$C(L) = e^{\alpha} * C(0)$$

$$\alpha = \frac{f_{Na^+} * L}{C(x) * Q_1(x)}$$

$$C_2(0) = e^{\alpha} * C(0) * (1 - \alpha)$$

Jedoch mussten wir α und die letzte Formel noch genauer beschreiben, so dass sie Bedingungen erfüllen. So muss α zwischen 0 und 1 liegen, e^{α} größer 0 und $(1-\alpha)$ größer 0, aber kleiner 1 sein.



$$0 \langle \alpha \langle 1$$

$$0 \langle e^{\alpha}$$

$$0 \langle (1-\alpha) \langle 1$$

Im Zuge von Überlegungen betrachteten wir den Ablauf in der Henle-Schleife, wenn α gegen 1 strebt. So ergab sich nach dem ersetzen von α durch α* folgende Formel:

$$C_2(0) = e * C(0) * (1 - \alpha^*)$$

Umgeformt nach α:

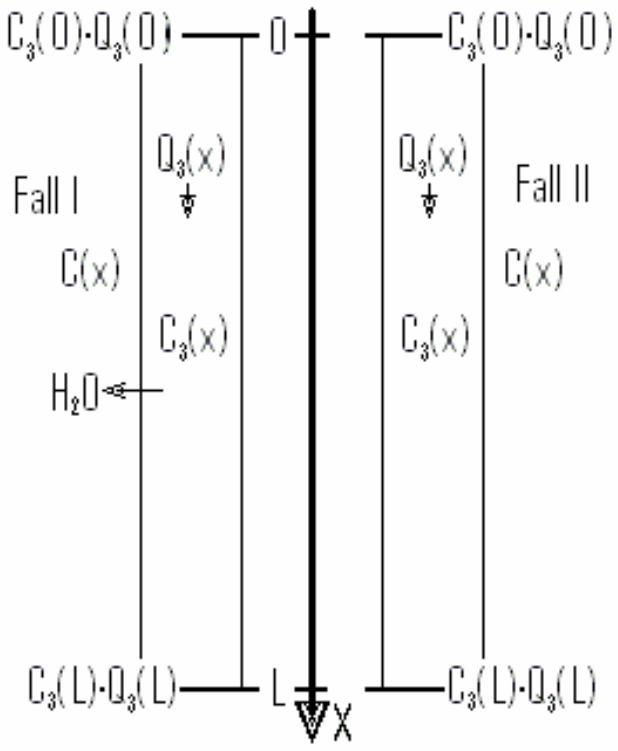
$$\alpha^* = 1 - \frac{C_2(0)}{C(0) * e}$$

Wir ersetzten e^{α} durch e, jedoch nicht $(1-\alpha)$ durch 0, da die Gleichung ansonsten ungültig wäre. Im nächsten Schritt kombinierten wir dies mit einer Formel, die den Fluss beschreibt, wo wir α durrch 0 ersetzt haben.

$$Q_1(0) = \frac{f_{Na+} L}{C(0)\alpha}$$

$$Q_1(0) \cdot C(0) = f_{Na+} L$$

Dies zeigt das Verhältnis von den anfänglichen Bedingungen und den Eigenschaften von der Henle-Schleife.



Nachdem wir dies geklärt haben, erweiterten wir das Modell um das Sammelrohr, welches den Vorurin sammelt und dessen Natriumkonzentration noch einmal, durch die Wirkung von ADH, regeln kann. So begannen wir mit einem Zwei-Varianten-System in dem Fall I eine so hohe Konzentration ADH gibt, dass die Membran der Sammelröhre sehr stark durchlässig ist, wodurch H_2O durch den osmotischen Druck austritt und somit der entstandene Urin eine höhere Natriumkonzentration, aber ein geringes Volumen hat. Im Fall II, bei dem wir eine sehr geringe ADH-Konzentration annahmen, ist das Volumen größer, die Natriumkonzentration jedoch geringer. In beiden Fällen wird allerdings die gleiche Menge Natrium ausgeschieden, wenn zu Beginn die gleichen Bedingungen herrschen und wir nicht beachten, dass der Kontrollmechanismus des ADH nicht in diesen Extremen auftritt. Aufgrund der Tatsache, dass es eine Gemeinsamkeit gibt und wir die Eigenschaften des Urins im Sammelrohr ohne ADH kennen, weil sie ident mit denen am Ende des aufsteigenden Tubulus sind, konnten wir die Eigenschaften des Urins im Falle des Vorhandenseins von ADH feststellen.

$$\frac{\tilde{Q}_3(L)}{Q_3(L)} = C_3(L)$$

	ohne ADH	mit ADH
$C_3(L)$	$C_2(0)$	$C(0)*e$
$Q_3(L)$	$\frac{f_{Na^+}*L}{C_1(0)*e}$	$\frac{f_{Na^+}*L}{(C_1(0)*e)^2}$
$\tilde{Q}_3(L)$	$\frac{f_{Na^+}*L*C_2(0)}{C_1(0)*e}$	$\frac{f_{Na^+}*L*C_2(0)}{C_1(0)*e}$

Beim Versuch das Modell insofern zu erweitern, dass wir die ADH-Konzentration variieren lassen können, scheiterten wir an der Tatsache, dass bis jetzt immer nur stationäre Werte betrachtet wurden. Bei dem Variieren der ADH-Konzentration spielt die Zeit allerdings eine bedeutende Rolle, da sich Konzentrations- und Widerstandsunterschied durch die zeitlich Abhängigkeit nicht sofort auf stationäre Gegebenheiten einstellen können.

3. Modelle und Anwendung

$$C_2(0) = e^{\alpha} * C(0) * (1 - \alpha)$$

$$\alpha = \frac{\gamma * f_{Na^+}}{C(0) * Q_1(0)} * x$$

Wir haben mit Hilfe der oben stehenden Formeln **3 Modelle** statuiert, die sich auf die **Henle-Schleife** und damit auf den Teil des Nephrons, der sich vom Ende des proximalen Tubulus bis hin zum distalen Tubulus erstreckt, beziehen.

- Als Erstes untersuchten wir die Auswirkung der *Resorption des Natriums* [f_{Na^+}] im aufsteigenden Tubulus auf die Endkonzentration [$C_2(0)$] vor dem dem Beginn des distalen Tubulus.

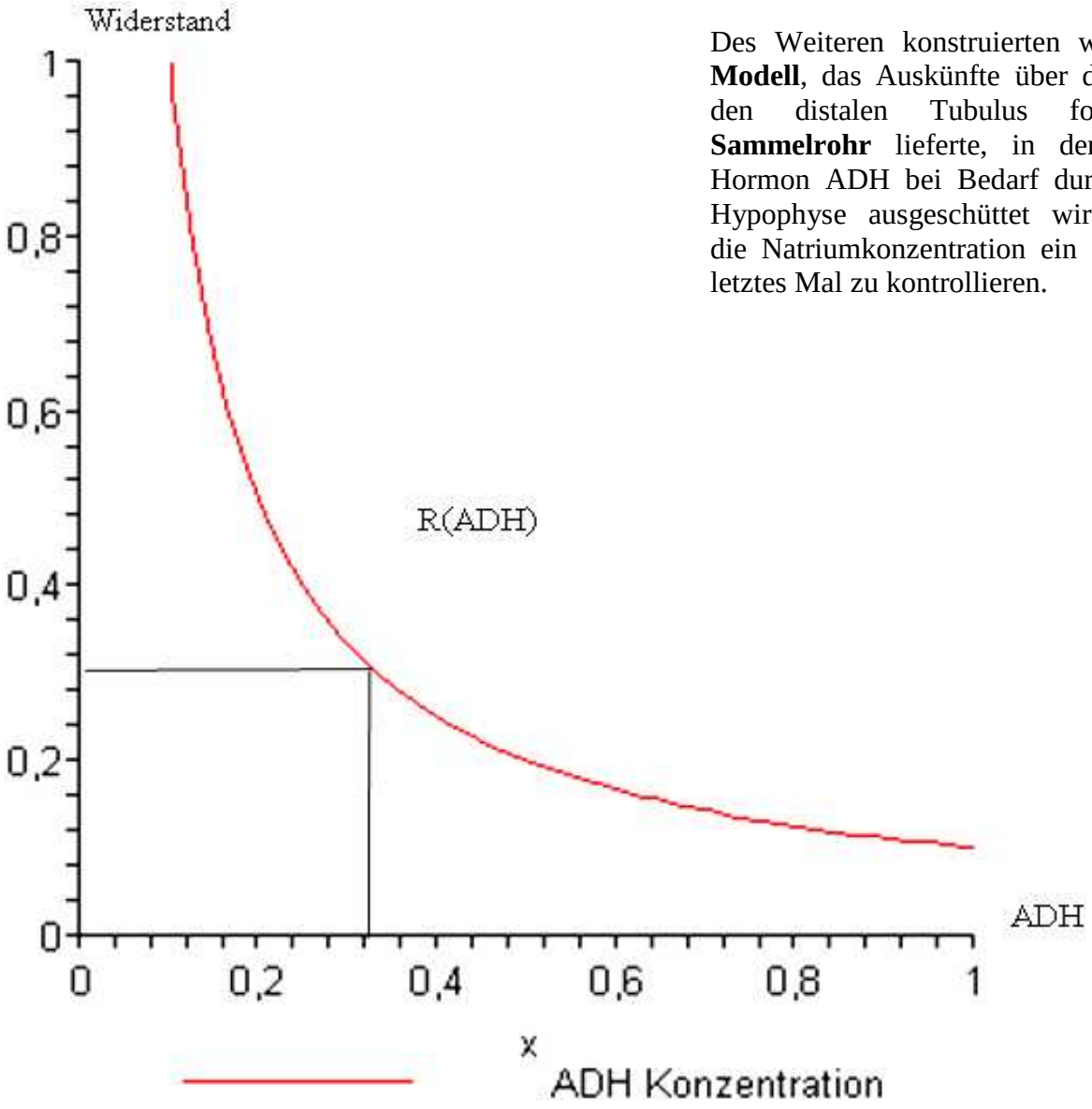
  =>Durch das Modell haben wir feststellen können, dass sich der Fluss des Natriums aus der für Natrium permeablen Wand des zweiten Tubulus indirekt proportional zu der Endkonzentration verhält. Dies wiederum heißt, dass mit zunehmendem Natriumfluss die Konzentration am Ende des aufsteigenden Tubulus abnimmt.

- Als Nächstes beschäftigten wir uns mit der Auswirkung von der *Eingangskonzentration* [$C_1(0)$] des Natriums am Beginn der Henle-Schlaufe auf die Konzentration am Ende des zweiten Tubulus [$C_2(0)$].

  =>Im Laufe unserer Arbeiten kamen wir zum Schluss, dass die Eingangskonzentration direkt proportional zu der späteren Natriumskonzentration vor dem distalen Tubulus ist, was heißt, dass um so größer die Anfangskonzentration ist, auch die Endkonzentration dementsprechend steigt.

- Als dritte und letzte Bedingung betrachteten wir die Auswirkung etwaiger Veränderungen des *Flusses* durch die beiden Tubuli [$Q_1(0)$] auf das $C_2(0)$.

  =>Hier konnten wir ebenfalls eine direkte Proportionalität des Durchflusses zur letztendlichen Natriumkonzentration feststellen.
  Je größer der Eingangsfluss, desto höher die Natriumskonzentration am Ende der beiden Tubuli.



Des Weiteren konstruierten wir **ein Modell**, das Auskünfte über das auf den distalen Tubulus folgende **Sammelrohr** lieferte, in dem das Hormon ADH bei Bedarf durch die Hypophyse ausgeschüttet wird, um die Natriumkonzentration ein drittes, letztes Mal zu kontrollieren.

Das Hormon *ADH* steuert den Widerstand und damit auch die Permeabilität der wasserdurchlässigen Membran der Sammelröhre, was wir in diesem Graphen veranschaulicht haben.
Die Funktionskurve R(ADH) beschreibt die Relation des Hormons und des Widerstands und somit der einzelnen Faktoren zueinander.

Man kann sagen, dass mit wachsender und gegen unendlich strebender ADH-Ausstoßung der Widerstand der Wand kleiner wird und letztendlich gegen Null strebt, so wie die Permeabilität der Membran des Sammelrohres gegenüber Wasser gegen Null strebt, wenn dies auch die ADH-Ausschüttung tut.

Dieses Modell half uns, die beiden extremen und dadurch einfacheren Annahmen, den Fall, in dem die enorm hohe Abgabe von ADH bewirkt, dass die Membran permeabel gegenüber Wasser wird, und jenen, in dem durch die enorm geringe Abgabe des Hormons der Widerstand höchst möglich wird, in einen Vergleich zu setzen.

	ohne ADH	**mit ADH**
Na^+ - Konzentration	$C_2(0)$	$C(0)*e$
Wasserausscheidung	$\frac{f_{Na^+} * L}{C_1(0)*e}$	$\frac{f_{Na^+} * L}{(C_1(0)*e)^2}$
Na^+ - Ausscheidung	$\frac{f_{Na^+} * L * C_2(0)}{C_1(0)*e}$	$\frac{f_{Na^+} * L * C_2(0)}{C_1(0)*e}$

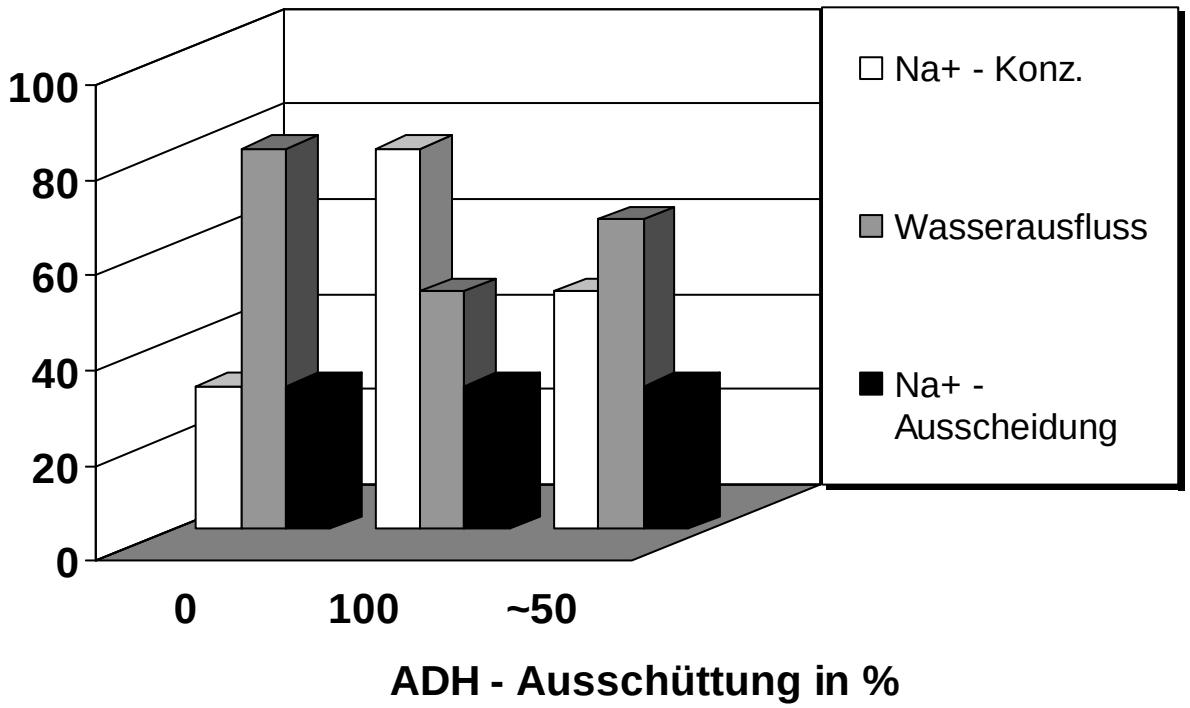
Die **Natriumkonzentration** bleibt ohne die Ausschüttung von ADH gleich der Konzentration am oberen Ende des distalen Tubulus [$C_2(0)$], wogegen sie sich durch die Abgabe des Hormons der Natriumkonzentration in den umliegenden Kapillarien im Level L [$C(0)*e$] angleicht, da die Osmose, die durch das Natriumgefälle nach außen hin entsteht, das Wasser zwingt, durch die Membran zu entweichen, um den Druck auszugleichen.

Die **Wasserausscheidung** ohne ADH ist gleichbleibend dem Wert vor dem distalen Tubulus, wobei sie sich durch die Ausschüttung des Hormons um das Quadrat verringert, da dieses im Nenner auftritt.

In der **Natriumausscheidung** selbst decken sich die Werte der beiden Extrema, da sich ja nur Wasser durch die permeablen Wände der Sammelröhre frei bewegen kann und nicht das Natrium. So wird selbst bei der Abgabe von ADH nur die Konzentration des Natriums geändert, nicht aber die Menge.

Zusammenfassend kann man also sagen, dass während die Natriumausscheidung ständig gleichbleibend ist, verändert sich die Natriumkonzentration indirekt proportional zum Wasserausfluss.

Wie bereits erwähnt sind in der Tabelle (siehe oben) nur die beiden vereinfachten Fälle, die Extrema, angeführt, die aber teilweise sehr realitätsfern sind. Bei der Vereinfachung der oben angeführten Werte haben wir diese Erkenntnisse noch einmal in dem folgenden Diagramm dargestellt, wobei auch der Fall im Mittel der beiden Extrema miteinbezogen wurde, welcher der natürlichen, täglichen Kontrolle durch die Niere am ähnlichsten ist.



Während die Natriumausscheidung, wie bereits erwähnt, in den drei Fällen ständig gleichbleibend ist, verhält sich die Natriumkonzentration im Urin indirekt proportional zum Wasserausfluss.

Projekt: Sportwissenschaften

Sind Tore nur Zufall?
Modellierung von Spielergebnissen bei Sportspielen

Gruppe:
Ramona Köppl, Christine Brandmüller, Dina Hofer, Basti Wilding, Gregor Fuchs, Benni Koller

Gruppenleiter:
Sigrid Thaller

Problemstellung

Wegen der geringen Torzahl spielt der Zufall bei Sieg oder Niederlage im Fußball eine größere Rolle als bei anderen Sportspielen. Je weniger Tore in einer Meisterschaft fallen, desto mehr unentschiedene Spiele gibt es. Daher wächst mit sinkender Torzahl die Chance einer schwächeren Mannschaft, zu punkten. Wenn weniger Tore fallen, ist also die Chance, dass nicht die spielstärkste Mannschaft die Meisterschaft gewinnt, größer.
Wie kann man die Spielstärke einer Mannschaft beschreiben? Welche Unterschiede gibt es zu anderen Sportspielen, zum Beispiel zu Tennis?
Ziel des Projektes ist es, verschiedene Modelle zu entwickeln und mit den Daten vergangener Meisterschaften zu überprüfen.

Modellierung der Spielstärke einer Fußballmannschaft

Das erstes Problem, mit dem wir konfrontiert wurden, war, eine Definition für die Spielstärke zu finden. Es gibt mehrere Ansätze:

Modell 1:

Unsere erste Definition der Spielstärke einer Mannschaft bestand daraus, die Gesamtzahl der geschossenen Tore durch die Anzahl der gespielten Matches zu dividieren:

$$Spielstärke = \frac{Geschossene \quad Tore}{Anzahl \quad der \quad gespielten \quad Spiele}$$

Doch wir erkannten schnell, dass diese Definition noch sehr ausbaufähig war.

Modell 2:

In unserem nächsten Ansatz bezogen wir die bekommenen Tore (=Gegentore) mit ein.

$$Spielstärke = \frac{Geschossene \quad Tore - Gegentore}{Anzahl \quad der \quad gespielten \quad Spiele}$$

Dieser Ansatz hat den Nachteil, dass besonders schlechte Mannschaften, die weniger Tore geschossen als bekommen haben, eine negative Zahl als Ergebnis für die Spielstärke haben, mit der es unmöglich ist, weiter zu rechnen.

Modell 3 a-c:

Es ließ sich nicht vermeiden andere Faktoren in unsere selbst kreierten Formeln mit einzubeziehen, wie die Siege, die Niederlagen, die Unentschieden, den Rang, die Gesamtspiele, alle geschossenen Tore und die Gegentore.
So ergaben sich für uns mehr oder minder brauchbare Formeln für die Spielstärke *a*.

Modell 3a:

$$a = \frac{Rang * Tore}{Rang(T1 - T2) * Spiele} + \frac{Siege - Niederlagen}{10} + \frac{Unentschieden}{30}$$

Modell 3b:

$$a = [1 - \frac{RangT2 - RangT1)}{10} * \frac{Gesamttore}{Spielanzahl}] + \frac{Siege - Niederlagen}{10} + \frac{Unentschieden}{30}$$

Modell 3c:

$$a = [1 - \frac{(RangT2 - RangT1)}{10} * \frac{eigeneTore * Gegentore}{Gesamtspiele}] + \frac{Siege - Niederlagen}{10} + \frac{Unentschieden}{30}$$

Definition des Ranges:
Der Rang ist die Platzierung einer Mannschaft in der jeweiligen Meisterschaft. Um die künftigen Spielausgänge berechnen zu können, benötigt man Daten von den ersten Spielen einer Meisterschaft, die Platzierung der Mannschaft nach den Vorrundenspielen bei der Fußballweltmeisterschaft oder ähnliches.

Modell 4: ULTIMEL ©

Beim Durchspielen mehrerer Spiele, Turniere und Meisterschaften erkannten wir, dass die Erfolgsquote bei der Vorhersage von ca. 60% noch nicht ausreichend war. Nach vielen

Versuchen, die Erfolgsquote zu optimieren, kamen wir zur **ulti**mativen Form**el** (Ultimel), mit der man den Spielausgang ungefähr zu 80% vorhersagen kann:

$$a = [1 - \frac{(RangT2 - RangT1)}{10}] \cdot \frac{eigeneTore}{Gegentore} + \frac{Siege - Niederlagen}{10} + \frac{Unentschieden}{30}$$

Wenn man das Verhältnis zwischen Sieg und Unentschieden betrachtet, sieht man, dass drei Unentschieden gleich viele Punkte bringen wie ein Sieg. Daher stehen in der obigen Formel als Nenner 30 und 10.

Regeln

- T2 - T1 darf keine negative Zahl ergeben!
- Bei einer negativen Spielstärke eines Teams von 0 bis -1 wird das erste 1- mit 2- ersetzt!
  {1 – [(Rang Team2…….}
  {2 – [(Rang Team2…….}
- Sinkt eine Spielstärke unter -1, so addiert man +2 hinzu
  … + (Unentschieden / 30) + 2
- Liegt eine Spielstärke über 3, so subtrahiert man -1
  … + (Unentschieden / 30) -1
- Hat eine Mannschaft 0 Gegentore, werden die Gegentore nur aus ihrer Formel gestrichen

$$\left[1 - \frac{RangT2 - RangT1}{10}\right] * \left(\frac{gesch.Tore}{Spiele}\right) \div \left(\frac{Gegentore}{Spiele}\right) + \frac{Siege - Niederlagen}{10} + \frac{Unentschieden}{30}$$

Poissonverteilung

Um weiter zu rechnen und die Wahrscheinlichkeit für ein gewisses Ergebnis zu ermitteln, bedienten wir uns der Poissonverteilung.

$$Pm(a) = \frac{a^m \cdot e^{-a}}{m!}$$

a … Quellstärke (Spielstärke)
e… Euler'sche Zahl
m… Anzahl der Tore
P… Wahrscheinlichkeit

Durch die Poissonverteilung lässt sich die Wahrscheinlichkeit ermitteln, mit der *m* Tore bei vorgegebener Spielstärke *a* geschossen werden.

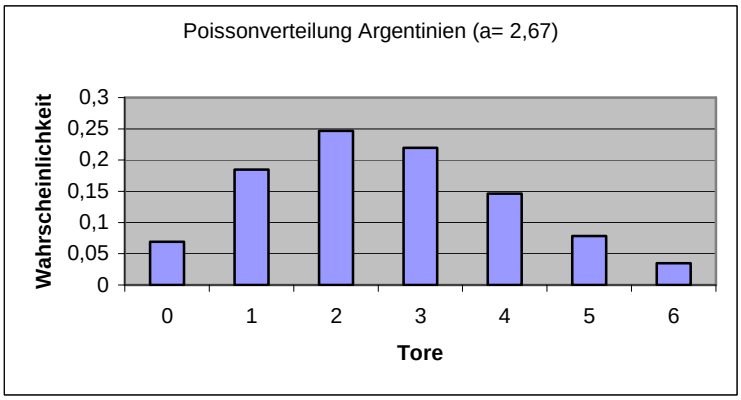


Diagramm 1: Torwahrscheinlichkeit Argentinien

Das Diagramm 1 zeigt am Beispiel von Argentinien die Torwahrscheinlichkeit bei einer Spielstärke von 2,67. Die Spielstärke Argentiniens wurde hierbei nach dem ersten Modell und den Daten der Vorrundenspiele der FIFA- Weltmeisterschaft 2006 ermittelt.

Die Wahrscheinlichkeit für einen Spielausgang *m*:*n* zwischen Mannschaften der Spielstärken *a* und *b* ist

$$P(m:n)(a) = \frac{a^m \cdot e^{-a}}{m!} \cdot \frac{b^n \cdot e^{-b}}{n!}$$

Veranschaulichung unserer Theorien anhand der Fußballweltmeisterschaft 2006:

Um die Effektivität unserer verschiedenen Definitionen der Spielstärke zu veranschaulichen, versuchten wir den Weg Italiens bei der Fußballweltmeisterschaft 2006 anhand ihrer Leistungen in den Vorrundenspielen vorauszusagen. Die folgenden Tabellen zeigen die Wahrscheinlichkeit für einen bestimmten Spielausgang an.

Modell 1:

$$Spielstärke = \frac{Geschossene \quad Tore}{Anzahl \quad der \quad gespielten \quad Spiele}$$

Achtelfinale: Italien vs Australien

Tore Italien
Tore Australien

Spielstärke Italien: 1,66666667
Spielstärke Australien: 1,66666667

Die Spielstärken für Italien und Australien wurden aus den Vorrundenergebnissen nach Modell 1 berechnet und sind gleich groß. Dadurch sind die Wahrscheinlichkeiten für einen Sieg Italiens oder einen Sieg Australiens auch gleich.

Tab 1: Wahrscheinlichkeiten der Spielergebnisse im Achtelfinale Italien vs Australien nach Modell 1

	0	1	2	3	4	5	6
0	4%	6%	5%	3%	1%	0%	0%
1	6%	10%	8%	5%	2%	1%	0%
2	5%	8%	7%	4%	2%	1%	0%
3	3%	5%	4%	2%	1%	0%	0%
4	1%	2%	2%	1%	0%	0%	0%
5	0%	1%	1%	0%	0%	0%	0%
6	0%	0%	0%	0%	0%	0%	0%

Wahrscheinlichkeit Sieg Italien **38%**
Wahrscheinlichkeit Sieg Australien **38%**
Wahrscheinlichkeit Unentschieden **23%**

Wahrscheinlichster Spielausgang: 1:1
Wahrer Spielausgang 1:0

Viertelfinale: Italien vs Ukraine

Da die Spielstärke der Ukraine gleich der Australiens und Italiens ist, ergeben sich die gleichen Ergebniswahrscheinlichkeiten wie für das Spiel Italien vs Australien und wir haben die Tabellen weggelassen.

Wahrscheinlichster Spielausgang: 1:1
Wahrer Spielausgang 3:0

Halbfinale: Italien vs Deutschland

Tore Italien
Tore Deutschland

Spielstärke Italien: 1,66666667
Spielstärke Deutschland: 2,66666667

Tab 2: Wahrscheinlichkeiten der Spielergebnisse im Halbfinale Italien vs Deutschland

	0	1	2	3	4	5	6
0	1%	2%	2%	1%	0%	0%	0%
1	3%	6%	5%	3%	1%	0%	0%
2	5%	8%	6%	4%	2%	1%	0%
3	4%	7%	6%	3%	1%	0%	0%
4	3%	5%	4%	2%	1%	0%	0%
5	0%	2%	2%	1%	0%	0%	0%
6	1%	1%	1%	1%	0%	0%	0%

Wahrscheinlichkeit Sieg Italien **23%**
Wahrscheinlichkeit Sieg Deutschland **56%**
Wahrscheinlichkeit Unentschieden **18%**

Wahrscheinlichster Spielausgang: 1:2
Wahrer Spielausgang 2:0 n.V.

Finale: Italien vs Frankreich

Tore Italien
Tore Frankreich

Spielstärke Italien: 1,66666667
Spielstärke Frankreich: 1

Tab 3: Wahrscheinlichkleiten der Spielergebnisse im Finale Italien vs Frankreich

	0	1	2	3	4	5	6
0	7%	12%	10%	5%	2%	1%	0%
1	7%	12%	10%	5%	2%	1%	0%
2	3%	6%	5%	3%	1%	0%	0%
3	1%	2%	2%	1%	0%	0%	0%
4	0%	0%	0%	0%	0%	0%	0%
5	0%	0%	0%	0%	0%	0%	0%
6	0%	0%	0%	0%	0%	0%	0%

Wahrscheinlichkeit Sieg Italien **53%**
Wahrscheinlichkeit Sieg Frankreich **23%**
Wahrscheinlichkeit Unentschieden **24%**

Wahrscheinlichster Spielausgang: 1:0 oder 1:1
Wahrer Spielausgang (1:1)(1:1)(1:1) 6:4 n.E.

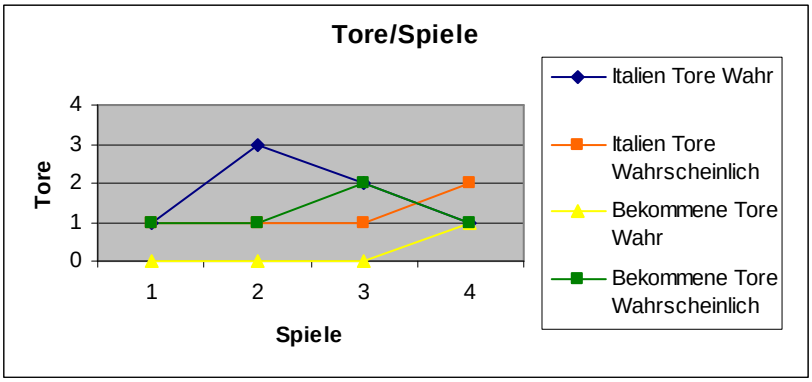


Diagramm 2: Vergleich Vorhersage Modell 1 – Spielausgang

Im obigen Diagramm kann man erkennen, wie die Vorhersagen mit den tatsächlichen Spielausgängen übereinstimmen.

Modell 2:

$$Spielstärke = \frac{Geschossene\ \ Tore - Gegentore}{Anzahl\ \ der\ \ gespielten\ \ Spiel}$$

Achtelfinale: Italien vs Australien

Tore Italien
Tore Australien

Spielstärke Italien: 1,33333333
Spielstärke Australien: 0

Tab 4: Wahrscheinlichkeiten der Spielergebnisse im Achtelfinale Italien vs Australien nach Modell 2

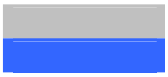
	0	1	2	3	4	5	6
0	26%	35%	23%	10%	3%	1%	0%
1	0%	0%	0%	0%	0%	0%	0%
2	0%	0%	0%	0%	0%	0%	0%
3	0%	0%	0%	0%	0%	0%	0%
4	0%	0%	0%	0%	0%	0%	0%
5	0%	0%	0%	0%	0%	0%	0%
6	0%	0%	0%	0%	0%	0%	0%

Wahrscheinlichkeit Sieg Italien **74%**
Wahrscheinlichkeit Sieg Australien **0%**
Wahrscheinlichkeit Unentschieden **26%**

Wahrscheinlichster Spielausgang: 1:0
Wahrer Spielausgang 3:0

Viertelfinale: Italien vs Ukraine

Tore Italien
Tore Ukraine



Spielstärke Italien: 1,33333333
Spielstärke Ukraine: 0,33333333

Tab 5: Wahrscheinlichkeiten der Spielergebnisse im Viertelfinale Italien vs Ukraine nach Modell 2

	0	1	2	3	4	5	6
0	19%	25%	17%	7%	2%	1%	0%
1	6%	8%	6%	2%	1%	0%	0%
2	1%	1%	1%	0%	0%	0%	0%
3	0%	0%	0%	0%	0%	0%	0%
4	0%	0%	0%	0%	0%	0%	0%
5	0%	0%	0%	0%	0%	0%	0%
6	0%	0%	0%	0%	0%	0%	0%

Wahrscheinlichkeit Sieg Italien **63%**
Wahrscheinlichkeit Sieg Ukraine **9%**
Wahrscheinlichkeit Unentschieden **28%**

Wahrscheinlichster Spielausgang: 1:0
Wahrer Spielausgang 3:0

Halbfinale: Italien vs Deutschland

Tore Italien	
Tore Deutschland	
Spielstärke Italien:	1,33333333
Spielstärke Deutschland:	2

Tab 6: Wahrscheinlichkeiten der Spielergebnisse im Halbfinale Italien vs Deutschland nach Modell 2

	0	1	2		4	5	6
0	4%	5%	3%	1%	0%	0%	0%
1	7%	10%	6%	3%	1%	0%	0%
2	7%	10%	6%	3%	1%	0%	0%
3	5%	6%	4%	2%	1%	0%	0%
4	2%	3%	2%	1%	0%	0%	0%
5	0%	1%	1%	0%	0%	0%	0%
6	0%	0%	0%	0%	0%	0%	0%

Wahrscheinlichkeit Sieg Italien	**25%**	Wahrscheinlichster Spielausgang: 1:1 oder 1:2
Wahrscheinlichkeit Sieg Deutschland	**52%**	Wahrer Spielausgang 2:0 n.V.
Wahrscheinlichkeit Unentschieden	**22%**	

Finale: Italien vs Frankreich

Tore Italien	
Tore Frankreich	
Spielstärke Italien:	1,33333333
Spielstärke Frankreich:	0,66666667

Tab 7: Wahrscheinlichkeiten der Spielergebnisse im Finale Italien vs Frankreich nach Modell 2

	0	1	2	3	4	5	6
0	14%	18%	12%	5%	2%	0%	0%
1	9%	12%	8%	4%	1%	0%	0%
2	3%	4%	3%	1%	0%	0%	0%
3	1%	1%	1%	0%	0%	0%	0%
4	0%	0%	0%	0%	0%	0%	0%
5	0%	0%	0%	0%	0%	0%	0%
6	0%	0%	0%	0%	0%	0%	0%

Wahrscheinlichkeit Sieg Italien	**53%**	Wahrscheinlichster Spielausgang: 1:0
Wahrscheinlichkeit Sieg Frankreich	**19%**	Wahrer Spielausgang (1:1)(1:1)(1:1) 6:4 n.E.
Wahrscheinlichkeit Unentschieden	**29%**	

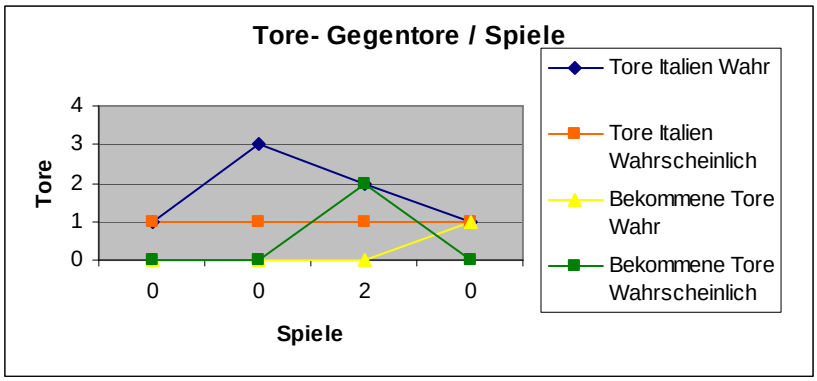


Diagramm 3: Vergleich Vorhersage Modell 2 – Spielausgang

Modell ULTIMEL ©

$$a = [1 - \frac{(RangT2 - RangT1)}{10}] \cdot \frac{eigeneTore}{Gegentore} + \frac{Siege - Niederlagen}{10} + \frac{Unentschieden}{30}$$

Achtelfinale: Italien vs Australien

Tore Italien	
Tore Australien	
Spielstärke Italien:	0,23
Spielstärke Australien:	0,03

Tab 8: Wahrscheinlichkeiten der Spielergebnisse im Achtelfinale Italien vs Australien nach Modell ULTIMEL

	0	1	2	3	4	5	6
0	77%	18%	2%	0%	0%	0%	0%
1	2%	1%	0%	0%	0%	0%	0%
2	0%	0%	0%	0%	0%	0%	0%
3	0%	0%	0%	0%	0%	0%	0%
4	0%	0%	0%	0%	0%	0%	0%
5	0%	0%	0%	0%	0%	0%	0%
6	0%	0%	0%	0%	0%	0%	0%

Wahrscheinlichkeit Sieg Italien	**20%**
Wahrscheinlichkeit Sieg Australien	**2%**
Wahrscheinlichkeit Unentschieden	**78%**

Wahrscheinlichster Spielausgang: 0:0
Wahrer Spielausgang 1:0

Viertelfinale: Italien vs Ukraine

Tore Italien	
Tore Ukraine	
Spielstärke Italien:	3,93
Spielstärke Ukraine:	0,88

Tab 9: Wahrscheinlichkeiten der Spielergebnisse im Viertelfinale Italien vs Ukraine nach Modell ULTIMEL

	0	1	2	3	4	5	6
0	1%	3%	6%	8%	8%	6%	4%
1	1%	3%	6%	7%	7%	6%	4%
2	0%	1%	2%	3%	3%	2%	2%
3	0%	0%	1%	1%	1%	1%	0%
4	0%	0%	0%	0%	0%	0%	0%
5	0%	0%	0%	0%	0%	0%	0%
6	0%	0%	0%	0%	0%	0%	0%

Wahrscheinlichkeit Sieg Italien	**78%**	Wahrscheinlichster Spielausgang: 3:0
Wahrscheinlichkeit Sieg Ukraine	**4%**	Wahrer Spielausgang 3:0
Wahrscheinlichkeit Unentschieden	**7%**	

Halbfinale: Italien vs Deutschland

Tore Italien
Tore Deutschland

Spielstärke Italien:	2,53
Spielstärke Deutschland:	1,73

Tab 10: Wahrscheinlichkeiten der Spielergebnisse im Halbfinale Italien vs Deutschland nach Modell ULTIMEL

	0	1	2	3	4	5	6
0	1%	4%	5%	4%	2%	1%	1%
1	2%	6%	8%	7%	4%	2%	1%
2	2%	5%	7%	6%	4%	2%	1%
3	1%	3%	4%	3%	2%	1%	0%
4	1%	1%	2%	1%	1%	0%	0%
5	0%	0%	1%	0%	0%	0%	0%
6	0%	0%	0%	0%	0%	0%	0%

Wahrscheinlichkeit Sieg Italien	**54%**	Wahrscheinlichster Spielausgang: 2:1
Wahrscheinlichkeit Sieg Deutschland	**26%**	Wahrer Spielausgang 2:0 n.V.
Wahrscheinlichkeit Unentschieden	**19%**	

Finale: Italien vs Frankreich

Tore Italien
Tore Frankreich

Spielstärke Italien:	2,57
Spielstärke Frankreich:	2,07

Tab 11: Wahrscheinlichkeiten der Spielergebnisse im Finale Italien vs Frankreich nach Modell ULTIMEL

	0	1	2	3	4	5	6
0	1%	2%	3%	3%	2%	1%	0%
1	2%	5%	7%	6%	4%	2%	1%
2	2%	5%	7%	6%	4%	2%	1%
3	1%	4%	5%	4%	3%	1%	1%
4	1%	2%	2%	2%	1%	1%	0%
5	0%	1%	1%	1%	1%	0%	0%
6	0%	0%	0%	0%	0%	0%	0%

Wahrscheinlichkeit Sieg Italien	**48%**	Wahrscheinlichster Spielausgang: 2:1 oder 2:2
Wahrscheinlichkeit Sieg Frankreich	**31%**	Wahrer Spielausgang (1:1)(1:1)(1:1) 6:4 n.E.
Wahrscheinlichkeit Unentschieden	**19%**	

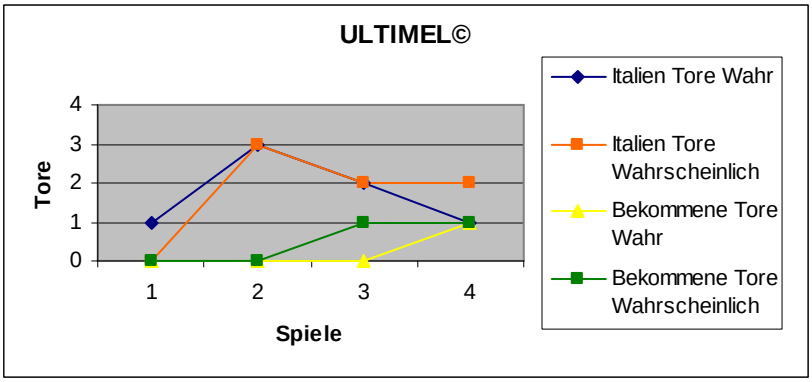


Diagramm 4: Vergleich Vorhersage Modell ULTIMEL – Spielausgang

Wie man erkennt, stimmen die Berechnungen in manchen Fällen nicht mit der Realität überein, da der Zufall unberechenbar ist. Es ist möglich das Ergebnis eines Spiels bis zu einem gewissen Grad vorauszusagen, allerdings ist aufgrund der meist geringen Torzahl der Zufall ein nicht zu unterschätzender Faktor.

Beispiel Bundesliga:

Tab 12: Bundesliga

Spiel		Ergebnis	Berechnung	Wahrscheinlichkeit in %
Mattersburg	**Sturm**	**1:0**	**1:0**	**44:14:42**
Ried	**Rapid**	**1:2**	**1:0**	**49:22:29**
Austria	**Salzburg**	**0:2**	**0:2**	**01:81:18**
GAK	**Pasching**	**2:1**	**0:0**	**07:48:45**
Altach	**Tirol**	**2:0**	**0:1**	**17:50:32**

Tabelle 12 zeigt das Ergebnis und die Vorhersage nach ULTIMEL für Bundesligaspiele. Die rechte Spalte zeigt die berechneten Wahrscheinlichkeiten für Sieg, Niederlage und Unentschieden.

Beispiel Achtelfinale WM 2006

Tab 13: Achtelfinale WM 2006

Spiel		Ergebnis	Berechnung	Wahrscheinlichkeit in %
Deutschland	Schweden	2:0	2:0	84:04:12
Argentinien	Mexiko	2:1 n. V.	0:0	20:03:77
England	Ecuador	1:0	2:1	55:24:20
Portugal	Niederlande	1:0	2:1	59:23:17
Italien	Australien	1:0	0:0	20:03:77
Schweiz	Ukraine	0:3 n. E.	0:0	39:29:32
Brasilien	Ghana	3:0	1:0	65:09:25
Spanien	Frankreich	1:3	0:1	17:58:25

Wie man an den obigen Tabellen erkennen kann, stimmen die mit ULTIMEL berechneten Ergebnisse mit einigen wahren Spielergebnissen überein. Wer das Spiel für sich entscheiden kann, stimmt mit ULTIMEL beinahe immer überein, die genaue Toranzahl jedoch nur in manchen Fällen.

Unentschieden

Je weniger Tore in einer Saison fallen, desto höher ist die Anzahl der Unentschieden.
Um die Wahrscheinlichkeit, dass bei einer gewissen Toranzahl ein Spiel unentschieden endet, zu berechnen, formten wir die Poissonverteilung um:

Wahrscheinlichkeit für *m* Tore: $$Pm(a) = \frac{a^m \cdot e^{-a}}{m!}$$

Wahrscheinlichkeit für Ergebnis *m:n*: $$P(m:n) = Pm(a) \cdot Pn(b)$$

Wahrscheinlichkeit für ein Unentschieden: $$Pu = \sum_{m=n} Pm(a) \cdot Pm(b)$$

Bei einem Unentschieden haben beide Teams die gleiche Toranzahl, also wird $m = n$ gesetzt.

Mit folgenden Näherungen

$$N \cong a + b$$
$$a \cdot b \cong (N/2) \cdot (N/2)$$

ergibt sich

$$Pu = e^{-N} \cdot \sum_{m} \frac{(N/2)^{2m}}{(m!)^2}$$

Pu … Wahrscheinlichkeit für ein Unentschieden
N… Gesamtzahl Tore/Spiel
a… Spielstärke Team 1
b… Spielstärke Team 2
m… Toranzahl Team 1
n… Toranzahl Team 2
e… Euler'sche Zahl

Tab 14: Wahrscheinlichkeit für Unentschieden

	N						
m	**2**	**2,1**	**2,2**	**2,3**	**2,4**	**2,5**	**2,6**
0	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
1	1,0000	1,1025	1,2100	1,3225	1,4400	1,5625	1,6900
2	0,2500	0,3039	0,3660	0,4373	0,5184	0,6104	0,7140
3	0,0278	0,0372	0,0492	0,0643	0,0829	0,1060	0,1341
4	0,0017	0,0026	0,0037	0,0053	0,0075	0,0103	0,0142
5	0,0001	0,0001	0,0002	0,0003	0,0004	0,0006	0,0010
6	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
7	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
8	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
9	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
10	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
SUMME	2,2796	2,4463	2,6291	2,8296	3,0493	3,2898	3,5533
Pu	31%	30%	29%	28%	28%	27%	26%

Anhand der Tabelle 14 kann man erkennen, dass bei wenigen Toren, also auch einer geringeren Spielstärke, die Wahrscheinlichkeit auf ein Unentschieden größer ist.

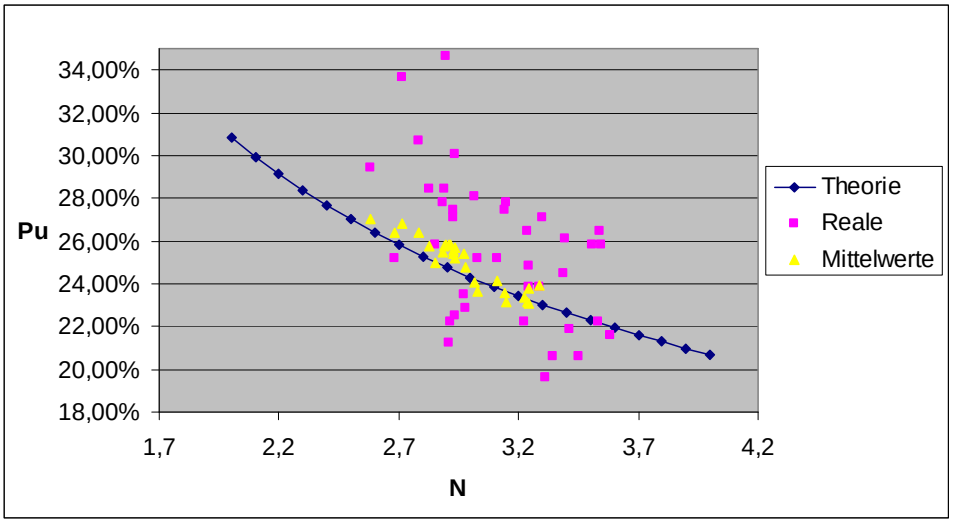


Diagramm 5: Wahrscheinlichkeit für Unentschieden in Abhängigkeit der Torzahl

Diagramm 5 veranschaulicht, dass bei weniger Toren pro Spiel die Wahrscheinlichkeit für ein Unentschieden steigt. Für das Diagramm wurden Werte aus der deutschen Bundesliga von 1963 bis 2005 verwendet.

Vergleich Fußball – Tennis

Tennis
- Begrenzte Satzanzahl
- Unbegrenzte Zeit
- 2 Spieler

Fußball
- Unbegrenzte Toranzahl
- Begrenzte Zeit
- 22 Spieler

Die Wahrscheinlichkeit, einen Satz zu gewinnen, kann man aus der Wahrscheinlichkeit x, das nächste Spiel zu machen, ausrechnen:

$$S(x) = x^6 + 6x^6y + 21x^6y^2 + 56x^6y^3 + 126x^6y^4 + 252x^7y^5 + 504x^7y^6$$

S…Wahrscheinlichkeit den Satz zu gewinnen
x...Wahrscheinlichkeit Spieler A das nächste Spiel zu machen
y...Wahrscheinlichkeit Spieler B das nächste Spiel zu machen
***x+y* = 1**

Die Wahrscheinlichkeit für den Gewinn eines 3-Satz Matches ist:

$$M(S) = S^3 + 3S^3T + 6S^3T^2 = S^3(10 - 15S + 6S^2)$$

S…Satzgewinnwahrscheinlichkeit
T…Gegenwahrscheinlichkeit
M...Wahrscheinlichkeit auf Matchgewinn

Auswirkung der Unterschiede

Beim Tennis ist durch die hohe Punktanzahl eine präzisere Berechnung der Wahrscheinlichkeit für einen Sieg möglich. Beim Fußball hingegen ist durch die geringe Toranzahl eine Berechnung äußerst diffizil.

Die Wahrscheinlichkeit, den Satz oder das Match zu gewinnen, ist größer als die Wahrscheinlichkeit, den nächsten Punkt zu machen.

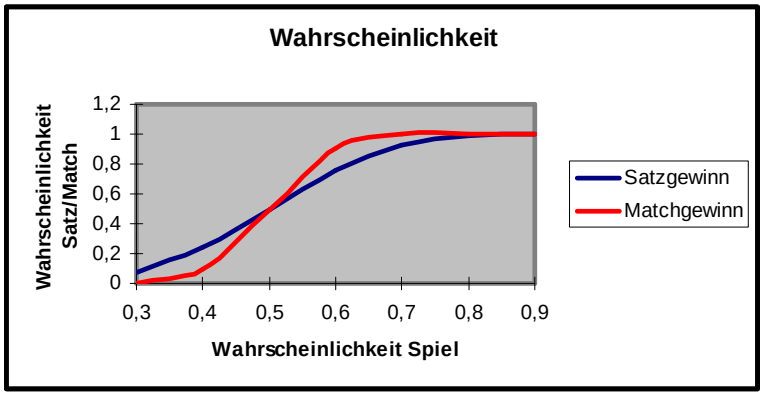


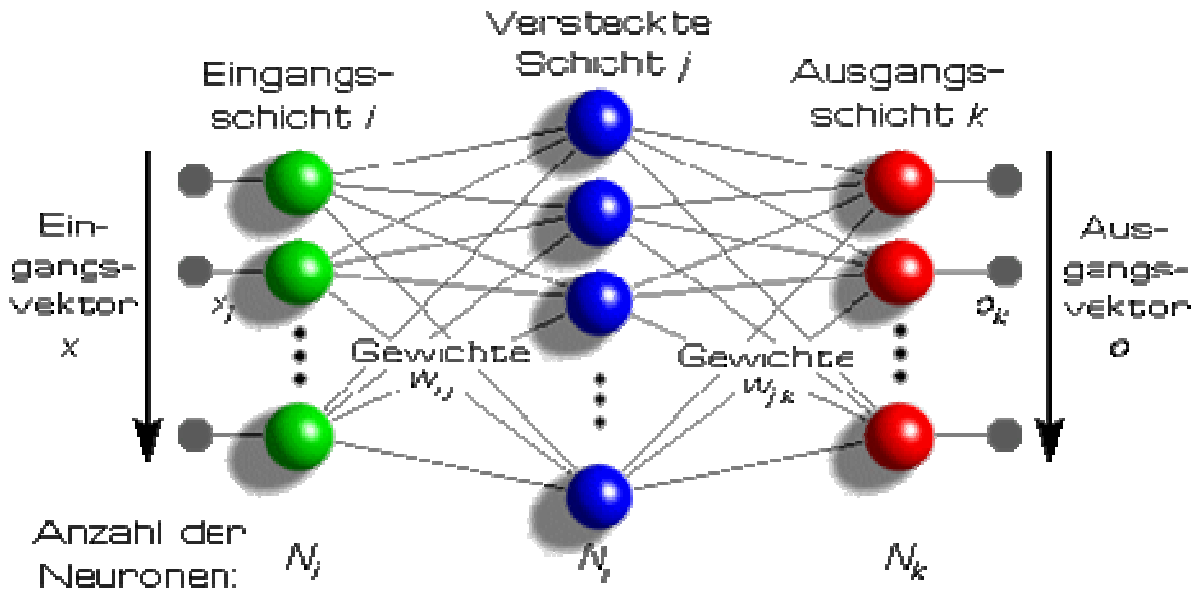
Diagramm 6: Wahrscheinlichkeiten für Satz- und Matchgewinn

Diagramm 6 zeigt die Wahrscheinlichkeiten für einen Satz -und Matchgewinn in Abhängigkeit von der Wahrscheinlichkeit, ein Spiel zu gewinnen. Mit zunehmender Wahrscheinlichkeit, das nächste Spiel für sich entscheiden zu können, steigt auch die Wahrscheinlichkeit, den Satz für sich entscheiden zu können und – in noch höherem Maße – die Wahrscheinlichkeit, das Match gewinnen zu können.

Quellenangabe:

Gaston Fischer (1980), Exercise in probability and statistics, or the probability of winning at tennis, Am. Phys. 48(1)
John Wesson, „Fußball - Wissenschaft mit Kick“ (2006), Verlag: Spektrum
www.wikipedia.org, “Tennis” (Zugriff am 18.1.2007)
www.sport1.at (Zugriff am 18.1.2007)

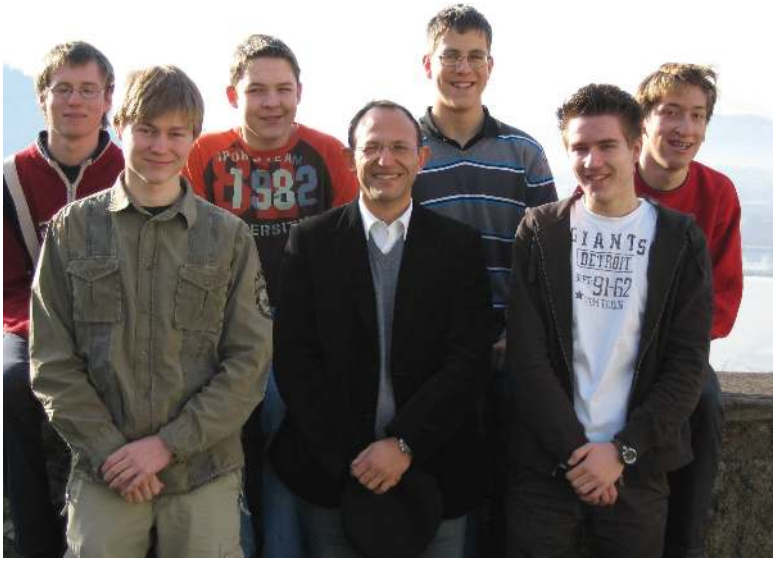
Neuronale Netze



Ziel: *Gesucht waren Programme, die fähig waren, Bilder bzw. Buchstaben zu unterscheiden und zu erkennen.*

Index

1. Teilnehmer



Matthias Schlaipfer(BORG Kindberg)

Patrick Schwarz(BORG Birkfeld)

Tobias Froihofer(BORG Birkfeld)

Christian Höflehner(BG/BRG Stainach)

Florian Andritsch(BRG Kepler Graz)

Daniel Steuber(BRG Kepler Graz)

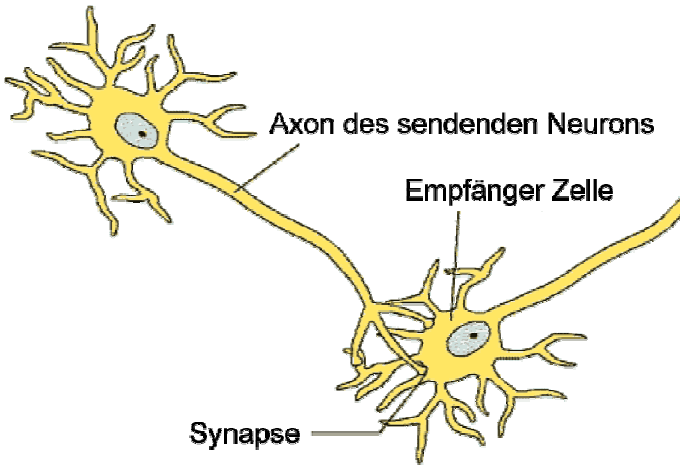
2. Leitung

Ao. Univ.-Prof. Mag. Dr.phil. Alfio Emanuele Borzì

Wissenschaftliches Personal am Institut für Mathematik und
wissenschaftliches Rechnen an der Karl-Franzens-Universität in Graz

Neuronale Netze beim Mensch

2.1. Allgemeines



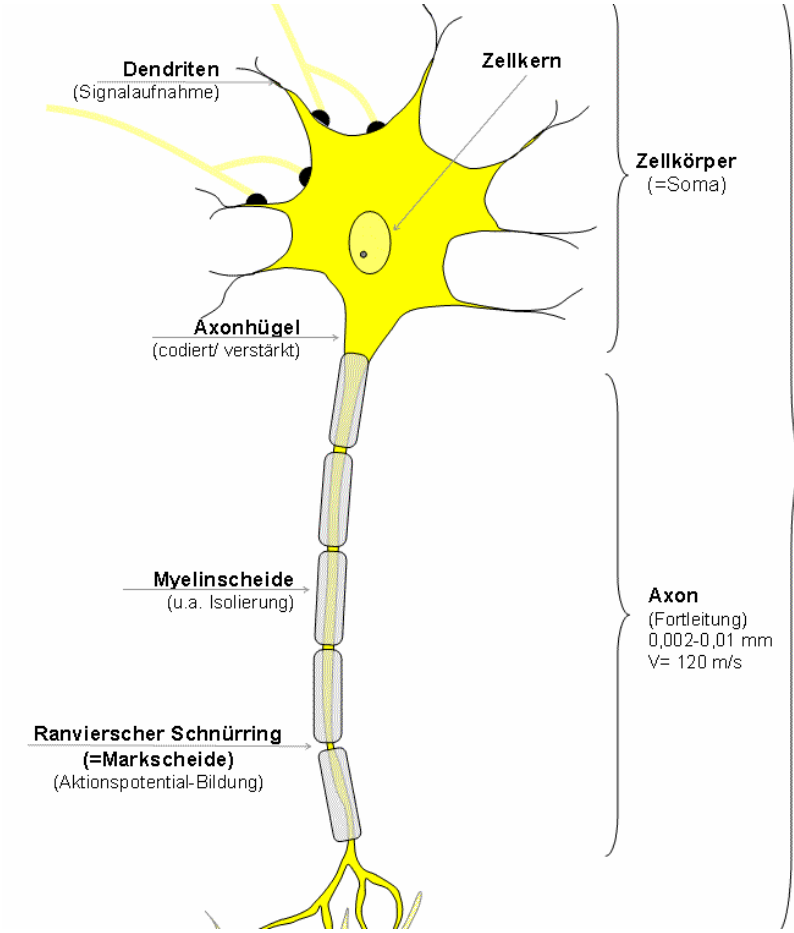
Natürliche Neuronale Netze sind aus Neuronen und Glia aufgebaute Netze. Zwischen den Zellen und Zellverbänden neuronaler Netze findet auf chemischem und elektrischem Weg ein Informationsaustausch statt.

Eine Neuron (griechisch: neũron, der Nerv) ist eine auf Erregungsleitung spezialisierte Zelle. Durch ihre elektrische Erregbarkeit und Leitfähigkeit sind Nervenzellen in der Lage Nervenimpulse selektiv weiterzuleiten und im Verbund befähigt, Informationen zu verarbeiten und gegebenenfalls zu speichern. Das menschliche Gehirn enthält zwischen 30 und 100 Milliarden Neuronen. Sie sind ein Hauptbestandteil der menschlichen Informationsverarbeitung und des Lernens.

3.2. Aufbau einer Nervenzelle

2.1.1. Die Dendriten

Dendriten sind feine plasmatische Verästelungen am Soma(Zellkörper). Sie empfangen Aktionspotentiale von anderen Neuronen und leiten diese weiter. Dendriten stehen in Kontakt mit 100.000 bis 200.000 Fasern anderer Neuronen



2.1.2. Der Axonhügel

Der Axonhügel ist der Ursprung des Axons und seine Aufgabe ist es, Aktionspotentiale von Dendriten an Axon weiterzuleiten

2.1.3. Das Axon

Das Axon ist ein langer Fortsatz der Nervenzellen, der verzweigt ist und in Synapsen mündet. Es kann eine Länge von 1 µm bis zu 1 m aufweisen und dabei zwischen 0,5 und 10 µm dick werden. Weiters dient es zur Übertragung innerhalb der Nervenzelle und zur Weiterleitung zu Synapsen und damit zu anderen Nervenzellen.

2.1.4. Die Synapse

Die Synapse dient der Übermittlung zwischen 2 Nervenzellen. Sie stellt somit eine Schnittstelle dar, in der eine Information chemisch auf eine andere Zelle übertragen werden kann. Mehrere Synapsen verschalten sich auf diese Weise unter einander zu einem neuronalen Netzwerk. Je näher eine Synapse am Soma, also am fremden Zellkörper ansetzt, desto stärker ist ihr Einfluss auf die Nervenzelle, je länger der Weg, den die Erregung zurücklegen muss, desto schwächer ist der Einfluss.

2.2. Arbeitsweise einer Nervenzelle

- Input der Dendriten von anderen Synapsen)
- Wenn das Schwellenpotential erreicht wird, erfolgt die Freisetzung von Aktionspotential
- Dieses wird über Synapsen an andere Nervenzellen weitergegeben

3. Modelle:

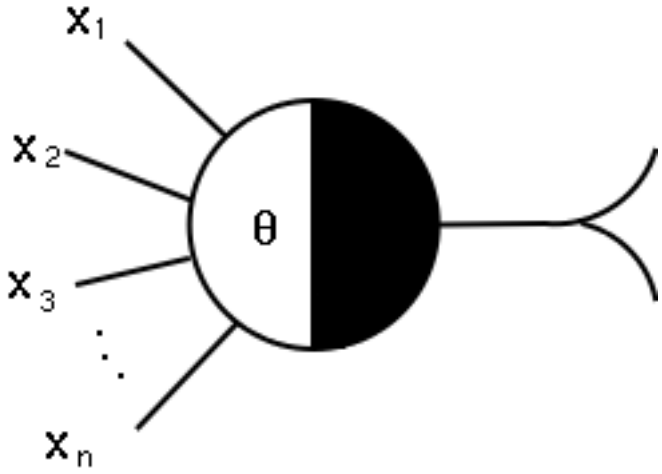
3.1. Allgemeines

Eine konzeptionelle Abstraktion des Untersuchungsgegenstandes mit dem Ziel, allgemeine Prinzipien der neuronalen Informationsverarbeitung in biologischen Systemen herauszuarbeiten, wird in der theoretischen Biologie vorgenommen. In der Neuroinformatik wird versucht, künstliche neuronale Netze computergestützt zu simulieren.

3.1.1. Binäre Inputs:

Obwohl ein Computer auf unterster Ebene mit binären In- und Outputs(1,0) arbeitet werden diese weniger häufig verwendet als die Bipolaren Inputs(1,-1), da die resultierenden Programme eine längere Lernphase aufweisen. Das liegt daran, dass symmetrische Netzwerke weniger als halb so viele netzwerkunabhängige Gewichte besitzen wie ein unsymmetrisches Netzwerk(binär).

3.2. McCulloch-Pitts-Zelle



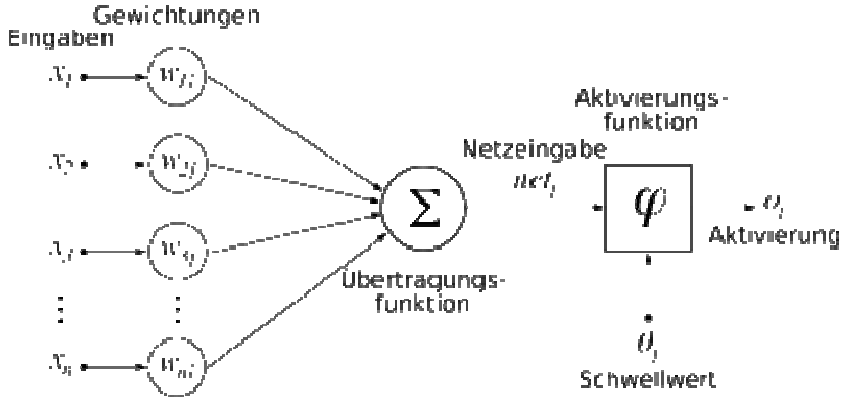
Dies war das erste Modell Überhaupt für Künstliche Neuronale Netze. Sie lernt welche Kombinationen der Eingänge „richtig“ sind und welche „falsch“. Dann Liefert sie entweder 1(richtig) oder -1(falsch) zurück.

3.3. Hebb-Regel

Je häufiger ein Neuron A gleichzeitig mit Neuron B aktiv ist, umso bevorzugter werden die beiden Neuronen aufeinander reagieren. Dies hat Hebb anhand von Veränderungen der synaptischen Übertragung zwischen Neuronen nachgewiesen.

3.3.1. Erklärung

Die Eingaben ($x_1, x_2, \ldots, x_i$)werden mit Durch Multiplikation mit Gewichten wichtiger bzw. unwichtiger und tragen einen großen teil zum Lernprozess bei. In diesem lernt der Computer, welche Eingaben richtig, und welche falsch sind. Und errechnet damit die Gewichte. Hat er fertig gelernt so kann man ihn auch testen. Wenn die Summe dieses mit Gewichten multiplizierten Inputs Größer ist als ein Schwellenwert, ist die Eingabe richtig, sonst ist sie falsch.



3.4. Perzeptron-Lernregel

w(neu) = w(alt) + yx
Diese Formel wird dadurch aufgelöst, dass y bekannt ist und für w fiktive Werte eingesetzt werden, bis alle x richtig qualifiziert wurden → benötigt Aufsicht beim Lernen.
Ein ungefähres Schema sähe so aus:

- Eingabe des Eingabemusters (Aktivierung der Input-Neuronen)
- Netz erzeugt einen Output t
- Vergleich der Ausgabe t mit der korrekten Version → Ergibt den Fehlervektor
- Backpropagation oder Fehlerrückführung über die Formel $E = ½*\Sigma(t_i-y_i)2$,

wobei E = der Fehler, t = die gewünschte Ausgabe und y = die gegebene Ausgabe

- Änderung der vorher eingegebenen Werte

3.5. Bias und Schwellwert

- Arbeitet wie ein Gewicht von einer Einheit, deren Wert immer +1 beträgt
- Erhöhter Bias → erhöhter Input auf folgende Einheit
- Ist ein Bias vorhanden:
  - y_in = 1, wenn net $\geq$ 0
  - y_in = -1, wenn net < 0
  - y_in = b + $\Sigma x_i w_i$
  - kennt man bereits einen Bias, errechnet man die weiteren über b(neu) = b(alt) + t
- Ist kein Bias vorhanden, wird ein fixer Schwellwert von 0 für die Aktivierungsfunktion verwendet:
  - y_in = 1, wenn net $\geq$ 0
  - y_in = -1, wenn net < 0
  - y_in = $\Sigma x_i w_i$

3.5.1. Beispiel anhand der Trenngerade/Entscheidungsgrenze:

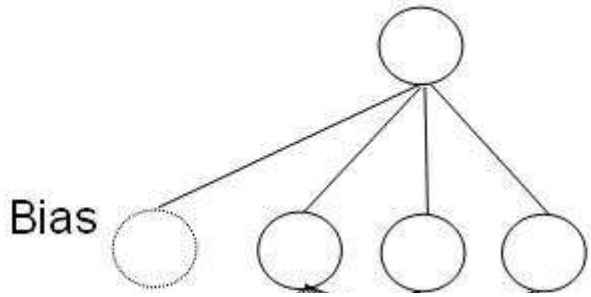
- Trenngerade = Grenze für die Werte von x_1 und x_2, für welche das Netz eine positive/negative Antwort gibt(decision regions)
- Mit Bias(z.B. bei der UND – Funktion):
  - $b + x_1w_1 + x_2w_2 = 0$
    - $b + \Sigma x_i w_i = 0$
    - >0 → positive Antwort
    - <0 → negative Antwort
  - Werte von w_1, w_2 und b werden erst im Laufe des Trainings ermittelt

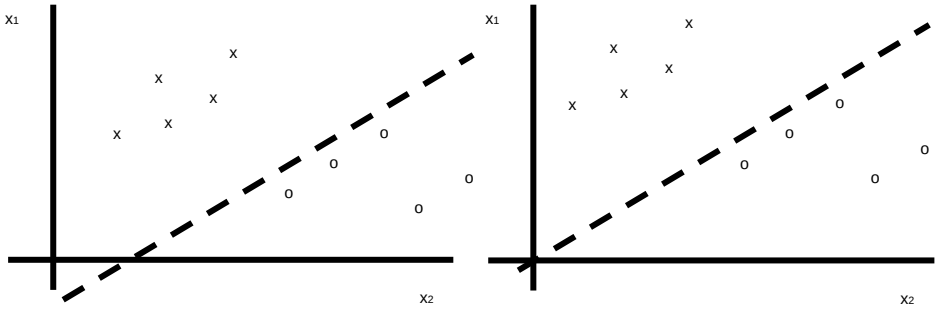
- Je nach Anzahl der eingegebenen Daten erhält man eine Gerade, eine Ebene oder eine Hyperebene

- Ohne Bias:
  - $x_1w_1 + x_2w_2 = 0$

3.5.2. Vorteil des Bias:

- Beeinflusst die Entscheidung/Antwort aufgrund vergangener Erfahrungen
  - Von Individuum zu Individuum verschieden
- Trennlinie fließt genau durch den Ursprung
  - ohne Bias fließt die Trennlinie beliebig nahe dem Ursprung





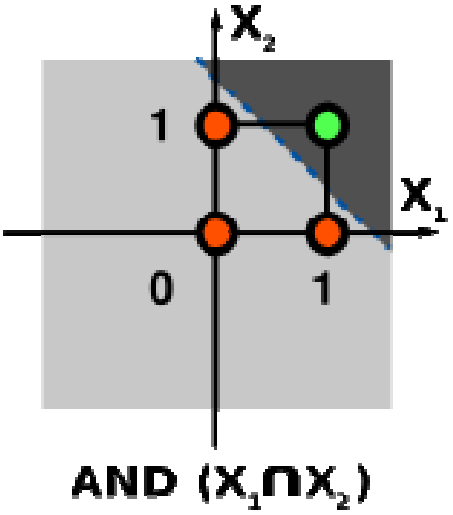
Liegen also alle richtigen Antworten (+1) auf einer und alle falschen Antworten (-1) auf der anderen Seite solch einer Trenngeraden ist das Problem „linear seperabel“. Single-Layer Netze können nur Probleme lösen, die linear seperabel sind.

3.5.3. Erste Beispiele:

3.5.3.1. Beispiel: AND-Funktion

Liegen bei einem Netz zwei Input Einheiten vor(x_1, x_2), so kann man ihm 4 verschiedene Eingabemuster vorgeben, worauf es zwei verschiedene Antworten t geben kann (t>0 → positiv/richtig; t<0 → negativ/falsch):

Input		Output
x_1	x_2	t
1	1	1
1	-1	-1
-1	1	-1
-1	-1	-1



Die Trenngerade dieser Funktion wäre $x_2 = - x_1+1$
b, w_1 und w_2 errechnet das Programm selbst, da man ihm x_1 und x_2, sowie t vorgibt. Durch diese 3 Vorgaben kommt er z.B. zu diesen 3 Gleichungen:

$1 = 1* w_1 + 1* w_2 +b$
$-1 = 1* w_1 + -1* w_2 + b$
$-1 = -1* w_1 + 1* w_2 + b$

Über das Additionsverfahren errechnet sich das Programm nun:

$b = -1$
$w_1 = 1$
$w_2 = 1$

3.5.3.2. Beispiel OR Funktion

Die OR Funktion wird auf die gleiche Art berechnet, wie die UND Funktion, nur, dass es hier nur einen negativen Output gibt, wenn beide Inputs negativ sind, wodurch aber auch 3mal so viele positive Bereiche entstehen.

Input		Output
x_1	x_2	t
1	1	1
1	-1	1
-1	1	1
-1	-1	-1

3.5.4. Praktische Beispiele

Nachdem uns diese Theorien bekannt waren begannen wir selbst mit der Programmierung von Neuronalen Netzen. Erste Beispiele waren dabei die oben bereits ausführlich beschriebenen AND und OR Funktionen. Nachdem wir diese problemlos gemeistert hatten, machten wir und auf die Suche nach komplexeren neuronalen Netzen. Da bildeten sich dann mehrere Gruppen die in verschiedene Richtungen gingen

4. Programme

4.1. Personenerkennung

4.1.1. Allgemeines

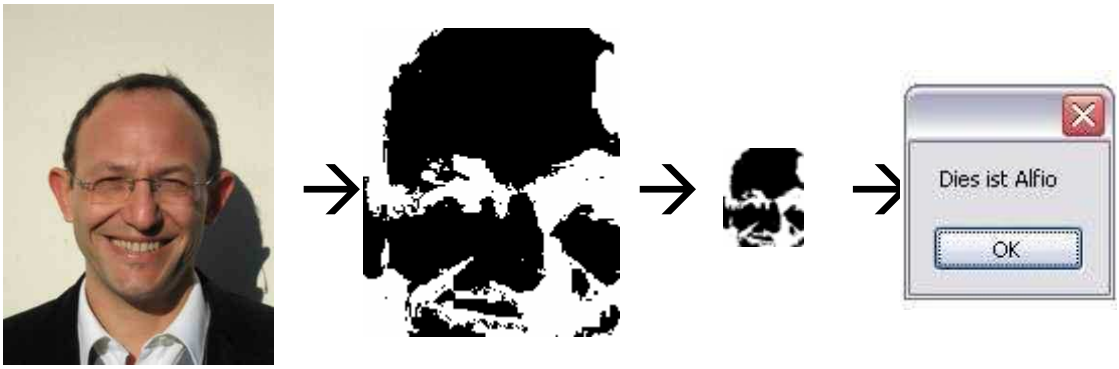
Hierbei wurde ein Programm in C# erstellt, das in der Lage ist, Gesichter anhand der Anordnung der Pixel zu erkennen. Das Bildformat und die Größe des Bildes spielen dabei keine Rolle. Sogar bei verrauschten, also nahezu unerkenntlichen Bildern erkennt das Programm die zugehörige Person.
Die Anwendung baut auf der oben beschriebenen Hebb'schen Lernregel w(neu) = w(alt) + yx.

4.1.2. Funktionsweise

Als Lernmaterialien stehen Bilder der zu lernenden Personen zur Verfügung. Diese werden auch vorher modifiziert damit das Programm auch lernt auf Fehler richtig zu reagieren. Die HSB Farbwerte der Bilder werden eingelesen, alle Hautfarben auf schwarz und alles Andere auf weiß gesetzt. Dadurch bleiben nur die Gesichtsfarben bestehen

Danach wird der weiße Rand weggeschnitten um störende Rahmen loszuwerden. Dieser ist vor allem unnötig wenn die Gesichtbilder, anschließend auf eine Einheitsgröße von 50x50 Pixel zurechtgeschnitten werden um zu kleine Gesichtsformen zu vermeiden. Danach beginnt der eigentliche Lernvorgang. Hier werden auch die einzelnen, zum Teil modifizierten, Bilder gelernt um sie später dann wiederzuerkennen. Die so entstandenen Gewichte, werden in einer Datei erneutes lernen zu ersparen, gespeichert.

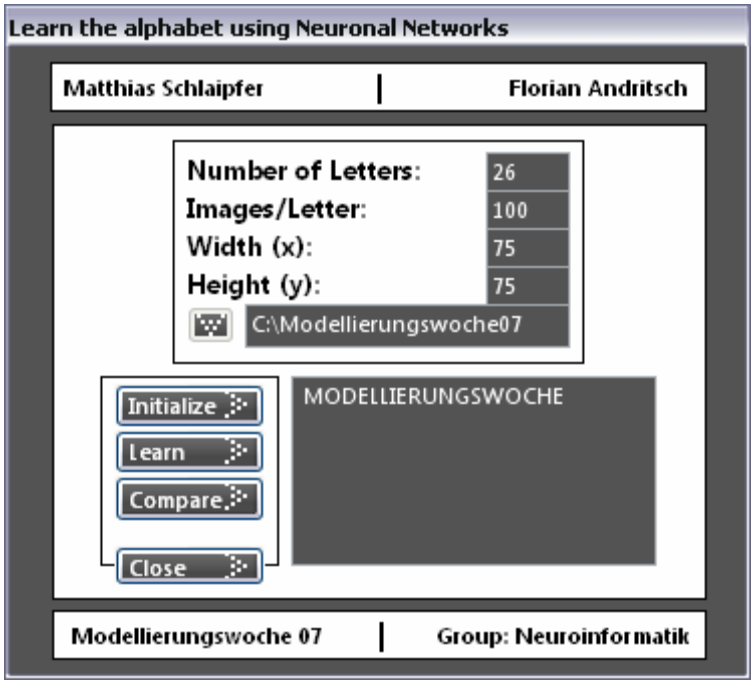
Wann man dem Programm jetzt weitere Bilder, auch von schlechter Qualität, zeigt erkennt es diese, und zeigt den Namen der jeweiligen Person an, sofern ihm diese bekannt ist.


Dies ist Alfio
OK

4.2. Texterkennung

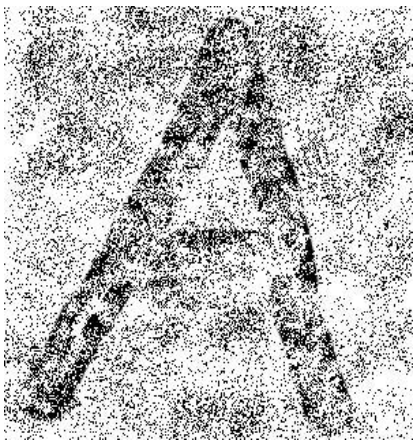
4.2.1. Allgemeines

Das parallel erstellte Programm ist in der Lage, Blockbuchstaben zu erkennen und zu benennen. Weiters kann es einzelne Buchstaben aus Texten filtern, dadurch werden unbearbeitbare Texte bearbeitbar. Dazu wird dem Programm erst das Alphabet beigebracht anhand mehrerer Beispiele der einzelnen Buchstaben.
Dieses Programm baute abermals auf der Heeb'schen Lernregel auf.



4.2.2. Funktionsweise

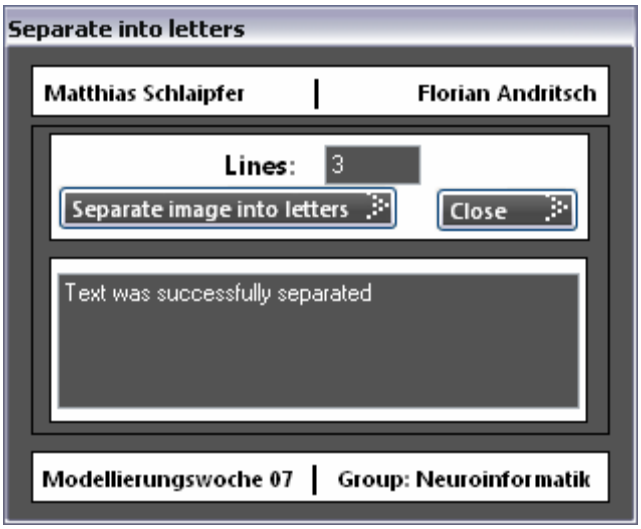
Zu Beginn werden auch hier die zum Lernen erstellten Bilder eingelesen. Diese werden so oft über die Hebb Regel gelernt bis die Abbruchsbedingung eingetreten ist. Die gelernten Gewichte und Bias werden im Programm gespeichert. Damit ist der Lernvorgang beendet.
Danach können Vergleichsbilder eingelesen werden. Selbst wenn diese nur ähnlich den gelernten Bildern, aber noch nicht bekannt sind, ist das Programm in der Lage diese zu erkennen.



4.2.3. Zusatzprogramme

a) Zum Zerschneiden eines eingescannten, handgeschriebenen Textes wurde von den Teilnehmern ein eigenes Programm entwickelt. Es kann aus einem Foto von

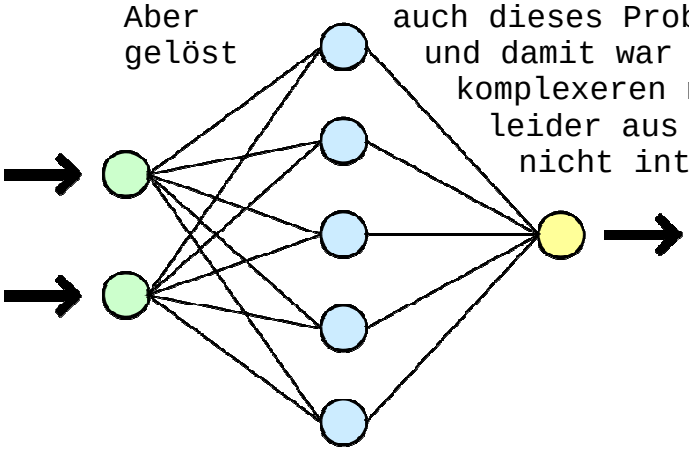
b) einem Text, die Buchstaben automatisch nacheinander herausschneiden und speichern.
Zuerst wird in diesem Programm das Foto nach leeren Pixelzeilen durchsucht, in Zeilen zerlegt und intern gespeichert. Diese werden dann nach leeren Pixelspalten durchsucht und extern in einer Bilddatei gespeichert. Aus Zeitmangel haben wir uns auf Blockbuchstaben beschränkt, obwohl noch viel möglich gewesen wäre.

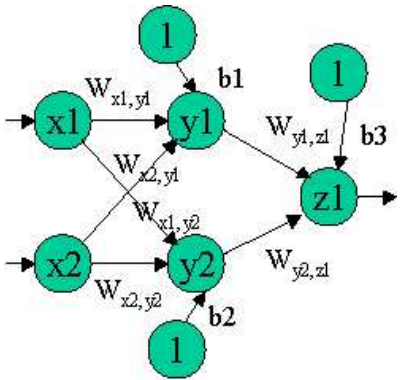


c) Weiters wurde ein Programm erstellt, dass uns automatisch beliebig viele Abwandlungen unserer ausgeschnittenen Ausgangsbuchstaben generiert, um einfach Vergleichsmaterial zu erhalten.

4.3. XOR

Die dritte Richtung in unserer Entwicklung eines neuronalen Netzes bestand darin, ein Programm zu erstellen, das das schwierige XOR-Problem(explicit OR) lösen kann. Das schwierige an dieser Richtung war, das im Gegensatz zu den anderen beiden Programmen kein zwei-, sondern ein dreischichtiges Netzwerk erstellt werden musste. Eine versteckte (hidden) Zwischenschicht ist notwendig, da die XOR-Funktion nicht linear seperabel, sondern logisch zu erschließen ist. Aber auch dieses Problem wurde schließlich von uns gelöst und damit war das der Einstieg in die Welt der komplexeren neuronalen Netze, den wir aber leider aus Zeitmangel nicht intensivieren konnten.





5. Outtakes

Getrunkene Getränke im Raum:	32 Liter
Maximale Dimensionen von Arrays:	3-4
Gearbeitete Zeit:	**360 Stunden(72h/tag)** (12h/person/tag) in 5 Tagen!!!
Chips zum Pokern:	500
Laptops:	7

mind.22

6. Quellcode

Lernen nach HEBB’schen Regel

```
        private void Lernen()
        {
            y_in = new int[anzahly];
            weight = new int[anzahly,breite,hoehe];
            weighttemp = new int[anzahly,breite,hoehe];
            bias = new int[anzahly];
            y = new int[anzahly];
            bool abbruch = false;
            int abbruchzaehler = 0;
         while (!abbruch)
         {
             for (int i = 0; i < anzahlbges; i++)
            {
            for (int u = 0; u < anzahly; u++)
            {

                y_in[u] = 0;

                   for (int b = 0; b < breite; b++)
                    {
                        for (int h = 0; h < hoehe; h++)
                        {
                        y_in[u] = y_in[u] + (x[i, b, h] * weight[u, b, h]);
                        weighttemp[u,b,h]=weight[u,b,h];
                        }
                    }
                    y_in[u]+= bias[u];
                    if (y_in[u] >= 0) y[u] = 1;
```

```
                    else y[u] = -1;

                }

                for (int u = 0; u < anzahly; u++)
                {
                   if (t[u, i] != y[u])
                    {
                       for (int b = 0; b < breite; b++)
                         {
                            for (int h = 0; h < hoehe; h++)
                                 {
                                     bias[u] = bias[u] + t[u, i];

                weight[u, b, h] = weight[u, b, h] + (t[u, i] * x[i, b, h]);

                                 }
                          }

                    }
                }
            }

            for (int u = 0; u < anzahly; u++)
            {
                for (int b = 0; b < breite; b++)
                {
                    for (int h = 0; h < hoehe; h++)
                    {
                        if (weighttemp[u, b, h] == weight[u, b, h])
                        abbruchzaehler++;
                    }
                }
            }
            if (abbruchzaehler == anzahly * size) abbruch = true;
            else abbruchzaehler = 0;
        }

        }
```

7. Quellen

Neuronale Netze – Rüdiger Brause ISBN#3-519-02247-8

Fundamentals of Neural Networks - Laurene Fausett ISBN#81-317 0053-4

de.wikipedia.org DNS 66.230.200.100

Alfio Borzi DNA nicht bekannt

und viele mehr

KRYPTOLOGIE

ALBERT KATHARINA, BLODER BERNHARD,
DITTMER LISA, KOCH TANJA, LASNIK MICHAEL,
SARTORY ALEXANDER, WINKLER GEORG

PROJEKTLEITER:
GÜNTER LETTL

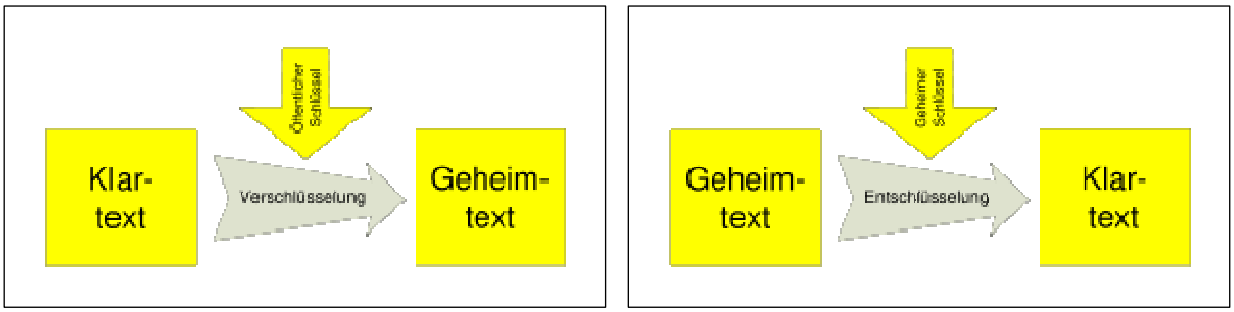
INHALTSVERZEICHNIS

EINLEITUNG

Definition

Die Kryptologie (vom griechischen kryptós, „verborgen“, und logos = Lehre, Kunde) ist die Wissenschaft, die sich mit dem Ver- und Entschlüsseln eines Textes beschäftigt. Unter Verschlüsselung versteht man im Allgemeinen das Verändern eines Textes, sodass ein Außenstehender die Botschaft nicht mehr lesen bzw. verstehen kann.

Die Kryptologie nutzt die Erkenntnisse der Mathematik und der theoretischen Informatik um Verschlüsselungsverfahren zu entwickeln und verschlüsselte Texte zu entschlüsseln. Die Kryptologie lässt sich in zwei Teilgebiete teilen: Kryptografie und Kryptoanalyse.
Die *Kryptografie* beschäftigt sich mit der Entwicklung von Verschlüsselungsverfahren. Man versucht Informationen, Daten oder Nachrichten so zu verschlüsseln, dass sie nur von berechtigten Personen gelesen werden können. In der Kryptografie unterscheidet man zwischen den Methoden der klassischen Kryptografie und denen der modernen Kryptografie. Die Methoden der klassischen Kryptologie sind unter anderem Transposition (die Buchstaben der Botschaft werden einfach anders angeordnet) und Substitution (die Buchstaben der Botschaft werden durch andere Zeichen oder Symbole ersetzt). Die moderne Kryptografie nutzt vorwiegend die Hilfe von Computern um Texte zu verschlüsseln, wobei die Buchstaben in Bytes (8 Bits entsprechen einem Buchstaben, also einem Byte) umgewandelt werden.
Als Gegenstück zur Kryptografie ist das Ziel der *Kryptoanalyse* die verschiedenen kryptografischen Verfahren auf ihre Sicherheit zu überprüfen, indem sie deren Schwachstellen aufzudecken versuchen.
Man unterscheidet auch zwischen zwei verschiedenen Arten von Kryptosystemen.
Ein symmetrisches Kryptosystem verwendet den gleichen Schlüssel zur Ver- und Entschlüsselung. Ein großer Nachteil des symmetrischen Verfahrens ist der Gebrauch desselben Schlüssels, denn ist dieser einem Angreifer bekannt, kann er an die verschlüsselte Information gelangen und auch Fehlinformationen durch Veränderung der Originalnachricht verbreiten bzw. an den eigentlichen Empfänger der Nachricht weiterleiteten. Ein asymmetrisches Kryptosystem hingegen arbeitet mit einem Schlüsselpaar. Dieses Schlüsselpaar besteht aus einem privaten Schlüssel (geheimen Schlüssel) und einem öffentlichen Schlüssel. Der öffentliche Schlüssel ist, wie der Name sagt, öffentlich zugänglich. Jeder Anwender kann diesen Schlüssel benutzen, um an den Eigentümer eine Nachricht zu versenden. Der private Schlüssel wird vom Besitzer geheim gehalten. Er dient dazu, die an ihn gesendete, verschlüsselte Nachricht (Geheimtext) zu entschlüsseln.



Geschichte

In der Antike wurde der Grundstein für die frühe Kryptologie gelegt. 500 v. Chr. benutzten die Spartaner die Skytala. Die Skytala war ein Zylinder um den ein Band gewickelt wurde, auf den der Klartext längs geschrieben wurde. Der Empfänger besaß einen Zylinder in der richtigen Größe und konnte somit den Text entziffern.

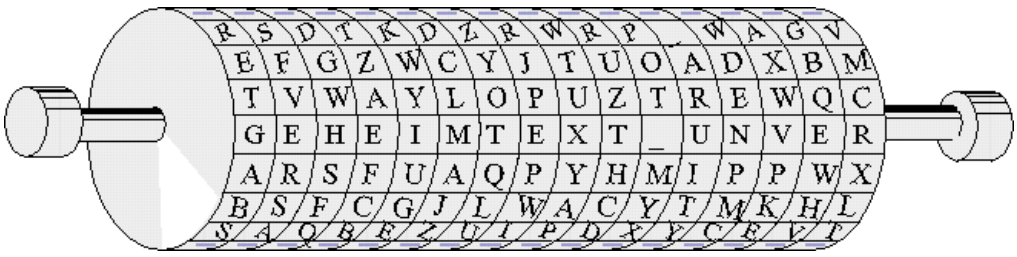
Datierte Funde weisen darauf hin, dass Gäius Julius Caesar sowie darauffolgenden römischen Kaisern diverse Kodierungsverfahren bekannt waren. Das Bekannteste war die so genannte Caesarverschiebung (siehe Verschlüsselungsmethoden).

Später gewann die Substitutionsverschlüsselung an Bedeutung. Hier wurden einfach die Buchstaben der Botschaft durch andere Buchstaben oder Symbole ersetzt. Dieses Verfahren bot im frühen Mittelalter ausreichenden Schutz vor Feinden bis zur Entwicklung der Häufigkeitsanalyse 900 n.Chr.

Die Häufigkeitsanalyse findet ihren Ursprung im Orient. Man glaubte damals, dass der Koran versteckte Botschaften beinhalte und aus diesem Grund begannen arabische Gelehrte die Buchstaben abzuzählen, nach ihrer Häufigkeit anzuordnen und diese zu deuten. In jeder Sprache kommen in einem normalen Text die Buchstaben mit unterschiedlicher Häufigkeit vor. In der deutschen Sprache ist zum Beispiel das „e“ der häufigste Buchstabe, der zweithäufigste das „n“. (Anwendung der Häufigkeitsanalyse siehe Caesarverschlüsselung)

Später entwickelte Blaise de Vigenère (1523-1596) ein Verschlüsselungsverfahren, das für lange Zeit als sicher galt. Das Vigenère-Verfahren ist eine Weiterentwicklung der Caesarsverschlüsselung, dessen Verschlüsselungsmethode durch ein Schlüsselwort verbessert wurde. 1854 fand der Brite Charles Babbage (1791-1871) endlich einen Weg die raffinierte Vigenère-Verschlüsselungsmethode (siehe Verschlüsselungsmethoden) zu knacken, doch erst Friedrich Kasiski veröffentlichte 1867 seine Lösung.

Im ersten Weltkrieg wurde die Jefferson-Walze, die von Thomas Jefferson 1790 entwickelt wurde, bei den US-Streitkräften zur Codierung von Nachrichten eingesetzt. Der Zylinder besteht aus mehreren drehbaren Holzscheiben, auf denen die Buchstaben des Alphabetes in beliebiger Reihenfolge aufgetragen waren. Der Klartext wird durch Drehen der einzelnen Scheiben eingestellt, und als Chiffretext wird eine beliebige andere Zeile auf der Walze gewählt. Die Entschlüsselung wird mit einer völlig identischen Walze durchgeführt: der Chiffretext wird eingestellt und in einer der anderen Zeilen erscheint der (sinnvolle) Klartext.



Ein weiteres Verschlüsselungsverfahren im ersten Weltkrieg war das Checkerboard (eng. „Schachbrett“) bzw. das ADFGX-Quadrat (siehe Verschlüsselungsverfahren), das von den Deutschen verwendet wurde. Dieses Verschlüsselungsverfahren beruht auf der Idee des Polybiosquadrates, welches angeblich bereits 100 v.Ch. von Polybios angewendet wurde. Das ADFGX-Verfahren ist zweistufig aufgebaut und basiert auf dem Prinzip der Substitution (Ersetzung von Zeichen durch andere) gefolgt von einer Transposition (Vertauschung der Anordnung der Zeichen).

Wirkliche Fortschritte in der Kryptologie gab es durch mechanische oder elektronische Verschlüsselungsapparate. Die wohl bekannteste dürfte die „Enigma“ sein: Ein nur schreibmaschinengroßes Gerät, welches aber fast während des gesamten zweiten Weltkriegs ein unüberwindbares Hindernis für die Abhörung des deutschen Funks darstellte. In dieser Zeit wurden die ersten Computer erfunden, die zu einem erheblichen Fortschritt in der Entschlüsselung von Geheimnachrichten führten.

Heutzutage spielt die sichere Übertragung von Informationen, wie z. B. Passwörtern oder Kreditkartennummern, eine besonders große Rolle. Um eine sichere Übertragung von Daten zu gewährleisten, entwickelten Diffie und Hellman 1976 die Idee des „Public Key“ - Verfahrens. Dabei handelt es sich um ein asymmetrisches Verfahren, bei dem jeder Teilnehmer einen öffentlichen und einen privaten Schlüssel erhält. 1977 wurde das RSA-Verfahren (siehe Verschlüsselungsmethoden), eine Umsetzung des „Publik-Key“-Verfahrens, verwirklicht.

VERSCHLÜSSELUNGSMETHODEN

Caesarverschlüsselung

Bei diesem Verschlüsselungsverfahren werden die Buchstaben des Alphabetes verschoben. So wird zum Beispiel bei einer Verschiebung um 3 Positionen aus dem „A“ ein „D“, aus dem „B“ ein „E“ usw.

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

Beispiel: verschoben
yhuvfkrehq

Methode zur Entschlüsselung

Bei ausreichend langen Texten kann zum Entschlüsseln die Häufigkeitsanalyse verwendet werden. Hierbei beachtet man die statistische Wahrscheinlichkeit, die angibt wie häufig die Buchstaben der (z.B. deutschen) Sprache in einem beliebigen Text aufscheinen.

	A	*B*	*C*	*D*	*E*	*F*	*G*
Deutsch	6.51%	1.89%	3.06%	5.08%	17.4%	1.66%	3.01%
Englisch	7.23%	0.6%	2.82%	4.83%	15.66%	1.67%	2.16%

	H	*I*	*J*	*K*	*L*	*M*	*N*
Deutsch	4.76%	7.55%	0.27%	1.21%	3.44%	2.53%	9.87%
Englisch	4.02%	7.87%	0.06%	0.64%	3.96%	2.36%	8.14%

	O	*P*	*Q*	*R*	*S*	*T*	*U*
Deutsch	2.51%	0.79%	0.02%	7.0%	7.27%	6.15%	4.35%
Englisch	7.16%	1.61%	0.07%	7.51%	7.15%	7.73%	2.72%

	V	*W*	*X*	*Y*	*Z*
Deutsch	0.67%	1.89%	0.03%	0.04%	1.68%
Englisch	1.17%	0.78%	0.3%	1.13%	0.1%

In der deutschen Sprache ist der Buchstabe „e“ bei weitem am häufigsten. Wurde also ein (deutscher) Text mit der Caesarverschlüsselung verschlüsselt, kann man davon ausgehen, dass es sich bei dem Zeichen mit der größten Häufigkeit um ein „e“ handelt. Bei der Verschlüsselung durch Substitution beliebiger Zeichen oder Buchstaben wäre es vielleicht ratsam weiter mit der Häufigkeitsanalyse fortzufahren, doch bei der Caesarverschlüsselung ist bereits der Schlüssel („wie man den Text ver-/entschlüsseln muss“) nach dem Auffinden einer Zuordnung bekannt. (z.B.: aus „e“ wird „h“ → bei dem Verschlüsseln wurde also um 3 Stellen „weitergezählt“)

Doch nicht jede Verschlüsselung beruht auf dem Prinzip von simpler Substitution allein, wie dies bei der Caesarverschlüsselung der Fall war. So lässt sich das Decodieren bei anderen Verschlüsselungsarten (wie dem Vigenère-Verfahren) oft nicht mehr mit Hilfe der Häufigkeitsanalyse durchführen – z.B.: wenn eine „geschicktere“ Substitution angewendet wurde, z.B. den Buchstaben „e“, „n“, etc. wurden mehrere Zeichen zugeordnet, so wären andere Vorgehensweisen vorteilhaft. Um nun zu erkennen, ob ein Text mit einem einfachen Substitutionsverfahren verschlüsselt wurde, ist es hilfreich sich der Wahrscheinlichkeits-rechnung zu bedienen.

Die Wahrscheinlichkeit, dass 2 zufällig gewählte (aus dem Text werde 2 Buchstaben willkürlich gewählt) Buchstaben gleich sind, lässt sich durch die Formel wie folgt berechnen:

$n_1,n_2,\ldots n_x$ …… Anzahl der jeweils vorkommenden Zeichen

Beispiel:
Verschlüsselter Text: ajiahdrnakdena
n_1(Anzahl aller „a“) = 4
n_2(Anzahl aller „d“) = 2
n_3 …
….

$$I = \frac{n_1 \cdot (n_1 - 1) + n_2 \cdot (n_2 - 1) + ... + n_x \cdot (n_x - 1)}{n \cdot (n - 1)}$$

In einem durchschnittlichen, unverschlüsselten, deutschen Text befindet sich der Wert für I ungefähr im Bereich 0,0762. (Englisch: I = 0,0611). Wenn alle Buchstaben in dem Text gleich häufig aufscheinen würden, so wäre I = 0,0385.
Je geschickter ein Text durch Zuweisung von neuen Werten verschlüsselt wurde (B.: „e“ wird zu „┼“ und „⌂“) um die Häufigkeit des verwendeten Buchstabens bzw. Zeichens zu senken, desto eher wird der Wert von I zu 0,0385 tendieren und das Dechiffrieren mit Hilfe von der Häufigkeitsanalyse fehlschlagen.

Vigenère –Verfahren

Ähnlich wie bei der Caesarverschlüsselung wird das Prinzip der Buchstabenverschiebung angewendet (z.B.: jedem Buchstaben wird der Buchstabe der 3 Stellen danach folgt zugeordnet). Um die geheime Nachricht gegen Decodierungsverfahren robuster zu machen, bedient man sich der Hilfe eines so genannten Schlüsselwortes. Man wählt nicht mehr einen einzigen Grad der Verschiebung (alle Buchstaben 3 weiter), sondern verschlüsselt die zu übermittelnde Botschaft mit Hilfe des Schlüsselwortes und eines Vigenère-Quadrates.

Ein Text wird in ein Schlüsselwort umgewandelt und mithilfe des Vigenère-Quadrates verschlüsselt. Um diesen Text zu dechiffrieren muss dem Empfänger das Schlüsselwort bekannt sein.

Beispiel:
zu verschlüsselnde Nachricht: Grüsse aus Seggau
gewähltes Schlüsselwort: Licht

G	r	u	e	s	s	e	a	u	s	S	e	g	g	a	u
L	i	c	h	t	L	i	c	h	t	L	i	c	h	t	L
R	Z	W	L	L	D	M	C	B	L	D	M	I	N	T	F

Vigenère-Quadrat			
		Text	
		A B C D E F G H I J K L M N O P Q R S T U V W X Y Z	
Key	A	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z	**Geheimtext**
	B	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A	
	C	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B	
	D	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C	
	E	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D	
	F	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E	
	G	G H I J K L M N O P Q R S T U V W X Y Z A B C D E F	
	H	H I J K L M N O P Q R S T U V W X Y Z A B C D E F G	
	I	I J K L M N O P Q R S T U V W X Y Z A B C D E F G H	
	J	J K L M N O P Q R S T U V W X Y Z A B C D E F G H I	
	K	K L M N O P Q R S T U V W X Y Z A B C D E F G H I J	
	L	L M N O P Q R S T U V W X Y Z A B C D E F G H I J K	
	M	M N O P Q R S T U V W X Y Z A B C D E F G H I J K L	
	N	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M	
	O	O P Q R S T U V W X Y Z A B C D E F G H I J K L M N	
	P	P Q R S T U V W X Y Z A B C D E F G H I J K L M N O	
	Q	Q R S T U V W X Y Z A B C D E F G H I J K L M N O P	
	R	R S T U V W X Y Z A B C D E F G H I J K L M N O P Q	
	S	S T U V W X Y Z A B C D E F G H I J K L M N O P Q R	
	T	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S	
	U	U V W X Y Z A B C D E F G H I J K L M N O P Q R S T	
	V	V W X Y Z A B C D E F G H I J K L M N O P Q R S T U	
	W	W X Y Z A B C D E F G H I J K L M N O P Q R S T U V	
	X	X Y Z A B C D E F G H I J K L M N O P Q R S T U V W	
	Y	Y Z A B C D E F G H I J K L M N O P Q R S T U V W X	
	Z	Z A B C D E F G H I J K L M N O P Q R S T U V W X Y	

Bestimmen der Länge des Schlüsselwortes mit Hilfe der Mathematik

Die Länge des Schlüsselwortes sei l und die Anzahl der Zeichen des Textes sei n. Dann ergibt sich für die Länge des Schlüsselwortes die Formel:

$$l = \frac{0{,}0377 \cdot n}{(n-1) \cdot I + 0{,}0762 - 0{,}0385}$$

Das Ergebnis dieser Formel sollte lediglich als Richtwert gelten (ganze Zahlen als Ergebnis werden eher rar sein), da es oft ungenau ist. Weiters ist es nur anwendbar, wenn der Text eine ausreichende Länge besitzt.

Ableitung der Formel:
Da die Ableitung der Formel auf den ersten Blick eher diffizil erscheinen mag, folgt eine etwas weitläufigere Erklärung:

n sei die Gesamtanzahl der Buchstaben des verschlüsselten Textes, l die Länge des verwendeten Schlüsselwortes. Nun ein kleines Gedankenexperiment: das Schlüsselwort wird von seinem ersten Buchstaben bis zu seinem letzten aufgeschrieben.

In einer Art Tabelle wird dann der Text der verschlüsselten Nachricht unter den jeweiligen Buchstaben des Schlüsselwortes geschrieben. Sobald der *l*-te Buchstabe eingetragen worden ist, beginnt man wieder in der 1. Zeile.

1	2	3	…	…	…	…	*l*
G	H	Z	…	…	…	…	K
K	V	…	…	…	…	…	…
…	…	…	…	…	…	…	…

In jeder Spalte dieser Tabelle sind dann ~ $\frac{n}{l}$ Zeichen. Wenn man einen beliebigen Buchstaben auswählt (dafür gibt es *n* Möglichkeiten), so erhält man für die Anzahl der Möglichkeiten, dass beide Buchstaben aus derselben Spalte sind, $n \cdot (\frac{n}{l} - 1)$, die Anzahl der Möglichkeiten , dass die beiden Buchstaben aus verschiedenen Spalten sind, ist $n \cdot (n - \frac{n}{l})$. Kombiniert man nun diese Aussagen, so erhält man:

$$I = \frac{0{,}0762 \cdot n \cdot (\frac{n}{l} - 1) + 0{,}0385 \cdot n \cdot (n - \frac{n}{l})}{n \cdot (n-1)}$$

I ist (wie oben) die Wahrscheinlichkeit, dass 2 zufällig gewählte Buchstaben gleich sind. Innerhalb einer Spalte sind diese Buchstaben (sofern die Anzahl der Buchstaben groß genug ist) etwa in den Relationen der Häufigkeitsanalyse vorhanden (sprich: am meisten „e“, dann „n“, …etc.), daher erhält man auch mit derselben Wahrscheinlichkeit zwei gleiche Buchstaben wie im Deutschen (nämlich 0,0762). Bei Buchstaben in verschiedenen Spalten geht man davon aus, dass sie mehr oder weniger regelmäßig verteilt sind (da nicht mehr verschlüsselter Buchstabe = gleicher Buchstabe in der unverschlüsselten Nachricht gilt), also nimmt man hier als Wahrscheinlichkeit 0,0385 an. Dies mit der Anzahl aller wählbarer Buchstabenpaare $n \cdot (n-1)$ kombiniert ergibt die oben genannte Formel.

Nun wird diese Formel mit Hilfe algebraischer Umformungen nach *l* gelöst. Daraus ergibt sich die Formel mit der *l*, also die Länge des Schlüsselwortes, ausgerechnet werden kann (der Faktor I kann jederzeit berechnet werden, Formel siehe oben). Voila!:

$$l = \frac{0{,}0377 \cdot n}{(n-1) \cdot I + 0{,}0762 - 0{,}0385}$$

Checkerboard

Die Verschlüsselung eines Textes erfolgt dadurch, dass Klartextzeichen monoalphabetisch (es wird für jedes Zeichen des Klartextes stets dasselbe Geheimzeichen verwendet) durch Zeichenpaare ersetzt werden, die nur aus den Buchstaben „A“, „D“, „F“, „G“ und „X“ bestehen. In eine Tabelle werden jeweils in der ersten Horizontalen und Vertikalen die Buchstaben „A“, „D“, „F“, „G“ und „X“ eingetragen. In die restlichen 25 freien Felder werden alle Buchstaben des Alphabets eingetragen. Um nun eine Botschaft zu verschlüsseln ersetzt man den gewünschten Buchstaben der Botschaft durch das zugewiesene Buchstabenpaar.

Beispiel:
zu verschlüsselnde Botschaft: Mathematik

M A T H E M A T I K
AD DD XG DG FA AD DD XG AF GF

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

Handyverschlüsselung (entworfen von A. Sartory)

Die „Handyverschlüsselung“ wurde im Rahmen der Modellierungswoche entworfen. Sie ist ein Verschlüsselungssystem, das sich auf die Verteilung der Buchstaben am Handy zurückführen lässt. Dabei wird jeder Buchstabe durch 2 Zahlen ersetzt, die dann anstelle der Nachricht verschickt werden. Die 2 Zahlen jedes Buchstabens werden folgendermaßen gewählt:
Die erste Zahl gibt die Handytaste an, auf der sich der Buchstabe befindet, an. (z.B.: A:2, also A liegt auf Taste 2; B:2, D:3, K:5,…). Da mehrere Buchstaben dieselbe Taste teilen, wird nun eine zweite Zahl angehängt, die angibt, an welcher Stelle sich der Buchstabe befindet (z.B.: A:21 (A:2.Taste, 1.Buchstabe), B:22, C:23,…). Auf Satzzeichen werden bis auf den Punkt (11), der die Nachricht gliedert, verzichtet.
Da dieses Verschlüsselungsverfahren nur ca. 30 der 99 Möglichkeiten benötigt, können Werte, die eigentlich keine Buchstaben ergeben würden (z.B.: 29, 67, 38, 12,…..), verwendet werden, um die Entschlüsselung, für jemanden, der das Verfahren nicht kennt, zu erschweren.

Schlüssel	*1	*2	*3	*4
1*	.			
2*	A	B	C	
3*	D	E	F	
4*	G	H	I	
5*	J	K	L	
6*	M	N	O	
7*	P	Q	R	S
8*	T	U	V	
9*	W	X	Y	Z

Beispiel zur Entschlüsselung einer Handyverschlüsselung:
Verschlüsselte Nachricht:
831532737488234253998232747432534582624176116143818511421621623193 36

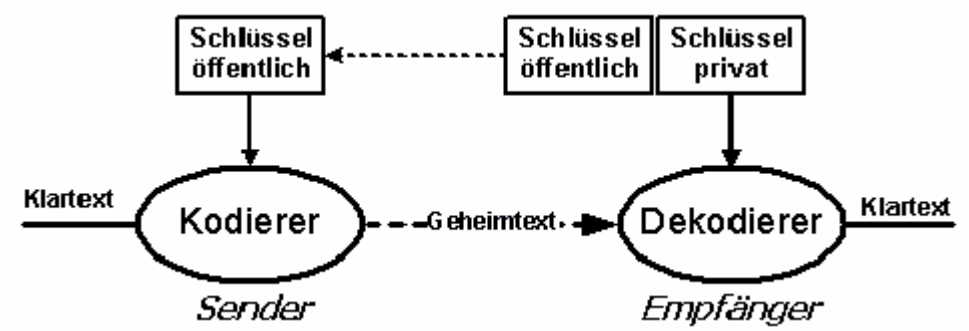
1. Schritt: In Zweiergruppen anschreiben:
83 15 32 73 74 88 23 42 53 99 82 32 74 74 32 53 45 82 62 41 76 11 61 43 81 85 11 42 16 21 62 31 93 36

2. Schritt: Nicht definierte Zahlen entfernen:
83 32 73 74 23 42 53 82 32 74 74 32 53 82 62 41 11 61 43 81 11 42 21 62 31 93

3. Schritt: Entschlüsseln:
VERSCHLUESSELUNG.MIT.HANDY
Nachricht:
Verschlüsselung mit Handy

Public Key

Unter „Public Key“-Verfahren versteht man eine Verschlüsselungsmethode, die einen sicheren Datentransfer im Internet ermöglicht: Selbst wenn der Schlüssel und die verschlüsselte Nachricht bekannt sind, sollte es für Außenstehende unmöglich sein, den geheimen Text zu entschlüsseln.
1976 entwickelten Whitfield Diffie und Martin Hellman die Idee eines neuen Chiffrier-modells, das erstmals zur Verschlüsselung einen asymmetrischen Schlüssel benutzen sollte. Jedem Teilnehmer in einem System ist ein öffentlicher Schlüssel („Public Key“) zugeordnet, der in einem öffentlichen Verzeichnis steht. Mit diesem Schlüssel kann jeder andere Teilnehmer dem Besitzer eine Nachricht schicken, welche mit diesem Schlüssel chiffriert ist. Die Botschaft kann von Außenstehenden nicht gelesen werden, denn nur der Empfänger kann mit seinem privaten Schlüssel („Private Key“) den verschlüsselten Text dechiffrieren. Dazu muss es für Außenstehende unmöglich sein, irgendwie aus dem „Public Key“ den „Private Key“ bestimmen zu können.



Doch es gelang Whitfield Diffie und Martin Hellman nicht, diese Idee in die Praxis umzu-setzen. 1977 entwickelten Ronald L. Rivest, Adi Shamir und Leonard M. Adleman ein Verfahren, mit dem die Idee eines Public Keys-Verfahrens verwirklicht werden konnte. Dieses revolutionäre Verfahren ist heute als das RSA-Verfahren bekannt.

RSA-Verfahren

Die unverschlüsselte Nachricht (Klartext) wird mit m (für engl.“message“) und die verschlüsselte Nachricht wird mit c (für engl.“chiffre“) benannt. Der öffentliche Schlüssel (Public Key) wird mit e und der private Schlüssel (Private Key) mit d bezeichnet.

Um ein RSA-Schlüsselsystem zu entwerfen, verwendet man zwei große Primzahlen p, q und berechnet n als das Produkt der beiden Primzahlen $p*q$. Als öffentlichen Schlüssel wählt man eine Zahl $e \in \{1,2,..., \varphi(n)\}$ mit $ggT(e, \varphi(n)) = 1$, wobei $\varphi(n) = (p-1)*(q-1)$ ist.

Eine zu verschlüsselnde Nachricht muss zuerst in eine Zahl $m \in \{1,2,3,\ldots,n-1\}$ umgewan-delt werden. Sämtliche Werte müssen ganzzahlig sein. Für das Verschlüsseln benötigt man als „Public Key“ e und n. Die Geheimnachricht c bildet man mit der Verschlüsselungs-vorschrift $m^e \equiv c \bmod(n)$.

Der „Private Key“ d zum Entschlüsseln wird durch $e*d \equiv 1 \bmod(\varphi(n))$ ermittelt. d ist also der inverse Rest zu e modulo n , und man kann ihn leicht mit dem Euklidschen

Algorithmus (siehe Zahlentheorie) berechnen. Um die Geheimnachricht c wieder in den Klartext m zurückzuverwandeln, muss sie nach der Entschlüsselungsvorschrift $c^d \equiv m \bmod(n)$ berechnet werden.

m	unverschlüsselte Nachricht (Klartext)
c	verschlüsselte Nachricht (Chiffre)
e	öffentlicher Schlüssel
d	privater Schlüssel
p, q	Primzahlen
n	Produkt der Primzahlen p und q

Sicherheit

Bis heute sind beim RSA-Verfahren keine großen Schwachstellen bekannt. Da es unendlich viele Primzahlen gibt, gibt es auch unendlich viele Schlüssel, die zum Verschlüsseln einer Nachricht verwendet werden können. Das RSA-System gilt derzeit als sehr sicher, da es selbst für moderne Rechner unmöglich scheint, sehr große Zahlen in deren Primfaktoren zu zerlegen (n=p*q). Das RSA-Verfahren könnte jedoch geknackt werden, wenn es jemandem gelingen würde einen sehr schnellen Algorithmus zur Primfaktorenzerlegung zu finden.

Beispiel für RSA

(P, C, K, E, D)
P= plain text, Klartext (Menge der Texte die man verschlüsseln will,
Menge der Wörter die man mit Buchstaben schreiben kann)
C= chiffre text, Verschlüsselungstexte (Menge der Verschlüsselungen)
K= keys = Menge der Schlüsseln
E= encryption functions = Verschlüsselung
D= decryption functions = Entschlüsselung

$E = \{e_k \mid k \in K\}$ $e_k: P \rightarrow C$
$D = \{d_k \mid k \in K\}$ $d_k: E \rightarrow P$

e= Schlüssel zum Verschlüsseln (öffentlich bekannt)
d= Schlüssel zum Entschlüsseln

2 Primzahlen p,q; $n = p \cdot q$;

$\varphi(n) = (p-1) \cdot (q-1)$

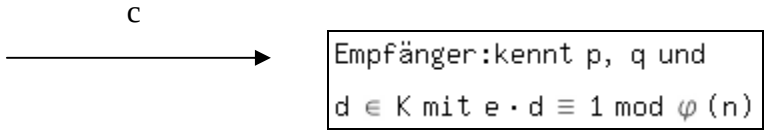
$P = (0,1,2,3,.....n-1) = C$

wähle $e \in (1,2,..., \varphi(n)) = K$

$ggT(e, \varphi(n)) = 1$

Verschlüsseln: $m \in \mathbb{P} : m^e \equiv c \bmod(n)$

m = message , Klartext
c = Chiffretext



Entschlüsselung: $cd \equiv m \bmod (n)$

privat: d, p und q $\Leftrightarrow \varphi(n)$

Öffentlicher Schlüssel: e und n

Obwohl *n* ein Teil des öffentlichen Schlüssels ist (also allgemein bekannt ist), gilt dieses System als sicher, da es bei ausreichend großen Zahlen derzeit unmöglich ist, *n* in seine Primfaktoren zu zerlegen. Je größer die Primzahlen *p* und *q* sind, desto sicherer ist der Schlüssel. Heutzutage sind die Primzahlen mehrere hundert Dezimalstellen lang.

Beispiel:$p = 11,\ q = 23 \Rightarrow n = 253;$

$\varphi(n) = (11 - 1) \cdot (23 - 1) = 10 \cdot 22 = 220$

Public Key:$e = 7,\ n = 253$

Private Key:$p = 11,\ q = 23,\ \varphi(n) = 220$ und $d = 63$

$7 \cdot d \equiv 1 \bmod (220)$

$$\frac{1 + x \cdot 220}{7}$$

$x = 1;\ \frac{221}{7} \rightarrow x \notin \mathbb{N}$

$x = 2;\ \frac{441}{7} = 63 \rightarrow 63 \in \mathbb{N} \Rightarrow d = 63$

Verschlüssle:$m = 101$

$e_7(101) = 101^7 = 101^{1+2+4} = 101 \cdot 101^2 \cdot 101^4 \equiv 101 \cdot 81 \cdot (-17) \equiv 73 \bmod (253)$

NR:$101^2 = 10201 \equiv 81 \bmod (253)$

$101^4 \equiv 81^2 = 6561 \equiv -17 \bmod (253)$

ZAHLENTHEORIE

Kleiner Satz von Fermat

Satz von dem Franzosen Pierre de Fermat (1608- 1665)

$a \in \mathbb{Z} \quad ggT(a,p) = 1 \qquad p \nmid a$
$p \in \mathbb{P}$

$a^{p-1} \equiv 1 \bmod (p)$ nur für nicht Teiler

$a^{p} \equiv a \bmod (p)$ richtig für alle $a \in Z$

Eulersche Phi-Funktion

Funktion von dem Schweizer Leonard Euler (1707-1783)

Euler'sche Phi-Funktion: $n \in \mathbb{N} \qquad \varphi(1) = 1$

$\varphi(n)$ = Anzahl der Zahlen zwischen $1 \le a \le n$ für die $ggT(a,n) = 1$ gilt

$\varphi(2) = 1;\ a = 1,2$
$\varphi(12) = 4;\ a = 1,2,3,4,5,6,7,8,9,10,11,12$
$ggT(a,12) = 1$

$p \in \mathbb{P}: \varphi(p) = p - 1$
zum Bsp: $p(13) = 12$

$$\varphi(p^k) = p^k - p^{k-1} \rightarrow \varphi(p^k) = p^{k-1} \cdot (p-1)$$

$ggT(n,m) = 1;\ \varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$
$n,m \ge 1$

$$\varphi\left(p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_j^{k_j}\right) = \varphi\left(p_1^{k_1}\right) \cdot \varphi\left(p_2^{k_2}\right) \cdot \ldots \cdot \varphi\left(p_j^{k_j}\right)$$

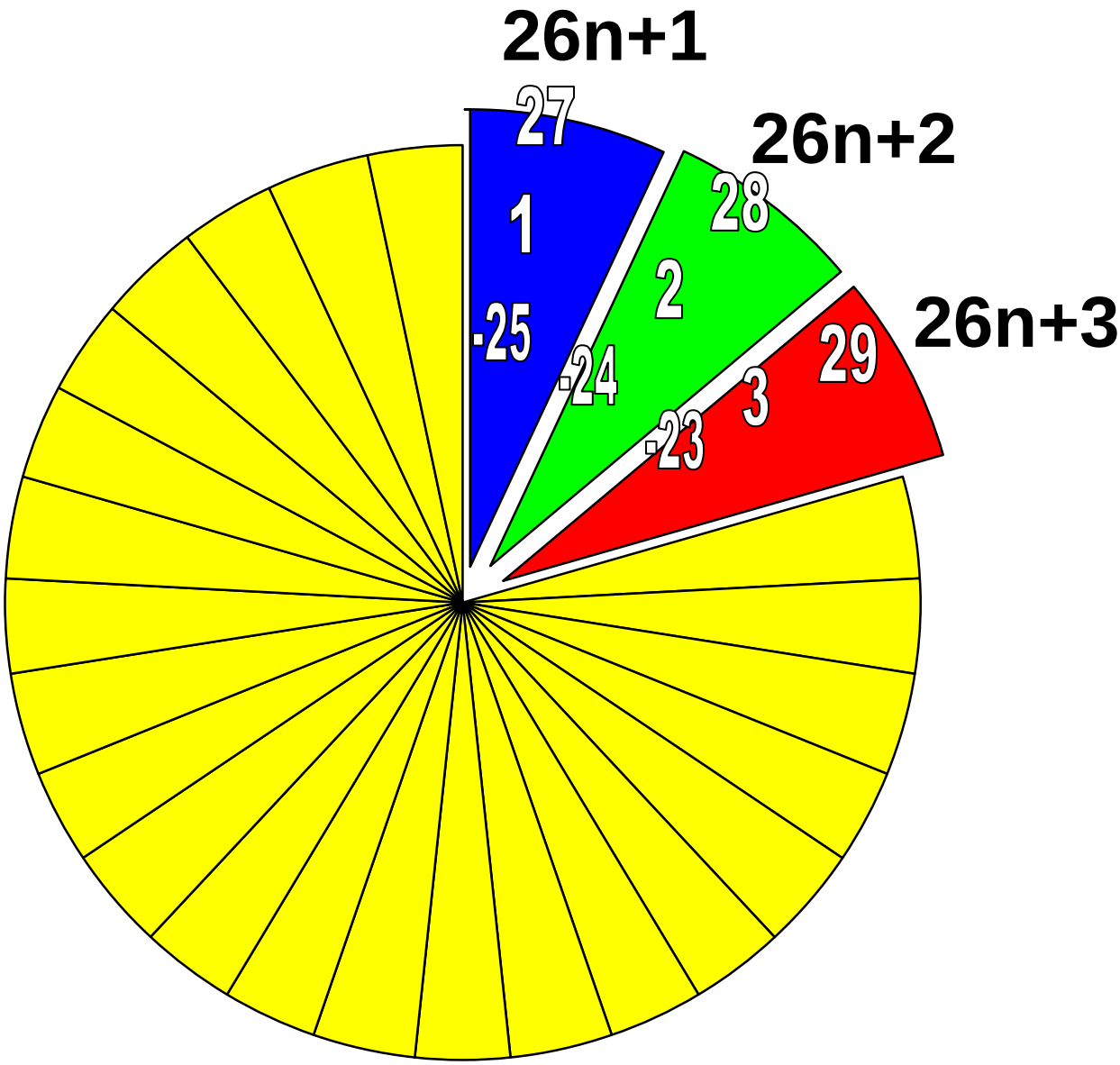
$$\varphi(12) = \varphi(2^2) \cdot \varphi(3^1) = 2^{2-1} \cdot (2-1) \cdot 3^{1-1} \cdot (3-1) = 4$$

Satz von Euler: $n \in \mathbb{N}$
Dann gilt für jedes $a \in \mathbb{Z}$ mit $ggT(a,n) = 1$

$$a^{\varphi(n)} \equiv 1 \bmod (n) \rightarrow a^{\varphi(n)+1} \equiv a \bmod (n)$$

Kongruenzrechnen

Man nennt zwei Zahlen kongruent eines Moduls (einer weiteren Zahl), wenn sie bei der Division durch den Modul denselben Rest haben.



$1 \equiv 27 \bmod (26)$

$1 \equiv 53 \bmod (26)$

$53 \equiv -53 \bmod (26)$

$(26 \cdot n + 1) \cdot (26 \cdot m + 3) = 26(n + m) + 4$

Restklasse 1 + Restklasse 3 = Restklasse 4

$175 - 53 \equiv (19 + 6 \cdot 26) - (1 + 2 \cdot 26) \equiv 19 - 1 \equiv 18 \bmod (26)$

$175 \cdot 53 \equiv ((-7) + 7 \cdot 26) \cdot (1 + 2 \cdot 26) \equiv (-7) \cdot 1 \equiv -7 \bmod (26)$

$1 \cdot ? \equiv 1 \bmod (26)$

$1 \cdot 1 \equiv 1 \bmod (26)$

$2 \cdot ? \equiv 1 \bmod (26)$: es gibt keine Lösung

$a \cdot x \equiv 1 \bmod (m)$

Zu jeder Zahl a mit $ggT(a, m) > 1$ gibt es kein $x \in \mathbb{Z}$ mit $a \cdot x \equiv 1 \bmod (m)$

Zu jeder Zahl a mit $ggT(a, m) = 1$ gibt es eine Zahl a' mit $a \cdot a' \equiv 1 \bmod (m)$
das heißt es gibt keine Lösung für $a = 2$ und $\bmod (26)$, da der ggT 2 ist.

Euklid'scher Algorithmus

Der Euklid'sche Algorithmus, benannt nach Euklid von Alexandria (ca. 365 v. Chr.) ist ein Algorithmus (genau definierte Handlungsvorschrift zur Lösung eines Problems) mit dem man den größten gemeinsamen Teiler zweier natürlichen Zahlen leicht berechnen kann.

$ggT(235177982, 3017562) = d$

$235177982 = 78 \cdot 3017562 - 191854$

$ggT(3017562, 191854) = d$

$3017562 = 16 \cdot 191854 - 52102$

$ggT(191854, 52102) = d$

$191854 = 4 \cdot 52102 - 16554$

$ggT(52102, 16554) = d$

$52102 = 3 \cdot 16554 + 2440$

$ggT(16554, 2440) = d$

$16554 = 7 \cdot 2440 - 526$

$ggT(2440, 526) = d$

$2440 = 5 \cdot 526 - 190$

$ggT(526, 190) = d$

$526 = 3 \cdot 190 - 44$

$ggT(190, 44) = d$

$190 = 4 \cdot 44 + 14$

$ggT(44, 14) = d$

$44 = 3 \cdot 14 + 2$

$ggT(14, 2) = 2$

$$\text{Entschlüsselung: } d_{63}(73) = 73^{63} = 73^{1+2+4+8+16+32}$$

$$= 73^1 \cdot 73^2 \cdot (73^2)^2 \cdot [(73^2)^2]^2 \cdot 73^{16} \cdot 73^{32} \equiv 73 \cdot 16 \cdot 3 \cdot 9 \cdot 81 \cdot (-17) \equiv 101 \bmod (253)$$

NR: $73^2 = 5329 \equiv 16 \bmod (253)$

$73^4 \equiv 16^2 = 256 \equiv 3 \bmod (253)$

$73^8 \equiv 3^2 \equiv 9 \bmod (253)$

$73^{16} \equiv 9^2 \equiv 81 \bmod (253)$

$73^{32} \equiv 81^2 \equiv -17 \bmod (253)$

Quellen: Wikipedia
„Kryptografie in Theorie und Praxis“ von Albrecht Beutelspacher
„Einführung in die Kryptographie“ von Johannes Buchmann
„Decrypted Secrets“ von F.L. Bauer

Woche der Modellierung mit Mathematik

im Schloss Seggau

14. – 20. Januar 2007

Projekt: Alternative Energie

Egger Alexander

Groß Georg

Hell David

Hierz Martin

Pendl Matthias

Teichtmeister Stephan

Triebl Robert

Projektleiter:

a.o. Univ.-Prof. Mag. Dr. Stephen L. Keeling

Inhalt

I. Problemstellung

1.1 Aufgabenstellung

Heutzutage ist alternative Energie ein sehr aktuelles Thema, und die neuesten Heizmethoden werden besonders aktiv im Programm für Umweltsystemwissenschaften an der Karl-Franzens-Universität Graz untersucht. Viele Leute steigen von einer traditionellen Öl- oder Erdgasheizung um, und sie installieren nun lieber ein System basierend z.B. auf Biomasse, Solarenergie oder Erdwärme.

Andererseits haben Konsumenten herausgefunden, dass ein solches System nicht von Jedermann installiert werden kann. In diesem Projekt wird ein bestimmtes Erdwärmesystem analysiert, das von einer internationalen Baufirma mit Material von einer internationalen Erdwärmefirma installiert worden ist. Nachdem gewisse Schwierigkeiten mit dem System aufgetreten waren, haben Techniker von einer oder der anderen Firma nach und nach ihre aktuellste Erklärung für die Systemfehler gegeben.

Das Ziel dieses Projekts ist, dass die Mitglieder der Gruppe sich an die Stelle des Konsumenten versetzen und an Hand der von den Firmen gegebenen Information eine Fehlersuche des Systems durchführen und anschließend entscheiden was mit dem System getan werden soll.

1.2 Spezielle Thematisierung

Unsere Aufgabe besteht darin, im speziellen Fall „Stephen Keeling“ die Probleme und Fehler bei der Installation der Heizung zu untersuchen und auf Änderungsvorschläge hinzuweisen, die die Funktionstüchtigkeit der Heizung wiederherstellen.

Bei Stephens Heizung wurden anstatt der sonst für diese Hausgröße üblichen sechs Erdwärmekollektoren zu je 100m langen Leitungen, anfangs nur ein Kreis mit 550m Länge verlegt, welcher aber später im Zuge der Bauarbeiten in drei unterschiedlich lange Kollektorkreise zerteilt wurde.

Ein weiters Problem, das es zu analysieren gilt, stellt die Schräglage, in der die Kollektoren verlegt wurden (zurückzuführen auf die Hangneigung), dar.

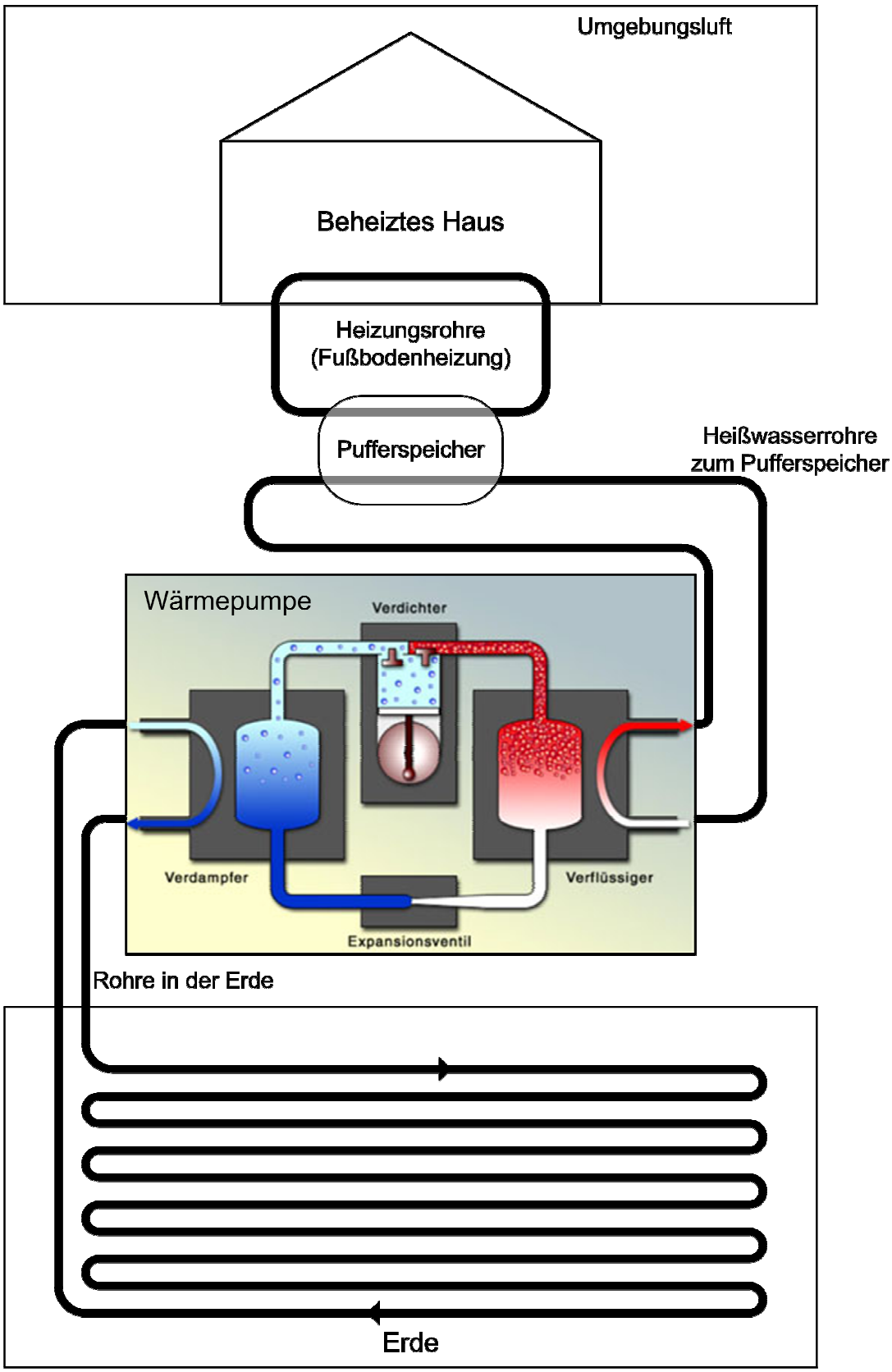
Abschließend sollte die Gruppe sich in einen Konsumenten versetzen und mögliche Lösungsvorschläge erstellen.

1.3 Fehler-Chronologie

- Pumpe fällt aus und zeigt Fehler 37 (=Niederdruck)
- Barometer hinter der Pumpe (vermutlich am Pumpeneingang) zeigt beim Pumpen einen Druckabfall an
- Frage nach einem Loch in einer Leitung
- Führt die unterschiedliche Leitungslänge zu einem Druckabfall?

- Luft in der Leitung?
- Leitung wurde mit Hochdruck durchgespült
- Druckverlust von 0,5 Bar in der folgenden Nacht (normalerweise stehen die Leitungen unter einem Druck von 1,5 Bar)
- Bei Abschaltung des fehlerhaften Kollektorkreises: kein Druckabfall mehr;
  Vermutung eines Lecks im Rohr liegt nahe
- Keine Druckschwankungen mehr am Barometer; Pumpe zeigt trotzdem noch Fehler 37

II. Funktionsweise einer Erdwärmeheizung



Innerhalb der Erdwärmekollektoren, die in einer Tiefe von 1,20m verlegt sind, zirkuliert unter einem Druck von 1,5 Bar entweder eine Wasser-Frostschutzmittel-Gemisch oder eine Sole-Lösung, die Wärmeenergie von der Erde aufnimmt, und so von -3°C auf ca. 0 bis 1°C erwärmt wird. (Die Temperaturdifferenz liegt je nach Wärmepumpe ungefähr bei 4°C)

In der Wärmepumpe gibt die Flüssigkeit aus den Kollektorkreisen die Energie über Heizspiralen an eine andere Flüssigkeit mit extrem niedrigem Siedepunkt ab, welche dann verdampft.

Durch einen Verdichter wird das Gas komprimiert, wodurch die Temperatur auf über 70°C ansteigt. Auf der anderen Seite des Wärmepumpenkreislaufes wird über weitere Heizspiralen die Energie wieder entzogen, und an den Pufferspeicher abgegeben. Dieser speist die Heizung und Warmwasserversorgung des Wohnhauses.

III. Lösungsansätze und Fehlertheorien

3.1 Loch in der Leitung

Eine erste und naheliegende Theorie war es, dass ein Loch in der Leitung existiert, welches für die abnormale Druckänderung verantwortlich scheint. Grund für das Entstehen des Loches könnten Baumängel sein, denn die Rohre wurden nicht wie üblich in einem Sandbett verlegt. Die Loch-Theorie wurde auch von Stephen bestätigt. Er teilte uns jedoch mit den (laut seinen eigenen Messungen) fehlerhaften Kreis bereits ausgeschalten zu haben.

3.2 Die Frage nach Kalkablagerungen

Wegen dem Druckabfall musste Stephen immer wieder über einen eigenen Anschluss an der Leitung frisches Wasser nachfüllen. Weil es sich dabei nicht um destilliertes, sondern um normales Leitungswasser handelte, kam die Theorie der Verkalkung wegen „verunreinigtem" Wasser auf. Jedoch mussten wir die Theorie bald wieder verwerfen, da die Simulation aufgrund der komplizierten Berechnung der turbulenten Strömung zu aufwändig gewesen wäre und unser Zeitkontingent gesprengt hätte.

3.3 Kommt es wirklich auf die Länge an?

Normalerweise werden die Kollektoren für Erdwärmeheizungen immer mit derselben Länge verlegt. Bei Stephen war dies aber nicht der Fall. Ursprünglich wurde nur eine 550 m lange Leitung verlegt. Da der Widerstand aber so hoch war, entschloss sich die Baufirma später diese lange Leitung in drei unterschiedlich lange Kollektoren zu zerteilen.

Mithilfe des Gesetzes von Poiseuille können wir sagen:

$$W(L) = \frac{8\eta L}{\pi R^4}.$$

Daraus können wir ablesen, dass der Widerstand von der Länge der Leitung direkt, und der Größe der Querschnittsfläche indirekt proportional abhängig ist.

3.4 Die Anzahl der Rohre

Die nächste Überlegung beschäftigt sich mit der Anzahl der Rohre und deren Abhängigkeit vom Widerstand.

Für parallel geschaltete Widerstände gilt das Kirchhoff'sche Stromgesetz:

$$\sum F_z = \sum F_A$$

Also: $\frac{1}{W_{Ges}} = \frac{1}{W_1} + \frac{1}{W_2} + ... + \frac{1}{W_n}$

Fluss . . . Stromstärke Ohmsches Gesetz: $W = \frac{U}{I}$

Druck . . . Spannung

$I_{ges} = I_1 + ... + I_n$

Also: $\frac{\Delta U}{R_{Ges}} = \frac{\Delta U}{R_1} + ... + \frac{\Delta U}{R_n}$

Analogie:

$\Delta p = F \cdot W = F_1 \cdot W_1 + ... + F_n \cdot W_n$

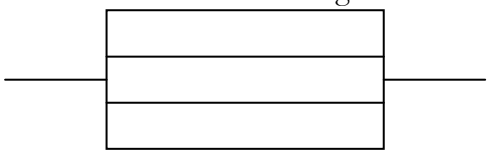
Nach Poiseuille gilt folgende Formel für Widerstände:

$W = \frac{8\eta L}{\pi R^4}$ . . . $\eta =$ Viskosität

$F = \frac{\Delta p}{W} \Rightarrow F = \frac{\Delta p \pi R^4}{8\eta L}$ gilt für laminare Strömungen

Parallel geschaltete Widerstände, wobei $w_1 = w_2 = ... = w_n$

Parallelschaltung



Serienschaltung

$W = w_1 + ... + w_n$

l …	Länge der einzelnen Widerstände
f …	Fluss durch einen einzelnen Widerstand
F …	Gesamtfluss durch die Parallelschaltung
w …	Einzelwiderstand
n …	Anzahl der Widerstände in Parallelschaltung
W_n …	Gesamtwiderstand in der Parallelschaltung
W …	Gesamtwiderstand der Serienschaltung bei gleicher Ohmzahl der Einzelwiderstände

Es gilt: $l = \frac{L}{n}$, $w = \frac{W}{n}$

Laut Kirchhoff:

$$F = f_1 + f_2 + ... + f_n = n \cdot f$$

$$W_n^{-1}\Delta p = w_1^{-1}\Delta p \cdot ... \cdot w_N \Delta p$$

$$\frac{1}{W_n} = \frac{1}{w_1} + ... + \frac{1}{w_N} = \frac{1}{\frac{W}{n}} + ... + \frac{1}{\frac{W}{n}} = \frac{n}{W} + .. + \frac{n}{W} = \frac{n^2}{W}$$

$$\Rightarrow W_n = \frac{W}{n^2}$$

In Worten: Der Gesamtwiderstand in einer Parallelschaltung ist gleich dem Gesamtwiderstand in einer Serienschaltung (gleiche Länge) durch die Anzahl der Leiter in der Parallelschaltung zum Quadrat.

Beispiele:

- 6 parallel geschaltete Leiter (Widerstände): 1Widerstand hat 100 Ohm

$$W_6 = \frac{W}{36} = \frac{600}{36} = \frac{50}{3}$$

- 3 parallel geschaltete Leiter:

$$W_3 = \frac{W}{9}$$

Parallel geschaltete Widerstände (Leitungen) mit unterschiedlichen Längen:

Annahme: $w_1 = 300\Omega \quad w_2 = 200\Omega \quad w_3 = 100\Omega$

Bei keiner Regulation gilt:

$$\frac{1}{W_{ges}} = \frac{1}{300} + \frac{1}{200} + \frac{1}{100} = \frac{11}{600} \Rightarrow W_{ges} = \frac{600}{11} \approx 54{,}54$$

Regulation:

Ziel: Widerstände in den kürzeren Röhren müssen vergrößert werden, damit die Entleerungszeit[1] in allen drei Rohren gleich ist (d.h. der Fluss muss in allen 3 Rohren unterschiedlich sein, da sie unterschiedliche Längen besitzen → die Wasserstrahlen müssen zum gleichen Zeitpunkt am Endpunkt ankommen). Folglich ist in allen Röhren eine gleich hohe Temperatur zu messen, ob jedes Teilchen die gleiche Durchlaufzeit hat. Dies ist deswegen erforderlich, da sonst eine ungleiche Energiegewinnung zu verzeichnen wäre.

v_A

v_B $\qquad v_A < v_B < v_C$

v_C

Der Gesamtwiderstand wird vergrößert (Bewies: siehe unten) indem ein so genannter Taco-Setter (hydraulisches Regulierventil) installiert wird. Dieses Gerät verringert die Querschnittsfläche für einen kurzen Rohrabschnitt (d.h. der Radius *R* wird kleiner).

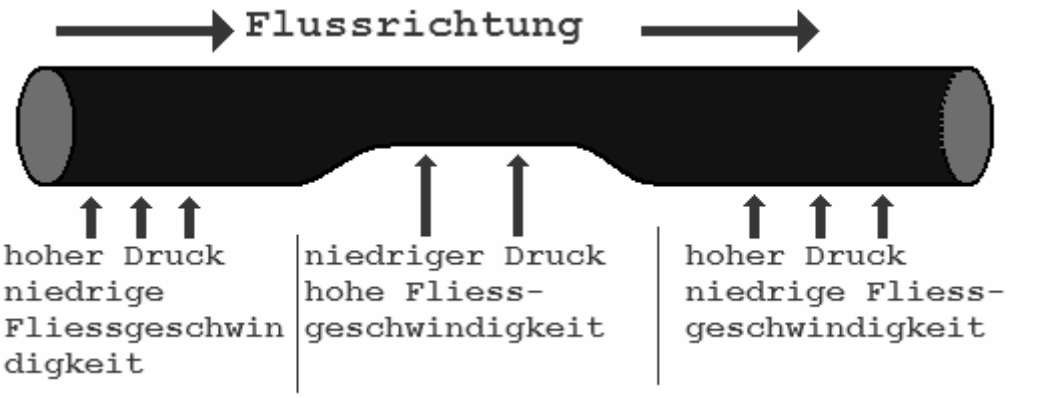


Abb. Schema eines Rohres mit einer Engstelle nach Bernoulli

Der Radius im Taco-Setter ist kleiner als im restlichen Rohr. Dadurch ist nach Bernoulli im Taco-Setter der Druck kleiner, weshalb der Gesamtwiderstand des Rohres steigt. Dabei gilt folgendes:

$W = \frac{8\eta l}{\pi R^4}$ Der Gesamtfluss F wird kleiner, da folgende Beziehung gilt: $F = \frac{\Delta p}{W}$

Der Taco-Setter ist aber nicht als Lösung des Problems geeignet, da die Widerstände sehr stark vergrößert werden, was eine zusätzliche Belastung für die Pumpe bedeutet.

Es gilt nämlich $F = v \cdot A = \frac{s \cdot A}{t} = \frac{\Delta p}{W}$. Da $\frac{\Delta p \cdot t}{A} = konst.$ gilt $W = \frac{c}{s}$.

[1] Entleerungszeit ist die Zeit, die ein Wassermolekül benötigt, um vom Beginn bis zum Ende eines Rohres zu kommen.

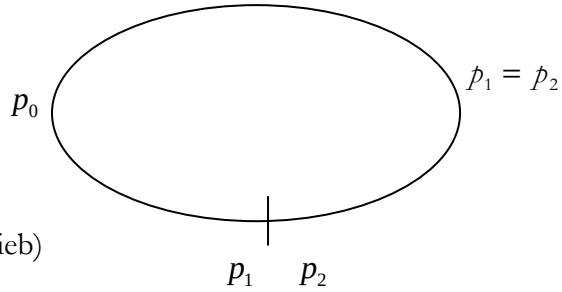
3.5 Problem des Druckabfalls

Problem: Fehleranzeige 37 → Niederdruck im System.

Alle Kollektoren sind offen; der Blick auf ein Barometer zeigt während des Pumpens einen Druckfall an.

Vermutung: das Barometer ist am Ende des Kreislaufes angebracht.

1. Fall Pumpe arbeitet nicht:



p_1 . . . Anfangsdruck

p_0 . . . Statischer Druck (Pumpe nicht in Betrieb)

p_2 . . . Bei Wärmepumpe ankommender Druck

Nach Bernoulli gilt:

Gesamtdruck = Statischer Druck + Hydrodynamischer Druck

$$p_{ges} = p_0 + \frac{\rho}{2} v^2 = const.$$

Da die Pumpe nicht in Betrieb ist, gibt es keinen hydrodynamischen Druck, also gilt:

$$p_{ges} = p_0$$

2.Fall Pumpe arbeitet, kürzester Kollektor geschlossen → kein Druckabfall ($p_0 = p_2 < p_1$) … „<“ wegen der Viskosität

3. Fall Pumpe arbeitet, kürzester Kollektor offen → Druckabfall ($p_2 < p_0 < p_1$)

Begründung:

Der Grund für den Druckabfall beim Pumpen liegt in den Luftblasen, die sich in den Leitungen befinden. Durch das Befüllen der Kollektoren konnte die Luft nicht vollständig verdrängt werden, da sie sich aufgrund der Hangneigung in den oberen Schleifen angesammelt hat und von dort mit dem normalen Pumpdruck nicht mehr zu entfernen war. Nachdem jedoch eine stärkere Pumpe an das System angeschlossen worden war, die alle drei Kreise durchgespült hat, war kein Druckabfall mehr zu verzeichnen. Wie unten bewiesen, kann jedoch ein möglichst großer Druckunterschied zwischen Anfang und Ende des Rohres die Luftblasen entfernen.

Wir haben die realen Gegebenheiten stark idealisiert, indem wir uns statt einer Hangneigung von ca. 7° uns die Situation bei einem Rohr das normal auf eine gerade Ebene steht, betrachtet haben. Außerdem sind wir statt der etwas unregelmäßigen Krümmung von exakten Halbkreisen ausgegangen.

p_1 = Druck am Beginn der Krümmung

p_2 = Druck am Ende der Krümmung

Der Gesamtdruck setzt sich aus dem statischen Druck und der Druckdifferenz zwischen p_1 und p_2, in Abhängigkeit von den Längen zusammen. Diese Druckdifferenz wird wegen der Viskosität verursacht.

$p = \rho g h$ . . . statischer Druck

Die Höhe ist auf der y-Achse aufgetragen, Dichte und Erdbeschleunigung (9,81 m/s²) sind konstant.

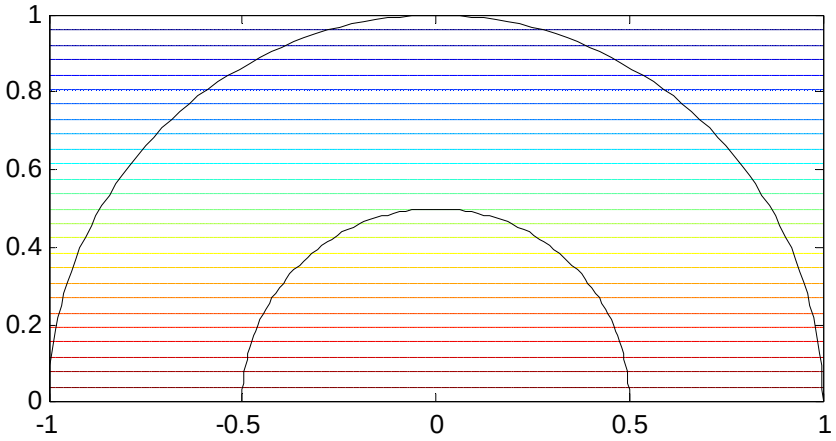
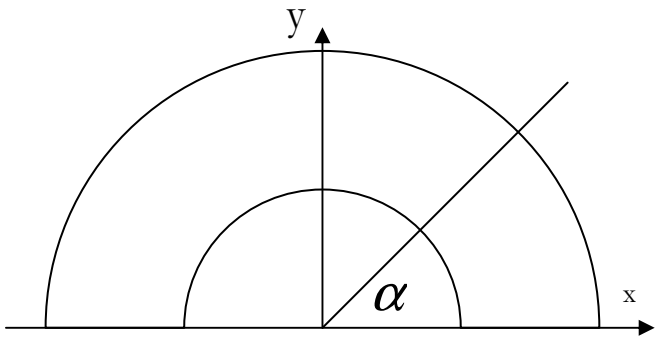


Abb. Druck sinkt mit der Höhe, $p_1 = p_2$ (mit Schwerkraft)

Druckdifferenz Δp bei hydrodynamischem Druck:

Um die Druckverhältnisse wie beim statischen Druck in Abhängigkeit von der Höhe zu beschreiben, haben wir auf eine Winkelfunktion zurückgegriffen.

$$\tan\alpha = \frac{y}{x}$$



Bei einem geraden Rohr gilt wegen der Viskosität: $p = \frac{l}{L}(p_2 - p_1) + p_1$

Die Länge l des Rohres beschreibt in diesem Fall einen Kreisbogen für p (Druck an irgendeiner Stelle im System). Daher gilt:

$l = \frac{\pi r \alpha}{180}$, $L = r\pi$ (ganzer Halbkreisbogen)

$$\Rightarrow p = \frac{\alpha}{180}(p_2 - p_1) + p_1$$

Oder $$\frac{\tan^{-1}\left(\frac{y}{x}\right)}{180}(p_2 - p_1) + p_1$$

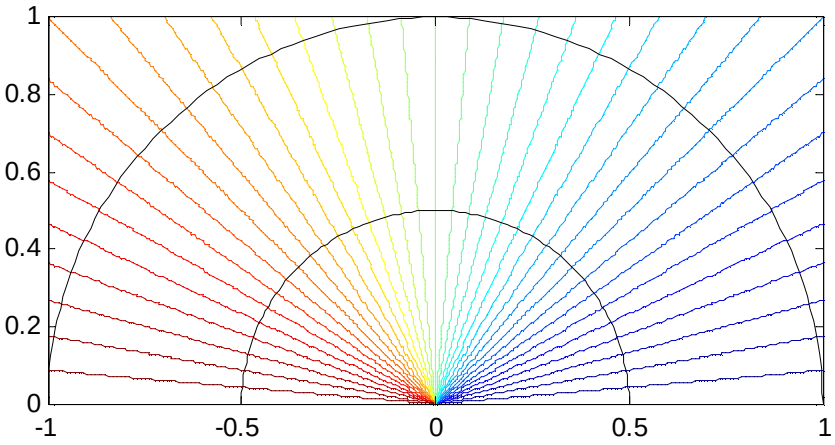


Abb. Ohne Schwerkraft, $p_1 > p_2$ (wegen Viskosität)

Wenn man die beiden Drucke addiert $p(y) + p\left(\tan^{-1}\left(\frac{y}{x}\right)\right)$, erhält man die Drucksituation im „realen" Rohr. Eine mögliche Luftblase hätte ihre Oberfläche bei einer dieser Linien gleichen Druckes (dieselbe Linie), da der Druck bei Gasen gleichmäßig verteilt wird.

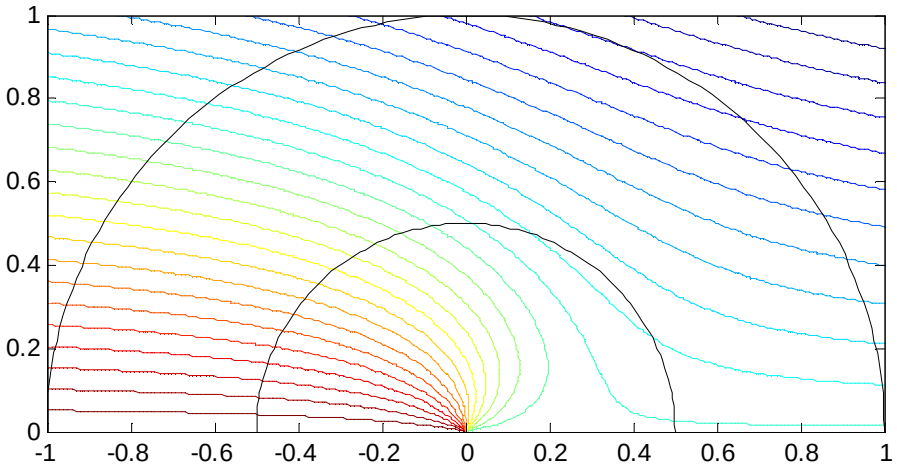


Abb. Niveaukurve; beide Systeme wurden addiert

Wenn Δp groß genug ist, wird daher aufgrund der Druckverhältnisse im Rohr weitergespült.

Ad Abb.: Je dichter die Linien, desto höher die Druckveränderung.

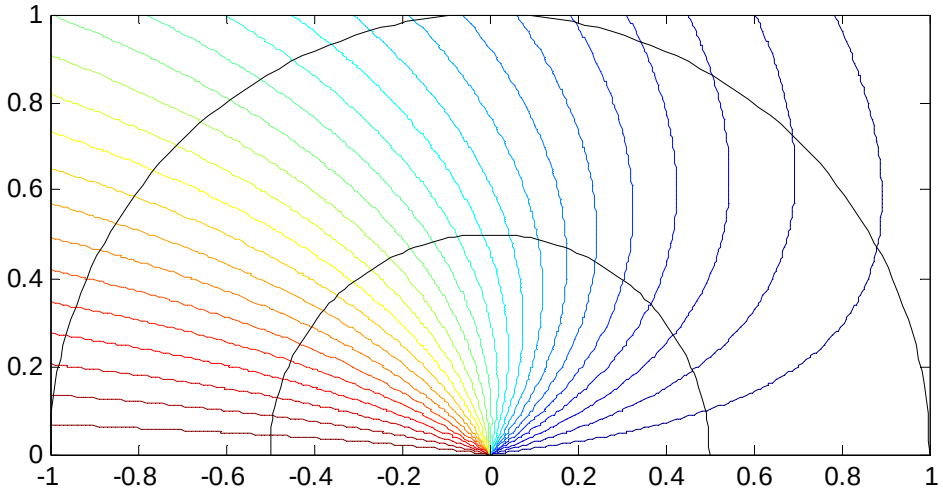
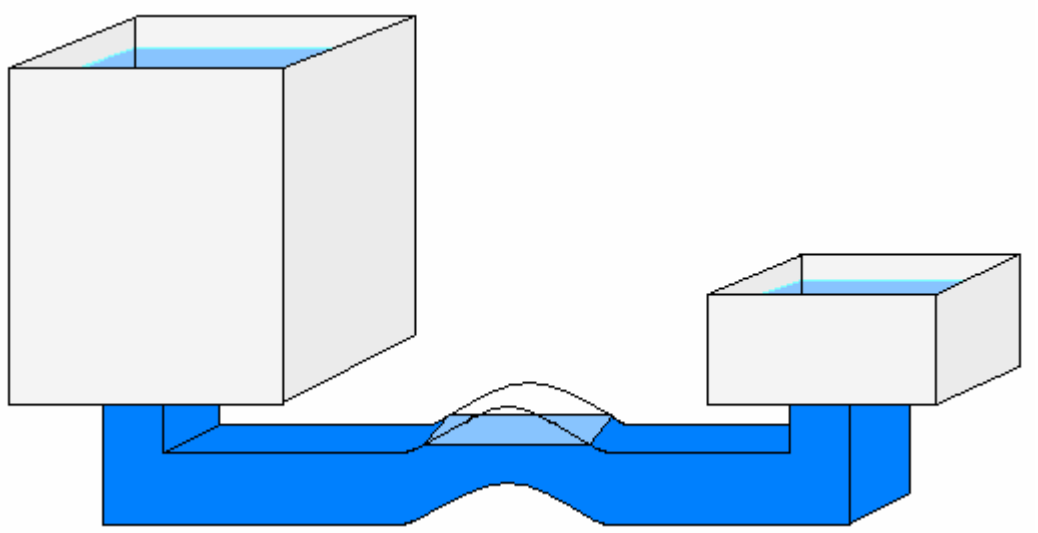


Abb. Δp ist groß genug; die Blase wird durchgespült.

Ursache des Druckverlustes beim Pumpen:

Vereinfachtes Beispiel:



Links befindet sich ein Gefäß mit größerer Höhe (daher herrscht hier ein größerer Druck) als im linken Gefäß. In einer kleinen Erhebung im Rohr befindet sich eine Luftblase. Wegen des ungleichen Drucks zwischen den Gefäßen, müssten sich die Wasserspiegel in beiden Behältern angleichen. Nach dem Öffnen einer „Klappe“ im größeren Gefäß, fließt das Wasser in den kleinern Behältern, sodass dieser übergeht. In diesem theoretischen Experiment steht jedoch eine Person mit einem Kübel neben dem kleineren Behälter, und transportiert ohne Berücksichtigung der Raum- und Zeitgesetze die überfließende Wassermenge zurück in den höheren Behälter, damit der Wasserspiegel dort konstant bleibt.

Durch das Öffnen der Klappe steigt der Druck in der Röhre an. Folglich wird der Luftpolster in der Biegung zusammengedrückt. Aufgrund der Volumsverkleinerung, wird zusätzlicher „Raum“ frei, und da vorausgesetzt ist, dass der Wasserspiegel im großen Behälter gleich bleibt, sinkt der Spiegel im kleinen Gefäß.

In unserem System aber kann der Wasserspiegel nicht sinken, weil es ein abgeschlossenes System ist, und somit das Gesamtvolumen konstant bleiben muss. Es kann daher die Luftblase nicht komprimiert werden. Folglich sinkt der Druck p_2 (dies lässt sich mathematisch erklären). Um dies zu veranschaulichen, stelle man sich eine Saugglocke über dem kleineren Behälter vor, der den Wasserspiegel wieder in die ursprüngliche Lage zurückzieht. Dies ist der Grund für die angesprochene Senkung des Drucks beim Pumpen.

Durch das Sinken des Drucks p_2 wird aber auch die Differenz Δp größer, was wegen der Formel $F = \frac{\Delta p}{W}$ zu einer Erhöhung des Flusses führt. Bei zu viel Luft jedoch könnte das Wasser gar nicht fließen.

3.6 Weitere Vermutungen – Denkansätze

Ein weiterer Fehler könnte es sein, dass in der Pumpe keine Verdampfung stattfinden kann, aufgrund zu niedriger Temperatur der Leitung aus der Erde.

IV. Simulation

Nach der rechnerischen Auswertung, ist vor allem die Simulation am Computer von großer Bedeutung. Die nötigen Gleichungen wurden zuerst von uns in Matrizen umgewandelt, um dem verwendete Simulationsprogramm das Rechnen damit zu ermöglichen.

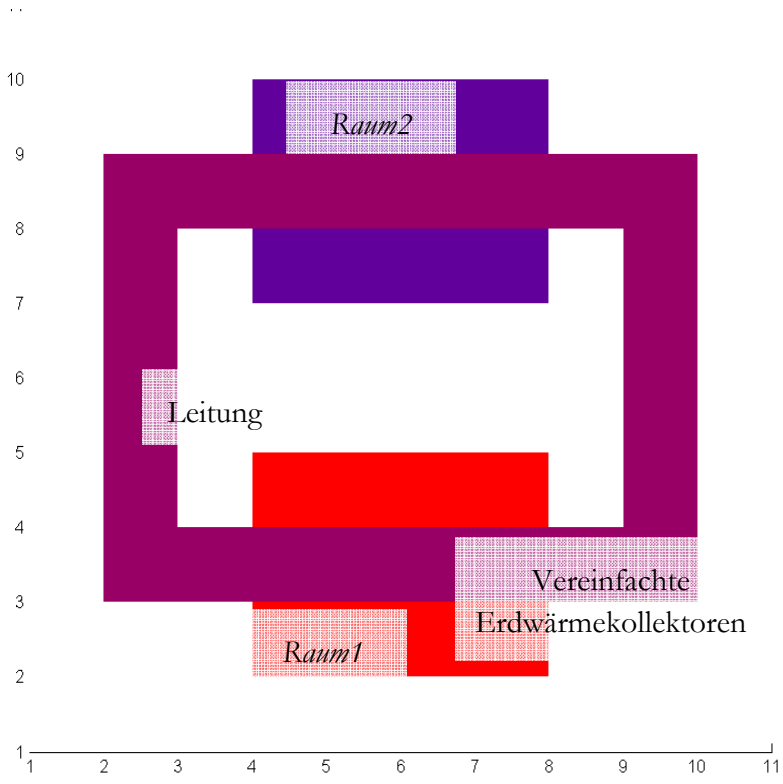
4.1 Erste Versuche mit einem „einfachen Modell“

Zur Simulation verwenden wir das Programm Matlab (Version 7.3.0), das es uns ermöglicht die Matrizen zu errechnen. Unsere Differentialgleichung besteht aus der Matrix *A* (siehe unten) und einer zweiten Matrix *b*. Dieses einfache Gleichungssystem ermöglicht es uns mit beliebigen Werten die Matrix immer wieder neu zu berechnen. Hier ein Auszug aus dem Programmcode des vereinfachten Modells:

```
A = [-h2*sigma2/(rho1*c1*v1),h2*sigma2/(rho1*c1*v1),0,0; ...
    h2*sigma2/(rho2*c2*v2),-h2*sigma2/(rho2*c2*v2)-a/v2,a/v2,0;...
    0, a/v3,-h3*sigma3/(rho3*c3*v3)-a/v3,h3*sigma3/(rho3*c3*v3);...
    0,0,h3*sigma3/(rho4*c4*v4),-h3*sigma3/(rho4*c4*v4)];
```

Bei diesem Modell handelt es sich um unsere ersten „Gehversuche“ mit dem für uns neuen Programm, bei dem wir eine einfache Art der Wärmeübertragung zwischen zwei Räumen über eine Leitung simulieren.

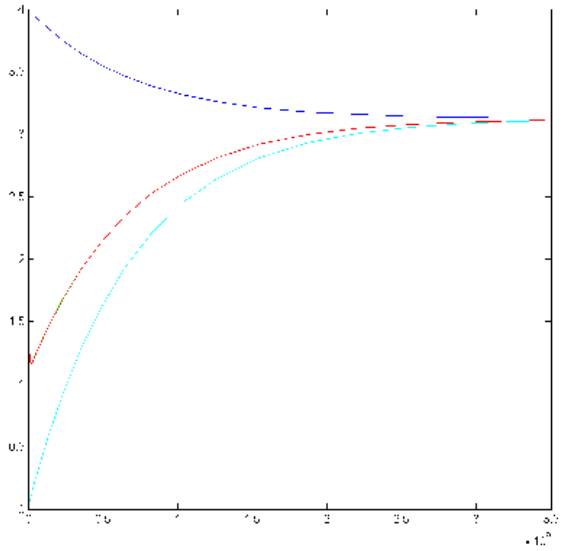
Der untere Bereich in der Grafik (*Raum1*) stellt sehr vereinfacht die Erde dar, der obere Raum soll im Laufe der Arbeiten durch das Haus ersetzt werden. Nachdem wir die Simulation durchlaufen ließen, hat sich *Raum2* schon erwärmt: Die ersten Versuche mit Matlab waren geglückt.



Den genauen Temperaturverlauf kann man aus der Temperaturkurve auf der rechten Seite ablesen.

Die rote Kurve stellt die Temperatur der Leitung (Kollektoren in der Erde) dar, Blau den Temperaturverlauf in der Erde und von der cyanfarbige Kurve kann man den Temperaturverlauf innerhalb des Hauses (*Raum2*) ablesen.

Dass uns dieses einfache Modell schon bald nicht mehr weiterhilft, erkannten wir als es darum ging, die Kompression des Gases innerhalb der Wärmepumpe darzustellen



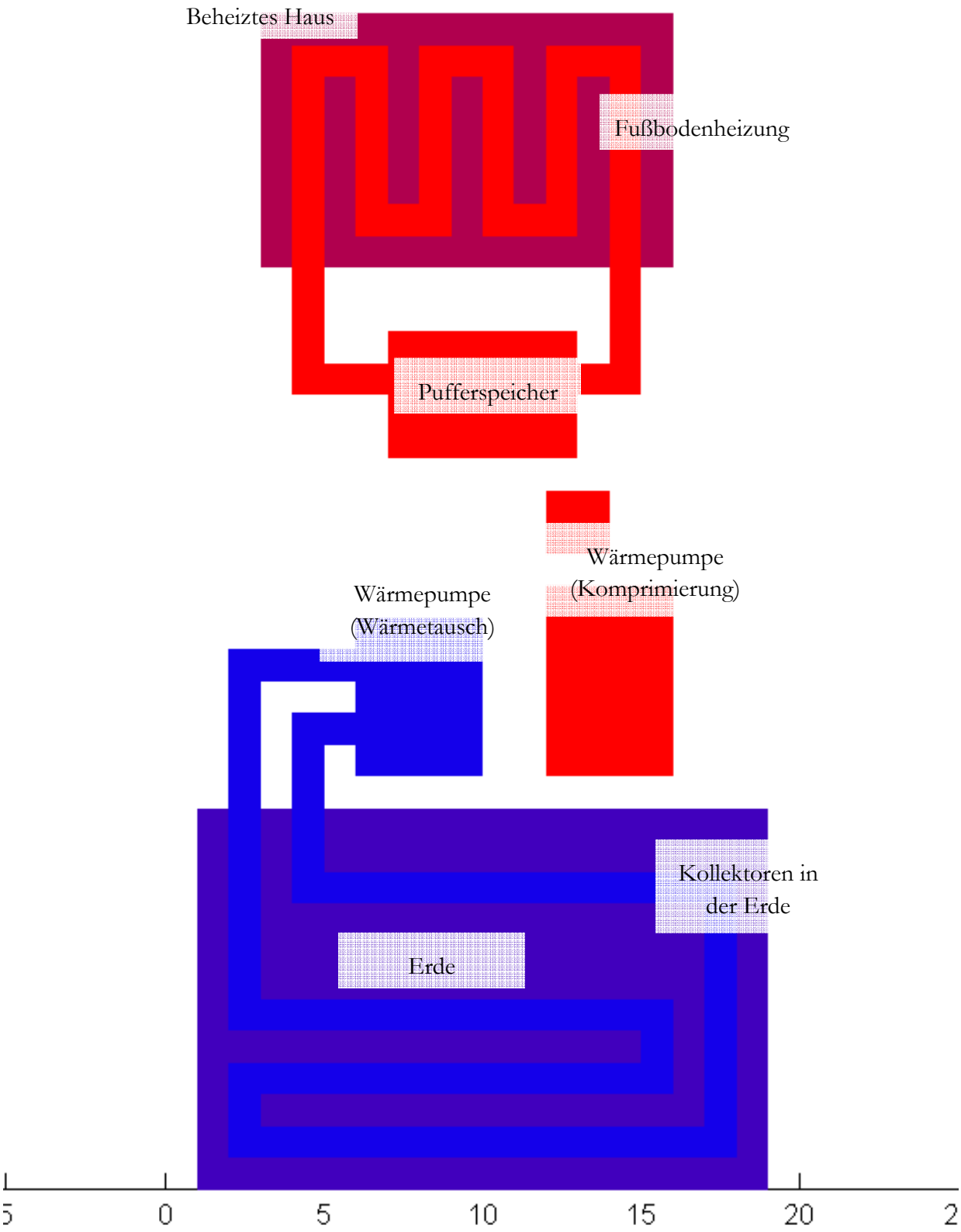
4.2 Komplexeres Modell

Im Laufe der Woche wuchs unser Gleichungssystem auf eine stattliche Größe an. Mit diesem war es uns dann möglich die Wärmepumpe, mitsamt der Gaszirkulation in ihr, wiederzugeben. Folgende Formeln haben wir errechnet:

$$\rho_1 c_1 v_1 T_1' = h_1 \sigma_1 (T_2 - T_1)$$
$$\rho_2 c_2 v_2 T_2' = h_1 \sigma_1 (T_1 - T_2) + \rho_2 c_2 a_1 (T_3 - T_2)$$
$$\rho_3 c_3 v_3 T_3' = h_2 \sigma_2 (T_p - T_3) + \rho_3 c_3 a_1 (T_2 - T_3)$$
$$\rho_4 c_4 v_4 \left(\frac{v_5}{v_4}\right)^{K-1} T_4' = h_2 \sigma_2 (T_3 - T_p) \rho_4 c_4 v_4 \left(\frac{v_5}{v_4}\right)^{K-1} T_4' = h_2 \sigma_2 (T_3 - T_p)$$
$$\rho_5 c_5 v_5 T_5' = h_3 \sigma_3 (T_4 - T_5) + h_4 \sigma_4 (T_6 - T_5)$$
$$\rho_6 c_6 v_6 T_6' = h_4 \sigma_4 (T_5 - T_6) + \rho_6 c_6 a_2 (T_7 - T_6)$$
$$\rho_7 c_7 v_7 T_7' = h_5 \sigma_5 (T_8 - T_7) + \rho_7 c_7 a_2 (T_6 - T_7)$$
$$\rho_8 c_8 v_8 T_8' = h_5 \sigma_5 (T_7 - T_8) + h_6 \sigma_6 (T_a - T_8)$$

Die schon im einfachen Modell können wir auch hier die Änderungen der Energie über längere Zeiträume beobachten, und haben, damit sich das Haus nicht bis ins unermessliche erhitzt und sich die Erde regenerieren kann, einen einfaches Thermostat eingebaut:

```
if(T(8,1)>(20))
    a1=0;
    a2=0;
end
```



Hier ist das komplexe Modell am Ende der Simulation zu sehen.

V. Fehlerbehebung – Empfehlungen

5.1 Empfohlene Lösung

Bei der „Taco-Setter-Lösung“ ist die Belastung für die Pumpe sehr hoch (hoher Gesamtwiderstand), deshalb empfehlen wir, die alten Leitungen zu entfernen und, wie ursprünglich geplant, sechs Leitungen zu je 100m zu verlegen. (siehe Konzeptzeichnung unten)