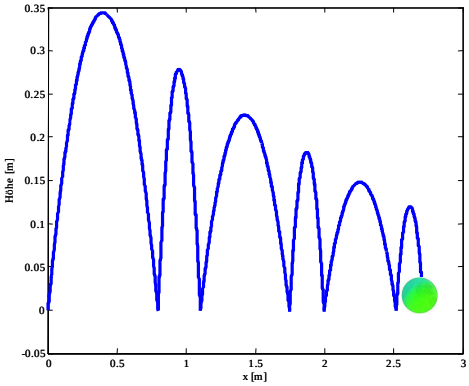
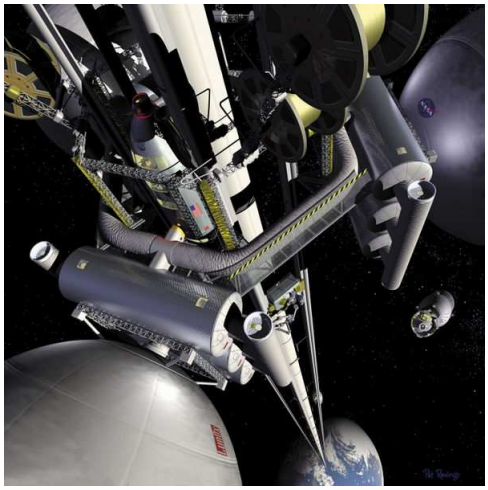
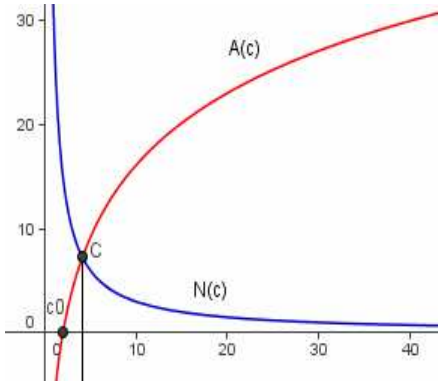
MATHEMATIK-MODELLIERUNGSWOCHE

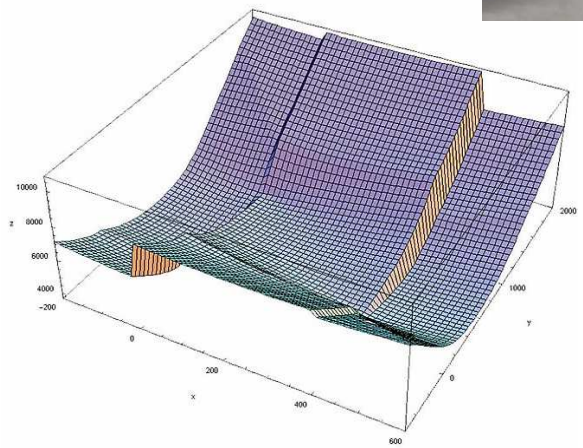
KURZBERICHT

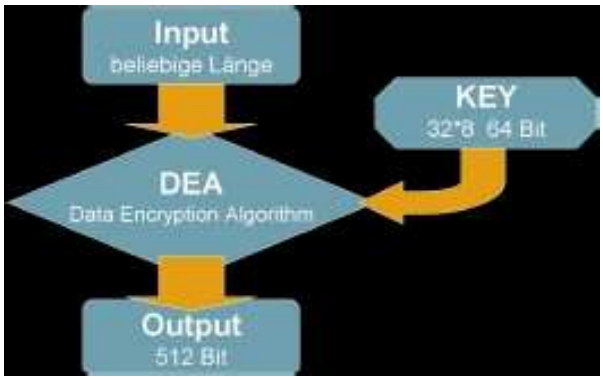
13. – 19. Jänner 2008











Das Land Steiermark

Bank Austria Creditanstalt

UNI GRAZ

MATHEMATIK

Mathematik-Modellierungswoche

Schloss Seggau, 13.01. – 19.01.2008

Ausführliche Dokumentation der einzelnen Projekte:
http://math.uni-graz.at/modellwoche/2008/

Das Land Steiermark

Bank Austria Creditanstalt

UNI GRAZ MATHEMATIK

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 Schülern und Schülerinnen großen Anklang gefunden hat. Ermutigt durch diesen durchschlagenden Erfolg haben wir seither jedes Jahr wieder eine Modellierungswoche angeboten. Hauptziel der Modellierungswoche ist es, Schüler und Schülerinnen 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 Schülern und 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 ist Dr. Stephen Keeling, dem hier für seinen großen Einsatz gedankt sei. Besonderer Dank gebührt dem Landesschulrat für Steiermark, und hier insbesondere Frau Landesschulinspektorin 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. Günter Lettl, Dr. Stephen Keeling, Dr. Peter Schöpf und Dr. Bernd Thaller – 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. Wir danken der Abteilung für Wissenschaft und Forschung der Landesregierung Steiermark und der Bank Austria – Creditanstalt für ihre Subvention.

Wir danken Frau Landesschulinspektorin Hofrat Mag. Marlies Liebscher und Herrn Präsident Wolfgang Erlitz vom Landesschulrat für Steiermark und Vizerektor Martin Polaschek und Dekan Karl Crailsheim von der Universität Graz für die finanzielle Unterstützung.

Schloss Seggau, am 19. 1. 2008

F. Kappel

(Leiter des Institutes für Mathematik und Wissenschaftliches Rechnen)

Projekt Sportwissenschaften

Reflexion von Bällen

Prof. Sigrid Thaller

Teilnehmer: Lisa Dittmer, Tanja Koch, Johann Körner, Michael Lasnik, Alexander Leitner, Patrick Reicher

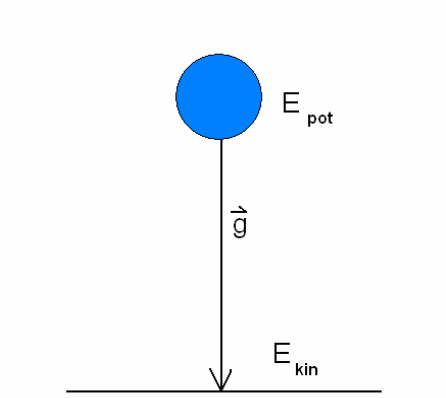
PROBLEMSTELLUNG:

In diesem Projekt soll das Reflexionsverhalten von Bällen unterschiedlichster Art untersucht werden. Wie hängt der Reflexionswinkel von der Rotation, der Elastizität oder der Geschwindigkeit des Balles ab? Gibt es noch weitere Einflussgrößen? Was passiert, wenn man einen rotierenden Hartgummiball in eine Ecke wirft?

ERGEBNISSE:

Stellen wir uns vor, wir sitzen auf einem Baum und lassen von dort einen Gummiball fallen. Wir beobachten dabei, dass der Ball immer schneller fällt bis er am Boden aufkommt. Aus physikalischer Sicht bezeichnet man dies als „Freien Fall“ (wobei wir hier den Luftwiderstand vernachlässigen). Der freie Fall ist eine gleichförmig beschleunigte Bewegung, in der ausschließlich die Fallbeschleunigung wirksam wird.

Welchen Kräften ist der Ball ausgesetzt?
Bevor wir den Ball loslassen, besitzt der Ball eine bestimmte **potentielle Energie**. Während des Falles wird diese potentielle Energie in kinetische Energie umgewandelt. **Kinetische Energie** ist jene Bewegungsenergie, die in der bewegten Masse eines Körpers enthalten ist.

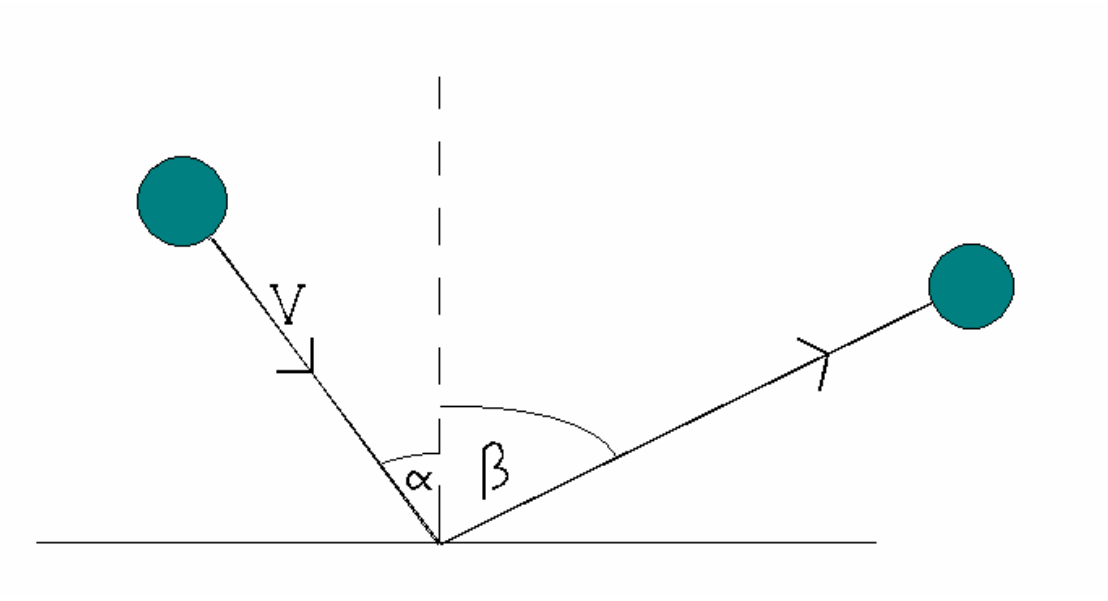


Während unseres Projektes entwickelten wir 3 mathematische Modelle, welche die Reflexion eines Balles am Boden oder an einer Wand beschreiben. In einer Woche der Modellierung ist es nicht möglich alle Einflussgrößen und Faktoren, welche das Verhalten des Balles beeinflussen, in ein Modell aufzunehmen. Daher trafen wir eine bestimmte Auswahl von Faktoren, um die Modelle zu veranschaulichen.

Gleitender und Rollender Ball

In unseren ersten zwei Modellen sind wir darauf eingegangen, wie sich ein Ball verhält, wenn er auf dem Boden aufkommt.

In unserem ersten Modell, anhand eines Cricketballes, nahmen wir an, dass der Ball bei Kontakt mit dem Boden gleitet oder besser gesagt durchrutscht. Mit Hilfe der bereits vorgegeben Formeln der Impulsänderung beim Stoß, der Drehimpulsänderung und der Formel des unelastischen Stoßes konnten wir durch Umformen die Bedingungen eines jeden Balles nach dem Aufprall auf dem Boden darstellen. Somit konnten wir aufgrund des Eintrittswinkels den Austrittswinkel und die Rotationsgeschwindigkeit des Balles vorhersagen.



Aus diesen Versuchen konnten wir einige Schlüsse ziehen:

Der Elastizitätskoeffizient *e*, der die Rückspringhöhe bestimmt, und der Reibungskoeffizient μ spielen eine wichtige Rolle, in welchem Winkel der Ball nach Kontakt mit dem Boden abspringt.

Die Drehung des Balles nach dem Aufprall hängt entscheidend von der Reibung zwischen Ball und Boden ab.

Die Rotation spielt keine Rolle, weil die Reibung unabhängig von der Geschwindigkeit ist.

Wenn ein Ball aber bestimmte Bedingungen erfüllt, gleitet er nicht nur, sondern beginnt auch zu rollen. Somit ergibt sich eine neue Formel, die wir durch weiteres Umformen erhalten haben. Durch Veränderung der Bedingungen nahm der Ball verschiedene Flugbahnen an, welche wir berechneten und versucht haben nachzustellen.

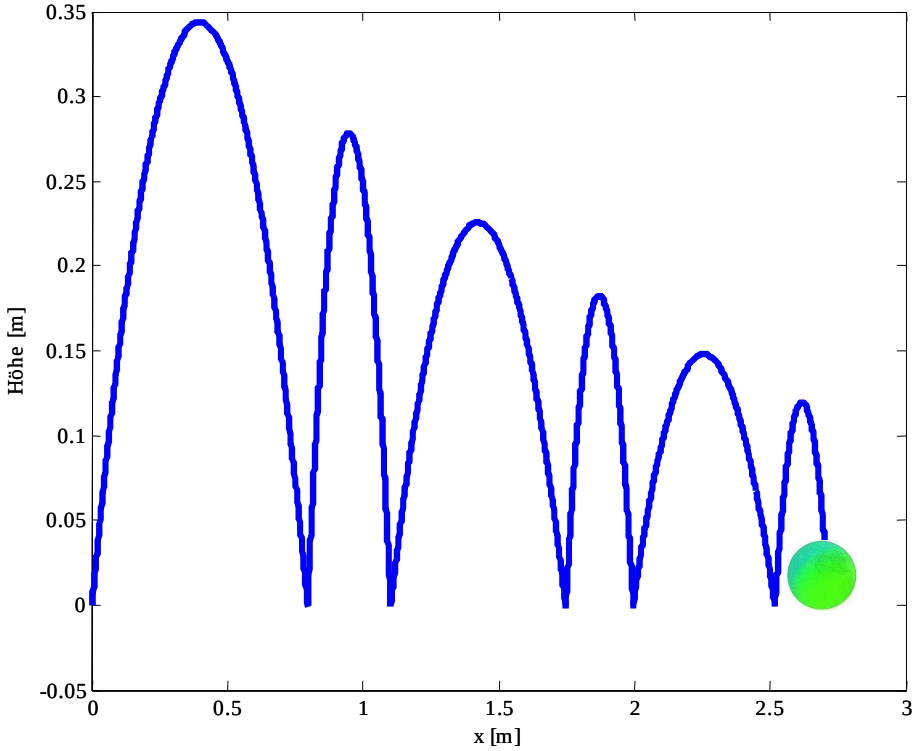
Reflexion von Gummibällen

Um Hartgummibälle zu beschreiben wurde weiteres Modell aufgestellt, das davon ausgeht, dass bei der Reflexion Energie und Impuls erhalten bleiben.

Im Laufe unserer Arbeiten wurde auch fleißig praktisch experimentiert. Nachdem

mathematische Modelle von der Reflexion von Bällen erstellt wurden, mussten diese natürlich auch mit konkreten Daten überprüft werden. Die Experimente stimmten mit den Berechnungen überein und wir konnten spezielle Bewegungen voraussagen.
Danach wurde ein Programm, anhand dieses Modells, erstellt, das das Verhalten eines Balles in verschiedenen Situationen beschreibt und veranschaulicht.

Doch je länger der Bewegungsablauf war, desto ungenauer wurde die Voraussage der Bewegung. Darum musste man einen Koeffizienten finden, der dieses Problem löst, indem Energieverluste berücksichtigt.



Mit der Verwendung des oben bereits erwähnten Elastizitätskoeffziententen konnten noch genauere Ergebnisse erreicht werden und wir konnten nun die Bewegung des Balles bis zum Stillstand verfolgen.
Die Experimente wurden auch auf Video aufgenommen, um Drehung und Flugbahn von Bällen auch in Zeitlupe untersuchen zu können. Vor allem der Drehsinn der Bälle war schwer mit freiem Auge zu erkennen, daher war die Videoanalyse von großem Vorteil.
Die mathematische Auswertung erfolgte mit MATLAB, ein Mathematikprogramm, in dem einem das Rechnen mit Matrizen sehr einfach gemacht wird.

Das Land Steiermark
Bank Austria Creditanstalt
UNI GRAZ
MATHEMATIK

Projekt: Geometrische Optimierung

Verlegung einer Pipeline mit minimalen Kosten

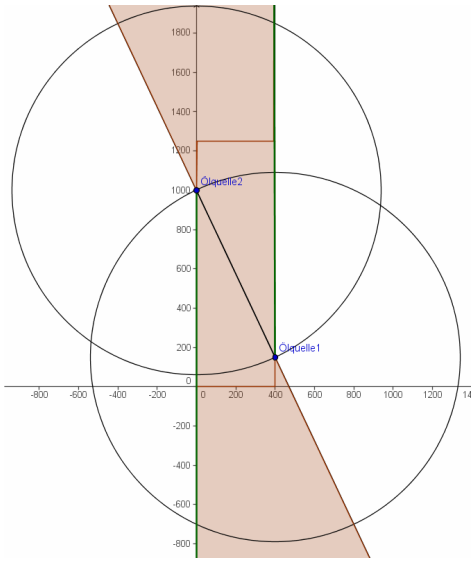
Prof. Peter Schöpf

Teilnehmer: Michael Draxler, Harald Fitzek, Sebastian Hofer, Rudolf Krainer, Lukas Schafzahl

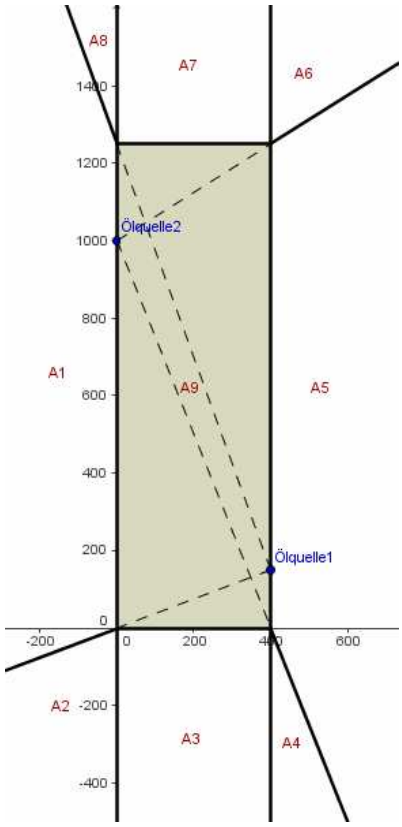
PROBLEMSTELLUNG:

Wir gingen von einer klaren Aufgabenstellung aus: Ein rechteckiger Sumpf mit zwei auf gegenüberliegenden Seiten platzierten Ölquellen A und B ist gegeben, diese Punkte sollen möglichst billig mit einer Pipeline mit nur einem Knick verbunden werden. Dabei ist zu beachten, dass der Rand des Sumpfes zum Trockengebiet zählt. Die Kosten per Meter Pipeline im Trockengebiet sind deutlich geringer als die im Sumpf.

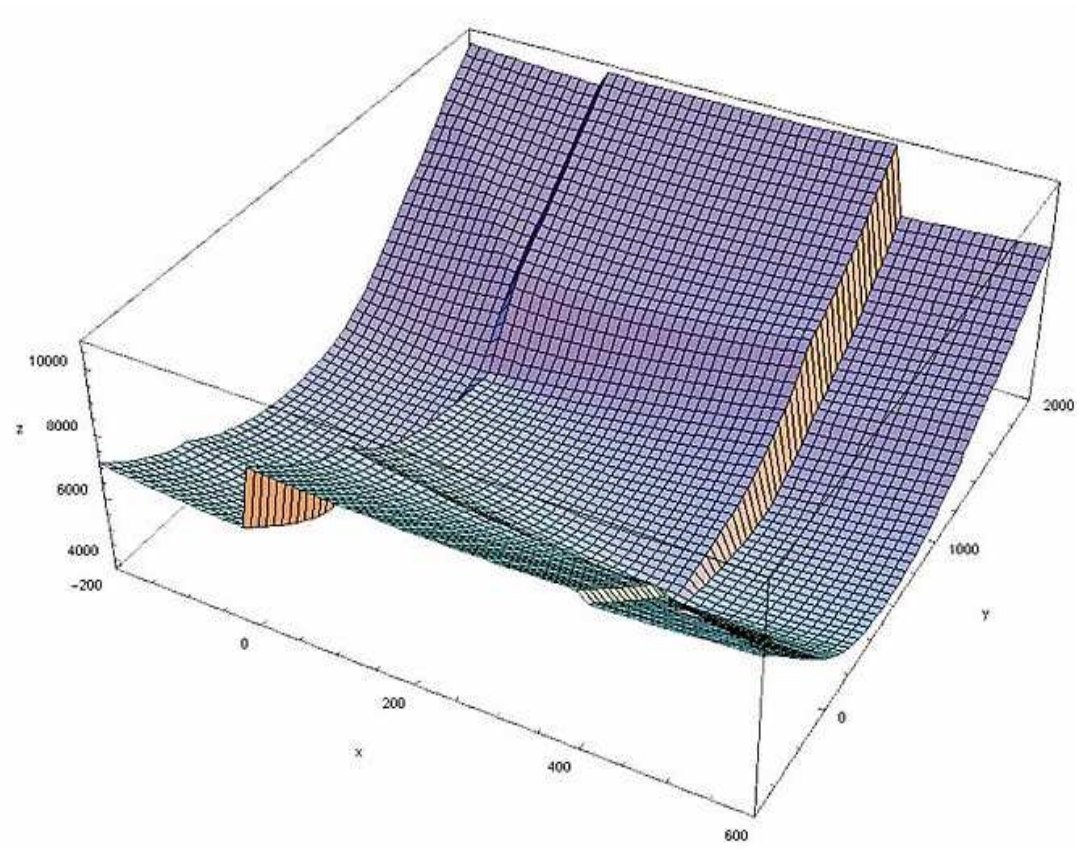
ERGEBNISSE:

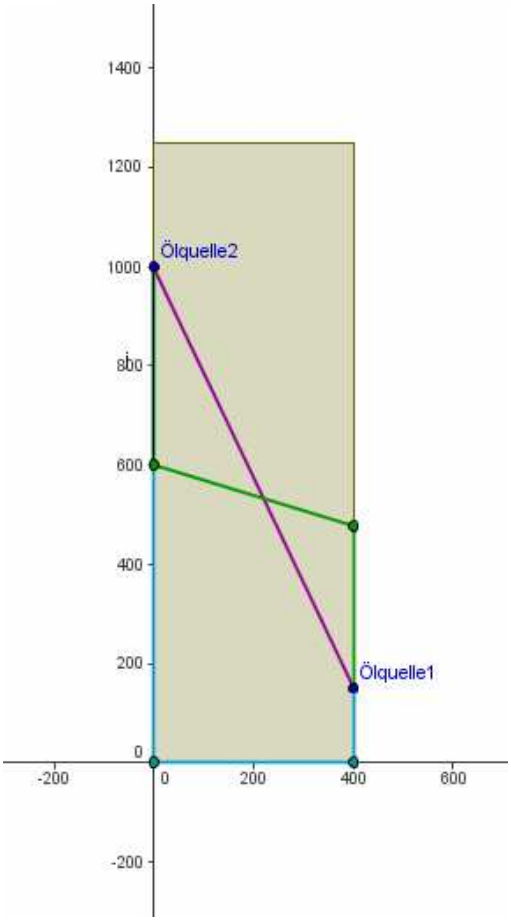


Zuerst versuchten wir, mithilfe logischer Überlegungen möglichst viele Bereiche auszuschließen. Wie in dieser Graphik zu sehen ist, schlossen wir sowohl Knicks in den Richtungen aus, in denen die Strecke im Sumpf länger gewesen wäre als die direkte Verbindung der beiden Punkte durch den Sumpf als auch Knicke im Sumpf, die bestenfalls gleich viel kosten würden wie die direkte Verbindung (gekennzeichnet durch die roten Bereiche). Der Knick kann zudem nur auf der y-Achse und auf der Geraden x=400 liegen, da man sonst einen unnötig langen Weg im Trockengebiet zurücklegen würde. Damit war die Lage des Knicke auf die grün markierten Geraden eingegrenzt.



Daraufhin war es kein Problem mehr, die Lage der optimalen Knicke zu berechnen, und wir versuchten, Formeln für die Kosten der Pipeline bei jedem möglichen Knick aufzustellen. Wir waren überrascht, dass wir neun Formeln benötigten, um jeden Bereich (in der Zeichnung A1-A9) abzudecken. Schließlich gelang es uns, alle Formeln zu finden und erstellten daraus ein dreidimensionales Diagramm, das die Kosten anschaulich darstellt.





Danach stellten wir uns die Frage, ob es möglich ist, mit zwei Knicken eine noch günstigere Lösung zu finden und fanden drei Möglichkeiten, die – abhängig vom Preisverhältnis – die günstigsten sein können. Bei sehr geringen Trockenpreisen ist die blaue, bei extrem hohen Trockenpreisen die lilafarbene Variante die beste. Dazwischen liegt die grüne Möglichkeit, bei der der Winkel vom Preisverhältnis abhängt. Von dieser existieren natürlich unendlich viele Parallele.

Später überlegten wir uns die optimalen Lagen zweier Knicke in einem Trapez und erstellten ein weiteres 3D-Diagramm, wobei wir einige Formeln an die veränderten Bereiche anpassen mussten.

Schlussendlich wollen wir noch beweisen, dass mehr als zwei Knicke zu keiner Verbesserung beim Rechteckssumpf führen.

Projekt: Mechanik - Raumfahrt

Weltraumaufzug

Prof. Bernd Thaller

Teilnehmer: Lukas von Berg, Georg Groß, Gernot Haselmann, Jakob Kleinschuster, Regina Seidl, Robert Triebl

PROBLEMSTELLUNG:

Die Idee, einen Lift ausgehend von einem bestimmten Punkt des Äquators zu einem geostationären Orbit zu konstruieren, stammt ursprünglich von Konstantin Tsiolkovsky. Arthur C. Clarke greift dieses Modell in seinem Roman „The Fountains of Paradise“ auf. Ihm schwebt vor, mit Hilfe dieses Lifts Materialien und sogar Menschen günstiger als mit Stufenraketen ins Weltall zu befördern.

Gleich zu Beginn des Projekts stellten sich für uns sehr viele interessante Fragen, aufgrund der uns zur Verfügung stehenden Zeit konnten wir aber nur auf einige dieser Punkte näher eingehen. Es ist unserer Ansicht nach nicht möglich, wirklich alle Elemente des „Space Elevator“ mathematisch zu modellieren, weshalb wir uns nur mit für uns interessanten und spannenden Teilaspekten auseinandersetzten:

- Was ist eigentlich ein geostationärer Orbit und in welcher Höhe befindet sich ein solcher?
- Angenommen es würde ein derartiger Lift zu diesem Orbit existieren, was würde passieren, wenn ich in einer bestimmten Höhe einfach „aussteigen“ würde? In welcher Bahn würde ich auf die Erde fallen? Treffe ich die Erde immer zwangsläufig?
- Würde das Gewicht des Kabels nicht unsere ganze Station herunterreißen? Wie könnte man diese Kraftwirkung ausgleichen?
- Welche alternativen, bereits heute bestehenden Materialien könnten für die Herstellung des Kabels verwendet werden?
- Wie viel Energie benötigt ein Lift mit einer gewissen Masse m, um diese gigantische Strecke zu überwinden?

ERGEBNISSE:

Ansätze:

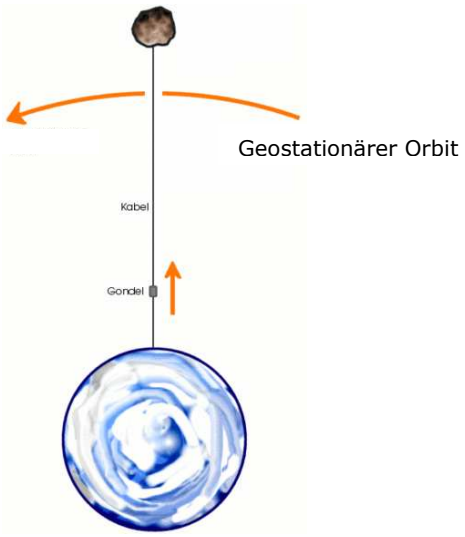
- Ein Satellit befindet sich genau dann in einem geostationären Orbit, wenn seine Umlaufzeit um die Erde genau der Länge eines siderischen Tages entspricht (ca. 23 Stunden, 56 Minuten, 4,09 Sekunden) und wenn seine Umlaufbahn in der Äquatorialebene der Erde liegt. Dadurch befindet sich der Satellit (der Körper) immer am selben Punkt über der Erde. Dies ist eine zwingende Voraussetzung, wenn eine Station im Orbit mit einem Punkt am Äquator der Erde verbunden werden soll. Doch in welcher Höhe befindet sich ein solcher Orbit?

Unsere Überlegung war folgende: Per Definition sind in einem solchen Orbit die Zentripetal- (Gravitationskraft) und die Zentrifugalkraft (Fliehkraft) gleich groß. Durch Umformungen folgt daraus, dass sich der geostationäre Orbit in ca. 36000 km Höhe befindet.

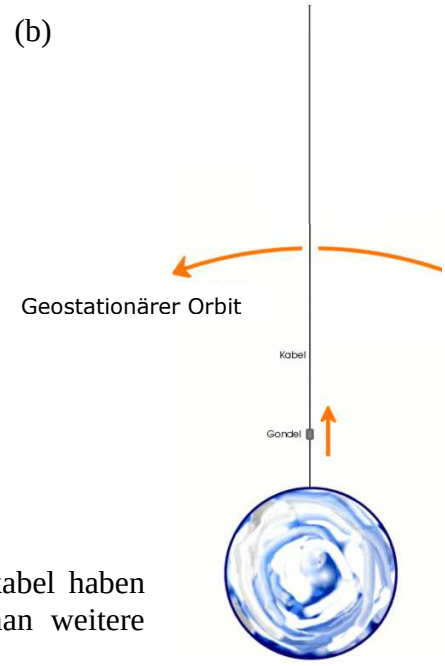
- Um zu berechnen, welche Bahn ein Mensch bzw. ein Körper, der in einer gewissen Höhe aus dem Lift „aussteigen“ würde, beschreiben würde, sind einige Vorüberlegungen notwendig. Wir kamen zum Schluss, dass eine solche Bahn ellipsenförmig ist und berechneten nun, in welcher Höhe man den Lift verlassen müsste, um nicht auf die Erde zu treffen (ca. $2{,}99*10^7$ m). Diese Höhe entspricht dem Abstand vom Erdmittelpunkt bis zum Absprungpunkt. Natürlich muss auch die Atmosphäre mit einberechnet werden, da man sonst verglühen würde. Außerdem berechneten wir, in welcher Höhe man abspringen müsste, um nach 3 Umläufen um die Erde wieder gleichzeitig mit dem Lift an der Ausstiegsstelle zu sein. ($3{,}18269*10^7$ m gemessen vom Erdmittelpunkt.)

- Um den Satteliten nicht aus seinem Orbit herunterzureißen, gäbe es mehrere relativ einfache Möglichkeiten. Man könnte entweder eine entsprechend schwere Masse als Gegengewicht an die Station anhängen (a), oder das Kabel in der gleichen Richtung, in der es von der Erde kommt, weiter auslegen. (b)

(a)



(b)



Wie berechneten sie Länge, die ein Ausgleichskabel haben müsste: ausgehend vom geostationären Orbit müsste man weitere $1{,}08*10^8$ m Kabel verlegen.

- Die Nanotechnologie ist noch nicht weit genug entwickelt um Kabel in einer Länge über 100 Meter herzustellen. Andere Materialien sind einfach viel zu schwer und würden unter ihrem eigenen Gewicht einstürzen. Das Problem des Kabels an sich wird sicher das am schwersten zu lösende.

- Die Energie, die man benötigt, um eine Masse m über diese ganzen 36.000 km zu bewegen, ist überraschender Weise gar nicht so unvorstellbar groß. Um eine kg über diese Strecke zu befördern benötigt man 13,45 kWh.

Das Land Steiermark
Bank Austria Creditanstalt
UNI GRAZ
MATHEMATIK

Projekt: Kryptographie

Ich bin ICH! – Bist du wirklich DU?

Prof. Günter Lettl

Teilnehmer: Alexander Bors, Stefanie Haselmann, Wolfgang Hrauda, Paul Laufer, Florian Andritsch, Florian Mikulik

PROBLEMSTELLUNG:

In vielen Situationen des Alltags muss man seine Identität nachweisen bzw. beweisen, damit man zu einer bestimmten Tätigkeit berechtigt ist:
Ich muss nachweisen können, dass ich rechtmäßig mit einer Bankomatkarte bezahle, vom Sparbuch oder Konto einen Geldbetrag abheben darf, einen besonders gesicherten Teil eines Firmengeländes betreten darf, einen Computer benützen darf oder ein Handy mit einer gültigen SIM – Karte verwende. Das Fachwort für diesen Problemkreis der Informationswissenschaft heißt „Identifikation“ oder auch „Benutzerauthentifikation“.
in diesem Projekt wollen wir unterschiedliche Modelle entwickeln und untersuchen, welche für derartige Problemstellungen angewendet werden können. Insbesondere wollen wir die Sicherheit bzw. Möglichkeiten zu Missbrauch analysieren. Gibt es auch mathematische Modelle zur Überprüfung meiner Identität, bei denen die überprüfende Instanz nichts von meinem Geheimnis (Passwort, PIN – Code, …) erfährt?

ERGEBNISSE:

1 Passwörter und Identifikation

Im Laufe der vergangenen Woche haben wir uns besonders mit der Wahl von sicheren Passwörtern beschäftigt. Dabei haben wir den sicheren Umgang und die vorgeschlagene Mindestlänge ausführlich beschrieben: Ein sicheres Passwort sollte aus mindestens acht Zeichen bestehen – sinnvoller Weise aus Groß- und Kleinbuchstaben sowie aus Ziffern. Außerdem sollte es regelmäßig gewechselt werden. Diese Regeln sollte man auf keinen Fall missachten, denn die Angreifer können mit so genannten „Passwort-Cracker“ – Programmen, die sie zu diesem Zweck verwenden, Passwörter sehr leicht entschlüsseln. Wenn das Passwort erst einmal geknackt ist, stehen dem Unbefugten sämtliche Möglichkeiten frei Daten zu verändern, zu zerstören, oder in Firmen-Netze einzudringen. Ein weiteres Thema, mit dem wir uns auseinander gesetzt haben, ist die Benutzerauthentifikation: Grundsätzlich kann man einen Menschen an folgenden Merkmalen erkennen: Charakteristische Eigenschaften, Besitz und Wissen. Zur Authentifikation zwischen Computer und Rechner verwendet man sehr häufig Passwörter: Der Rechner hat ein „Referenzpasswort“ P0 gespeichert, das dem Benutzer bekannt ist. Der Benutzer tippt zur Authentifikation sein Passwort P ein, und der Rechner überprüft, ob P und P0 übereinstimmen. Wenn es eine Übereinstimmung gibt, wird der Benutzer zugelassen. Auch bei der Sicherheit beim Handy funktioniert dieses System sehr ähnlich. Alle Schlüssel, die für die kryptographischen Operationen verwendet werden, werden auf der SIM-Karte (Subscriber Identity Module) gespeichert.

2 Vorbereitung für eine eigene Hash-Funktion

Als großes Ziel haben wir uns dann gesetzt, eine eigene Hash-Funktion zu erstellen, mit der wir von einem PC zum anderen verschlüsselte Daten senden können. Wir haben uns dazu entschlossen, alle unsere Programme in C zu programmieren.

Als Vorbereitung dafür, und für die Diffie-Hellman-Verschlüsselung der gesendeten Hash-Werte benötigten wir einige Funktionen und Programme, die uns zum Beispiel alle Primzahlen bis zu einem gewissen Grenzwert berechnen. Dies passiert, indem eine Schleife alle ungeraden Zahlen bis zu dem Grenzwert durchläuft, und diese mit allen kleineren Zahlen auf die Teilbarkeit überprüft.
Des Weiteren brauchen wir für die Diffie-Hellman-Verschlüsselung ein kleines Script, welches Zahlen in ihre Primfaktoren zerlegt. Bei diesem Programm wird eine Zahl eingegeben, und dann werden alle kleineren Zahlen ab 2 auf die Teilbarkeit überprüft.
Danach haben wir uns noch dazu entschlossen, dass wir den bereits verschlüsselten Hash-Code, den wir aus der Hash-Funktion erhalten, vor dem Senden noch einmal verschlüsseln, und statt in Hexadezimaler Schreibweise in Bitschreibweise (nur „0“ und „1“) versenden. Zuerst werden die Zahlen und Buchstaben des Hashs eingelesen, und mit Hilfe der ASCII-Tabelle (zB. „A“ = 65 = 2^0+2^6 = 01000001) in 512 Bit umgewandelt. Danach wird der Binärcode in 2 Hälften unterteilt. Die „rechte“ Hälfte wird per bitweisem exklusiven ODER mit der „linken“ Hälfte verrechnet (1+1=0; 0+0=0; 1+0=1; 0+1=1), Danach wird das Ergebnis als rechte Hälfte verwendet, somit ist die rechte Hälfte von der Linken abhängig. Nun werden die linken 256 Bit mit einem 32 Zeichen langen Schlüssel, der bereits vom User bestimmt wurde und in Binärdarstellung vorliegt, per exklusivem ODER verrechnet. Nun ist die 512 Bit lange Kette aus Nullen und Einsen so vermischt, dass diese ohne den Schlüssel nur schwer wiederhergestellt werden kann.
Diese Verschlüsselungsmethode wurde dem DES-Schlüssel nachempfunden, der fast die gleiche Methode zur Verschlüsselung verwendet, den Code jedoch nicht in einer, sondern in 16 Runden verschlüsselt. Entschlüsselt wird, indem die Schritte rückwärts ausgeführt werden.

3 Diffie-Hellman

Das Diffie-Hellman-Verfahren stellt eine Basis für einen sicheren Datenaustausch zwischen zwei Systemen. Über eine ungesicherte Leitung werden nur wenige Werte übermittelt, mit denen beide Kommunikationsteilnehmer unter Zuhilfenahme eines mathematischen Algorithmus ein und denselben Schlüssel errechnen können. Für einen außenstehenden Dritten bietet sich keine Möglichkeit, diesen Schlüssel innerhalb eines realistischen Zeitintervalls zu berechnen.
Im Verlauf der Modellierungswoche versuchten wir, ein solches System zu programmieren, indem wir unter Verwendung der Programmiersprache C eine Kommunikation zwischen zwei Computern aufbauten.

4 DES

DES - Data Encryption Standard, ein symmetrischer Algorithmus, bei dem derselbe Schlüssel für das Ver- und das Entschlüsseln verwendet wird. In DES werden jeweils Blöcke von je 64bit verschlüsselt, wobei die einzelnen Blöcke in 16 Runden mittels Substitutionen und Permutationen nach dem "Feistel"-Schema verschlüsselt.
Der Algorithmus läuft in zwei Schichten ab, und kann durch umgekehrte Anwendung der einzelnen Schlüssel und Permutationen wieder rückgängig gemacht werden. Mittlerweile gilt DES nicht mehr als sicher, da Supercomputer die Verschlüsselung in 22 Stunden knacken können. Triple-DES bzw. dreifache Anwendung von DES bring jedoch eine extrem hohe Sicherheit mit sich.
Im Laufe der Woche wurde der DES Algorithmus in der Programmiersprache C nachgebaut.

5 Hash-Funktionen

Eine Hash - Funktion dient zum Verschlüsseln einer beliebig langen Originalnachricht nach einem bestimmten Muster, so dass diese Verschlüsselung nicht mehr rückgängig gemacht werden kann. Eine gute Hash - Funktionen sollte so wenige Kollisionsmöglichkeiten wie möglich haben; eine Kollision tritt dann auf, wenn zwei verschiedene Eingabewerte denselben Output erzeugen.

6 MD5

Der Message Digest Algorithm 5 ist eine weit verbreitete Hash - Funktion. Der Output dieser Funktion ist immer 128 Bit lang und wird normalerweise als 32-stellige Hexadezimalzahl notiert. Die MD5 - Summe für den String „Ich bin ein Freak!“ beträgt zum Beispiel „d5f8426b80f7babe672ab8701a01e83c“.
Es wurden bereits mehrfach Kollisionen festgestellt, die allerdings auf die praktische Fälschungssicherheit von mit MD5 erzeugten Zertifikaten keine Auswirkung haben.
MD5 - Summen werden zum Beispiel zur Integritätsprüfung von Dateien verwendet, wobei die momentane MD5 - Summe einer Datei mit einer bereits von früher bekannten Summe verglichen wird.

Entwicklung eines eigenen Hash-Algorithmus: |MEGATRON|

Auf dem Wissen über die Funktionsweise des MD5 Algorithmus basierend, setzten wir uns das Ziel einen eigenen Algorithmus zu entwickeln. Ein Input beliebiger Länge wird auf eine 512bit lange Ausgabe abgebildet. In der Verarbeitungsphase werden die eingegebenen Bytes in Binärdarstellung, nach Codierung in 32 Runden mit verschiedenen Schlüsseln, mit Hilfe der Nachkommastellen von π (ebenfalls in Binärdarstellung) unter Verwendung einer exklusiven ODER-Verknüpfung abgeglichen. Die 512bit lange Kette wird in zunächst in acht 64bit lange Ketten geteilt, welche nach anschließenden Bit-Operationen weiter in acht 8x8 Blöcke zerlegt werden. Es folgen Verschiebungen, Drehungen, Spiegelungen und logische Verknüpfungen dieser Blöcke, bevor diese nach Bit-Shifts wieder zusammengesetzt werden. Damit selbst geringste Veränderungen im Eingabetext größtmögliche Differenzen im Ausgabecode zur Folge haben, wird eine Multiplikation aller Elemente der Menge des Ausgabe-Strings paarweise in pseudo-Hexadezimaldarstellung durchgeführt. Am Ende wird eine 512bit lange Ausgabe in Hexadezimalcodierung zusammengeführt.
|MEGATRON| scheint trotz vergleichsweise kurzer Entwicklungszeit recht sicher zu sein, denn bisher konnten keine Kollisionen ermittelt werden.

Projekt: Umwelt und Wirtschaft

Produktionsspitze des Erdöls

Prof. Stephen Keeling

Teilnehmer: Katharina Albert, Lukas Andritsch, Teodora Corduneanu, Elisabeth Gaar, Lisa-Maria Sommer, Daniel Steuber

PROBLEMSTELLUNG:

Die Produktionsspitze des Erdöls ist bereits erreicht und in naher Zukunft könnte unser Erdölvorrat erschöpft sein. Wegen ressourcenbedingter Grenzen sinkt das Angebot, trotz steigender Nachfrage. Der Großteil der modernen Welt im Großteil von der Verfügbarkeit der Ressource Erdöl abhängt, doch lässt sich dieses nicht leicht durch alternative Energieträger ersetzen. Da die Bevölkerung wächst, muss die vorhandene Energie notwendigerweise effizienter eingesetzt werden und dementsprechend werden sich auch manche Lebensstile ändern müssen.
Das Ziel des Projekts ist, ein Modell zu entwickeln, das möglichst viele Einflüsse auf den Preis des Öls zeigt, die Entwicklung der Bevölkerung aufgrund des Öls erklärt und die Produktion beinhaltet.

ERGEBNISSE:

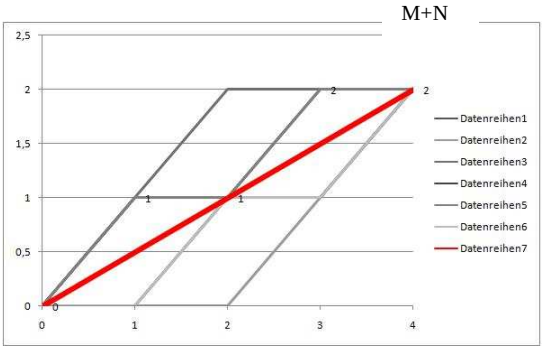
Logistische Funktion:

Die logistische Funktion wird sehr häufig im Zusammenhang mit Wachstumsprozessen verwendet. Ein großer Vorteil dabei ist dass man eine wieder abflachende Exponentialfunktion sehr gut beschreiben kann.

Als allgemeine Formel gilt: $f(t) = \dfrac{K}{1+e^{-\frac{t-t_0}{\tau}}}$

Hiebei gilt
K…Maximaler Wert den f(t) annehmen kann(Asymptote)
e…eulersche Zahl(2,718281828459)
t_0…Wendepunkt der Kurve
τ…Parameter, der Auswirkung auf die Steigung der Kurve hat(indirekte Proportional)

Entdeckung



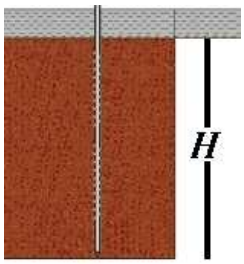
Wenn man sich die Welt als ein riesiges Gitter voller Felder vorstellt, die entweder Öl enthalten oder nicht, und man zufällig eines nach dem anderen aufbohrt, so lässt sich der Graph der Funktion der Entdeckung immer als **Gerade** darstellen: Die Wahrscheinlichkeit für jeden auftretenden Fall (in welcher Reihenfolge man die vollen bzw. leeren Felder aufbohrt) ist gleich groß, d.h. jeder Fall tritt nach einigem Probieren gleich oft auf und somit ist der Durschnitt eine Gerade. (Dies gilt für jede mögliche Anzahl von Öl- und Antiölfeldern).

N….Anzahl der Felder mit Öl
M…Anzahl der Felder ohne Öl

Doch aufgrund der Erfahrungen die der Mensch macht (niemand bohrt freiwillig ein zweites Mal in einen Berg wenn er beim ersten Mal nichts findet!!!), ist der Graph der Funktion eine **logistische Kurve**: nach anfänglichen Startschwierigkeiten, bei denen der Suchende willkürlich die Gegend absucht, kann er nach einiger Zeit die Eigenschaften des Bodens immer genauer bestimmen und aufgrund des Auswahlverfahrens steigt die Wahrscheinlichkeit des Erfolges. Nachdem ein Großteil der Ölfelder gefunden wurde, fällt die Häufigkeit des Entdeckens und die Kurve flacht ab.

Physikalischer Ansatz: Das Brunnenmodell - Ölproduktion
Hierbei wird die Ölproduktion anhand eines einfachen Brunnenmodells gezeigt.
Der Brunnen ist bis oben hin mit Öl gefüllt (H), dieses Öl wird mit einer Pumpe, die bis an den Grund des Brunnens reicht, gefördert. Wir gingen davon aus, dass die Pumpe mit einer konstanten Pumpenleistung arbeitet.

$H = h(0)$	Ausgangshöhe des Öls
A	Grundfläche des Brunnens
P	Produktion
F	Flussrate
V	Volumen
E	Gesamtentdeckung



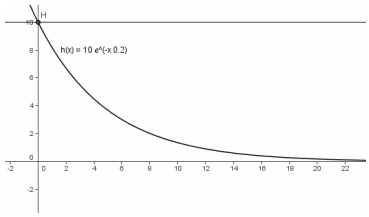
Da die Pumpenleistung konstant ist, wird die Menge des heraus gepumpten Öls weniger.

$$\rightarrow \quad h'(t) = -\alpha \cdot h(t)$$

Nach Lösen der Differentialgleichung kamen wir zu folgender Formel:

$$h(t) = H \cdot e^{-\alpha t}$$

$$\alpha = \frac{F}{V}$$



Die produzierte Menge ist somit abhängig von der Ölmenge die noch im Boden vorhanden ist:

$$P(t) = A \cdot H - A \cdot h(t) \rightarrow P(t) = V(0) - V(t)$$

Durch Ableitung von P ergibt sich

$$P' = \alpha(V(0) - P) = \alpha(E - P)$$

Um unsere Modellierung der Ölproduktion nicht nur für einen Brunnen verwenden zu können, passten wir die Formel für mehrere Brunnen an, allerdings unter der Annahme dass alle die gleichen Eigenschaften haben.

$$P_i' = \alpha_i\left(P_i^{\max} - P_i\right) \rightarrow P' = \sum_{i=1}^{N} \cdot P_i'$$

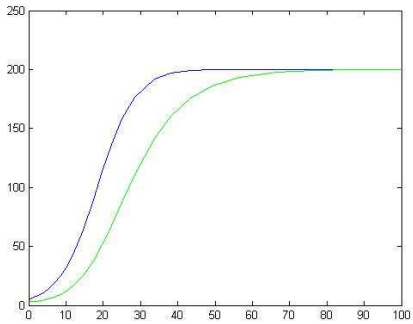
$$P' = \alpha \sum_{i=1}^{N} P_i^{\max} - \alpha \sum_{\hat{i}=1}^{N} P_i = \alpha(E - P)$$

Wir haben die Ölproduktion auch durch Zufluss von Salzwasser während der Ölförderung modelliert, unter der Annahme dass sich Salzwasser mit Öl mischt, und sind auf ein ähnliches Ergebnis gestoßen.

Kopplung von Entdeckung und Produktion

$$E' = \beta \cdot E(M - E)$$
$$P' = \alpha(E - P)$$

Wenn man Entdeckung und Produktion koppelt sehen beide logistisch aus.



Wirtschaftlicher Ansatz: Wirtschaftssystem

Bei unserem Wirtschaftssystem versuchen wir, die wichtigsten Einflüsse auf den Ölpreis zu bestimmen.
Um es zu vereinfachen nehmen wir an die einzige Ölfirma zu sein (ein richtiges Monopol!).
Laut den Gesetzten des freien Marktes Bestimmen somit Angebot und Nachfrage den Preis.

Co	Mindestpreis	
V	Vorrat	$V' = P' - N'$
B	Bevölkerung	$B' = \delta(F - B)B + \rho \cdot A'$

Um zur Funktion des Angebotes berücksichtigten wir, dass wir nicht mehr als den Vorrat anbieten können und dass unser Preis nicht kleiner als unserer Mindestreis (beinhaltet alle Kosten) sein soll.

Daraus ergab sich: $A' = V \cdot \ln\left(\frac{C}{C_0}\right)$

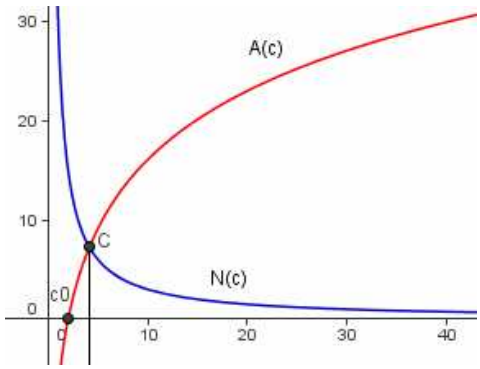
Die Nachfrage ist wiederum direkt von der Bevölkerung und indirekt vom Preis abhängig, die Konstante κ bestimmt den Verbrauch an Öl pro Person.

Man erkennt: $N' = \frac{\kappa B}{C}$.

Der Schnittpunkt von *N'* und *A'* ist somit *C*, der Ölpreis.

Das Kapital unserer Firma berechnet sich aus Einnahmen und Ausgaben. Die Einnahmen sind *C* mal das verkaufte Öl oder auch *C* mal die Nachfrage. Die Ausgaben sind *C*o mal das Angebot plus etwaige Fixkosten (γ).

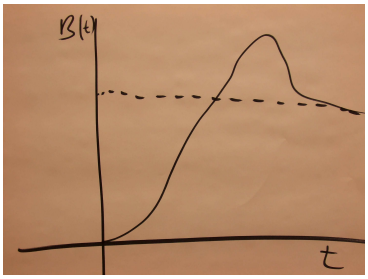
$\rightarrow K' = CN' - C_0 A' - \gamma$



Aus Angebot und Nachfrage ergibt sich der Preis.

Bevölkerungsformel

Da die Bevölkerung nicht gleich bleibt, muss auch für diese eine Formel gefunden werden. Daher überlegten wir uns, dass wir einen Zusammenhang zwischen vorhandenem Erdöl und der Bevölkerung herstellen sollten. Außerdem sollte auch noch bedacht werden, dass man mit alternativer Energie einen gewissen Bedarf an Energie decken kann. Dies sollte alles in unserer Formel berücksichtigt werden. Nach langem Überlegen und bereits 5 nicht passenden



Formeln kamen wir auf eine passende Formel in der die Bevölkerung vom aktuellen Erdölangebot am Markt abhängt. Diese hat ungefähr folgende Form:
Zuerst steigt in der Grafik der Wert solange, bis die Nachfrage an Öl befriedigt werden kann. Nachdem alles Erdöl aufgebraucht ist, sinkt die Bevölkerung auf einen Wert, der nur mehr mit erneuerbarer Energie gedeckt werden kann. Auf diese Art wurden alle notwendigen Parameter miteinbezogen.

MatLab Modell

Nachdem wir uns mit MatLab vertraut gemacht haben, haben wir ein Model unseres Gleichungssystems aufgestellt. Die ersten Probeläufe liefen gut, doch anfänglich hatten wir Probleme mit realistischen Zahlen und Parametern, doch nach öfterem Überarbeiten haben wir schließlich ein Modell erstellt, in dem wir die Zusammenhänge zwischen Entdeckung, Produktion, Vorrat, Kapital, Nachfrage, Angebot, Preis und Bevölkerung grafisch dargestellt haben. Mit diesem Modell haben wir nicht nur alle von uns gefundenen Funktionen in Verbindung gebracht, sondern haben auch die Möglichkeit, Aussagen über die weitere Ölpreisentwicklung zu treffen.

Das Land Steiermark
Bank Austria Creditanstalt
UNI GRAZ MATHEMATIK