Modul: Informatikgeschichte 7KGb
Vorgeschichte der Software

Datum:	16.10.2018
Beginn:	18:05 Uhr
Ende:	19:35 Uhr
Anwesend:	Dr. Peter Gros, Studierende des Moduls Informatikgeschichte
Protokoll:	Dario Lohmuller, Pascal Oertli

Inhaltsverzeichnis

Algebra und Algorithmus

Muḥammad ibn Mūsā al-Khwārizmī war ein persischer Mathematiker und schrieb 2 - für die Mathematik sehr bedeutsame - Bücher. Im ersten Buch behandelt al-Khwārizmī die indische Zahlenschrift. Darin stellte er das Rechnen mit Dezimalzahlen vor und führte die indische Ziffer Null in das arabische Zahlensystem über. Dies nahm natürlich nicht nur Einfluss auf das arabische Zahlensystem, sondern auch direkt auf alle modernen Zahlensysteme, welche aus dem arabischen System entstanden.
Aufgrund seines Einflusses auf die Mathematik wurde aus seinem Namen “al-Khwārizmī” später auch das Wort “Algorithmus” abgeleitet. Auch das Wort “Algebra” findet seinen Ursprung bei al-Khwārizmī, da er sein 2. Buch dem “Rechenverfahren durch Ergänzen und Ausgleichen” widmete (al-Kitāb al-muḫtaṣar fī ḥisāb al-ǧabr wa-ʾl-muqābala). Er war einer der ersten, welcher Algorithmen zum Rechnen mit simplen Operationen aufstellte und das Lösen von Gleichungen für Laien nachvollziehbar machte.
Aus “ al-ǧabr” wurde später “Algebra”.

Arabische Bücher wurden schon früh ins Lateinische übersetzt, weshalb auch damals schon die modernen Länder darauf Zugriff hatten und davon profitieren konnten.
Die römischen Ziffern eignen sich sehr schlecht für schriftliche mathematische Grundoperationen, weshalb bereits im Jahre 1202 Leonardo Fibonacci die arabischen Zahlen in Europa verbreiten wollte, da er sah, dass sie den römischen Zahlen überlegen waren.

Gerbert von Aurillac war ein französischer Papst, welcher im zehnten Jahrhundert in Frankreich lebte. Er zeigte grosses Interesse an der Mathematik und versuchte in seiner Tätigkeit als Lehrer die Verwendung der arabischen Zahlen zu fördern.
Aurillac wendete die erlernten arabischen Zahlen auf einen Rechenschieber (Abacus) an und konnte komplexe Berechnungen ausführen. Für die Menschen damals waren komplexe Rechnungen mit römischen Zahlen fast unvorstellbar.
Im 11. Jahrhundert erlebte der überarbeitete Abacus in Europa einen Aufschwung, aufgrund Aurillac’s Bemühungen.

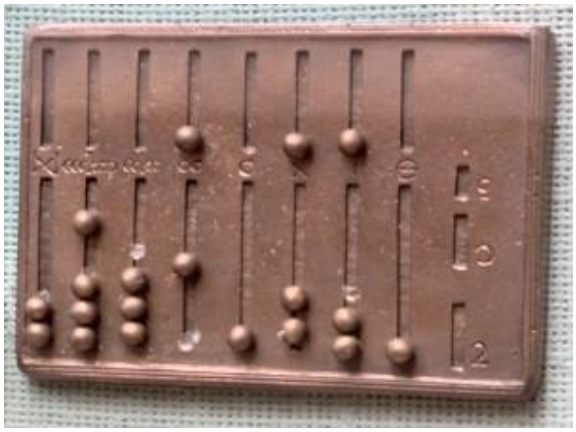

Abbildung 1 römischer Abacus

Raimundus Lullus, ein Missionar, Philosoph und Logiker, versuchte mithilfe von Logik Heiden und Muslime zum Christentum zu bekehren. Er war der Meinung, es wäre möglich religiöse Probleme mit Logik zu lösen und entwickelte eine logische Maschine, mit welcher er versuchen wollte, Wahrheit und Lüge mithilfe des Verstandes zu unterscheiden. Die Maschine bestand aus drehbaren Scheiben auf welchen Begriffe standen, die verschieden kombiniert werden konnten. Ebenfalls enthielten die Scheiben logische Operationen, wie: Gleichheit, Widerspruch, Übereinstimmung und Unterschied. Die Verknüpfungen entsprachen den Schlussformen des syllogistischen Prinzips.

Abbildung 2 Ars Magna

Der deutsche Gelehrte Athanasius Kircher entwickelte im 17. Jahrhundert ein System wovon er glaubte, die Welt erklären zu können. Er baute mit seinen Theorien auf den Arbeiten von Lullus auf und verwendete ähnliche Methoden um Graphen darstellen zu können.
Kircher's Arbeiten zählen als erste Vorläufer der Graphentheorie.
Des Weiteren erfand er die Organum Mathematicum, eine mathematische Rechenhilfe. Die Maschine unterstützte eine grosse Spanne an Rechenoperationen in den Bereichen Arithmetik, Geometrie, Musik, und viele mehr.

Abbildung 3 Organum Mathematicum

Erfindung der reinen Mathematik

George Boole veröffentlichte 1854 sein Buch “The Laws of Thought” indem er das Binärsystem beschrieb und ebenfalls erstmals boolesche Algebra auftauchte. Dies war aus heutiger Sicht ein wichtiger Grundstein für das das moderne Informationszeitalter.

Der deutsche Mathematiker und Philosoph Gottlob Frege beschäftigte sich ebenfalls mit Logik. Er war der Meinung, dass man die Logik auf einem grundlegend mathematischen Fundament aufbauen könne. Er schrieb das Buch “Grundgesetze der Arithmetik”, vor dessen Veröffentlichung er von Bertrand Russell auf einen fatalen Widerspruch hingewiesen wurde. Dies führte zu einem Paradox, welches die bisherige Entwicklung der Logik stark erschütterte.

Den Logik Paradoxen entgegenzuwirken versuchten auch die Herren Bertrand Russell und Alfred North Whitehead. Sie verfassten die “Principia Mathematica”, ein dreiteiliges Werk, welches sich mit Axiomen und formaler Logik auseinandersetzt.

Auch einer der wichtigsten Mathematiker der Welt, David Hilvert, beschäftigte sich mit der Logik. Er war von fester Überzeugung, dass der Mensch alles verstehen und erklären kann. Dies Zeigte auch seine berühmte Aussage 1930: *Wir müssen wissen und wir werden wissen.*
Er versuchte unter anderem ein Programm aufzustellen, um zu überprüfen, ob die Mathematik entscheidbar sei.
Aus seiner Arbeit mit Bezug auf die Prädikatenlogik entstand schlussendlich das sogenannte Entscheidungsproblem. Dieses stellt die Frage, ob es einen Algorithmus bzw. ein Programm gibt, welches für jeden Input eine korrekte Ja-/Nein-Antwort berechnen kann.

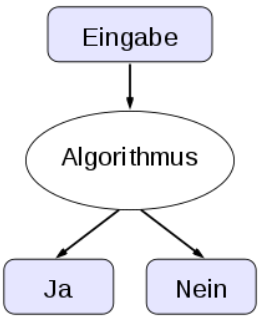

Abbildung 4 Symbolbild Entscheidungsproblem

Alan Turing wollte den Beweis dafür liefern. Dafür entwickelte er die Turing-Maschine, welche zeigen sollte, dass ein Problem mit endlich vielen Schritten lösbar sei. Allerdings lieferte er damit schlussendlich den Beweisen, dass das Entscheidungsproblem nicht lösbar ist. Es kann also keine Maschine, Programm oder Algorithmus geben, welche für alle möglichen Probleme eine Antwort findet.

Auch Kurt Gödel beschäftigte sich mit der mathematischen Logik und stellte, in einem seiner späten Werke, “Formalization, Mechanization and Automation of Gödels Proof of Gods Existence”, einen Gottesbeweis auf. Dies gelingt ihm auch mehr oder weniger. Zumindest mathematisch formal ist der Beweis korrekt. Allerdings muss Gödel für diesen Beweis einige Annahmen treffen, welche man nicht beweisen kann.

Annahme 1: Eine Eigenschaft oder ihre Umkehrung ist positiv, nie beides.	$\forall\phi[P(\neg\phi) \leftrightarrow \neg P(\phi)]$
Annahme 2: Eine Eigenschaft, die eine positive Eigenschaft beinhaltet, ist positiv.	$\forall\phi\forall\psi[(P(\phi) \wedge \Box\forall x[\phi(x) \rightarrow \psi(x)]) \rightarrow P(\psi)]$
Lehrsatz 1: Positive Eigenschaften sind möglicherweise beispielhaft.	$\forall\varphi[P(\varphi) \rightarrow \Diamond\exists x\varphi(x)]$
Definition 1: Ein göttliches Wesen enthält alle positiven Eigenschaften.	$G(x) \leftrightarrow \forall\phi[P(\phi) \rightarrow \phi(x)]$
Annahme 3: Die Eigenschaft, gottgleich zu sein, ist positiv.	$P(G)$
Schlussfolgerung: Möglicherweise existiert Gott.	$\Diamond\exists xG(x)$
Annahme 4: Positive Eigenschaften sind notwendigerweise positiv.	$\forall\phi[P(\phi) \rightarrow \Box P(\phi)]$
Definition 2: Die Essenz eines Individuums ist die Eigenschaft, die von diesem umgesetzt wird und beinhaltet notwendigerweise irgendeine seiner Eigenschaften.	$\phi \text{ ess. } x \leftrightarrow \phi(x) \wedge \forall\psi(\psi(x) \rightarrow \Box\forall y(\phi(y) \rightarrow \psi(y)))$
Lehrsatz 2: Göttlich zu sein ist die Essenz jeder götterähnlichen Existenz.	$\forall x[G(x) \rightarrow G \text{ ess. } x]$
Definition 3: Notwendige Existenz eines Individuums ist die notwendige Beispielhaftigkeit all seiner Essenzen.	$NE(x) \leftrightarrow \forall\phi[\phi \text{ ess. } x \rightarrow \Box\exists y\phi(y)]$
Annahme 5: Die notwendige Existenz ist eine positive Eigenschaft.	$P(NE)$
Lehrsatz 3: Notwendigerweise existiert Gott.	$\Box\exists xG(x)$

Abbildung 5 Gödels Gottesbeweis

Beginn des Informationszeitalters

1805 entwickelte Joseph-Marie Jacquard einen automatisierten Webstuhl. Der nach ihm benannte Jacquardwebstuhl funktionierte mit Lochkarten, welche das Webmuster vorgaben. Anfangs musste das Weben noch von Arbeitern getätigt werden, später wurde auch dies automatisiert und die ersten vollautomatischen, programmierbaren Webstühle waren geboren.

Das Prinzip der Lochkarte wurde bald in vielen Bereichen übernommen.
Beispielsweise dauerte früher eine komplette Volkszählung in den USA bis zu sechs Jahre, bis alle Daten zu erfasst und ausgewertet waren. Herman Hollerith gelang es diesen Prozess stark zu beschleunigen, indem er spezielle Lochkarten entwickelte, welche eine Person repräsentierten. Darauf wurden jegliche Daten (Alter, Rasse, etc..) aufgenommen, indem mit einem Pantographen an den entsprechenden Positionen ein Loch gestanzt wurde. Die Lochkarten wurden anschliessend in die Hollerith-Maschine eingelegt. Dabei wurden an den Stellen mit den Löchern ein elektrischer Kontakt geschlossen. Dies führte dazu, dass die jeweilige Zähluhr um eins inkrementiert wurde und man jederzeit den Überblick über alle erfassten Werte hatte.

Abbildung 6 Hollerith Maschine

Bald wurden auch andere auf diese neue Technologie aufmerksam und immer mehr neue Implementierungen entstanden.
Firmen begannen ganze Lagerverwaltungssysteme aufzubauen, welche nun dank Lochkarten-auswertung automatisiert werden konnten.
Auch ging es nicht lange und die ersten Stempeluhren entstanden, sodass Arbeitgeber stets den Überblick über die geleisteten Stunden aller Arbeiter haben konnten. Über diese Entwicklung freuten sich viele Arbeiter anfangs nicht. Einige Jahrzehnte später, stellten sich die Gewerkschaften jedoch gegen die Abschaffung von Stempeluhren, da es mittlerweile als Schutz der Arbeiter angesehen wurde. Da die Stunden jedes Arbeiters genauestens dokumentiert wurden, sicherte dies den Arbeitern die Bezahlung von Überstunden.

Später wurde es auch möglich, die Interpretation der Werte auf der Lochkarte zu definieren. Es konnten zum Beispiel die Werte der Karte als Buchstaben interpretiert werden, was es ermöglichte, das Alphabet auf die Löcher abzubilden. Dies trug ebenfalls zur Verbreitung der Lochkarten bei.

Die vielseitige Anwendung der Lochkarten führte jedoch nicht immer zu positiven Ergebnissen. Im Zweiten Weltkrieg nutzte das Rassenamt in Berlin die Hollerith-Maschine von IBM zur Judenverfolgung.

Aufkommen der Chiffriermaschinen

Die deutsche Wehrmacht suchte nach dem Ersten Weltkrieg eine neue Chiffriermaschine um die Kommunikation zwischen den deutschen Truppen zu verschlüsseln. Zuvor gab es nur veraltete oder manuelle verschlüsselungsverfahren, die für militärische Zwecke nicht mehr geeignet waren. Die deutschen wurden bei dieser Suche bei der Enigma fündig.
Die Enigma bestand grundsätzlich aus einer Tastatur, einem Steckbrett, mehreren Rotoren und einer Anzeige, alles in einem tragbaren Gehäuse (mit Ausnahme der extra Rotoren). Auf dem Steckbrett konnten diverse Konfigurationen gesteckt werden, die die Tasten mit der Ausgabe verschieden verknüpften. Der Rotor wurde nach jedem Tastenanschlag um eine Stelle gedreht, was zur Folge hatte, dass jeder Buchstabe auf eine andere Weise verschlüsselt wurde. Dies machte es umso schwieriger, von der Enigma verschlüsselte Texte zu knacken. Die deutschen verwendeten Monatslisten, die für jeden Tag im Monat die korrekte Einstellung der Enigma Maschine beschrieben. Dies beinhaltete das Layout der Steckbrett-Verbindungen und die Nummer des Rotors, sowie dessen Startposition.

Abbildung 7 Enigma

Ein grosses Problem der Enigma war jedoch, dass kein Buchstabe auf sich selbst abgebildet werden konnte. Das war die grösste Schwäche der Maschine. Reverse Engineering konnte betrieben werden, wenn man eine Idee hat, was die verschlüsselte Nachricht bedeuten könnte. Mit Annahmen und Ausprobieren konnte die richtige Einstellung der Maschine ermittelt werden.

Die Enigma galt trotzdem als sicher, da lange nicht in Betracht gezogen wurde, dass eine maschinelle Verschlüsselung durch maschinelle Entschlüsselung geknackt werden könnte, sofern genug Rechenleistung zur Verfügung stand. Mit den “Bomben” konnten viele der durch Enigma verschlüsselten Nachrichten durch die Alliierten entschlüsselt werden. Alan Turing war einer der Verantwortlichen für die Entwicklung dieser Entschlüsselungsmaschinen.
Es war über die ganze Zeit des Krieges wichtig, dass der Gegner nicht erfuhr, dass seine Kommunikation kompromittiert wurde. Effektiv konnte durch die Arbeit von Mathematikern die Dauer des Krieges verkürzt werden, da der deutsche Wehrmachts-Code geknackt wurde, ohne dass die deutschen sofort davon wussten.

Abbildungen:

Abbildung 1 römischer Abacus:
https://upload.wikimedia.org/wikipedia/commons/b/b5/RomanAbacusRecon.jpg

Abbildung 2 Ars Magna:
https://upload.wikimedia.org/wikipedia/commons/8/8f/Ramon_Llull_-_Ars_Magna_Fig_1.png

Abbildung 3 Organum Mathematicum:
https://upload.wikimedia.org/wikipedia/commons/thumb/b/b2/OrganumMathematicum.jpg/1920px-OrganumMathematicum.jpg

Abbildung 4 Entscheidungsproblem:
https://upload.wikimedia.org/wikipedia/commons/thumb/8/87/Entscheidungsproblem.svg/220px-Entscheidungsproblem.svg.png

Abbildung 5 Gödels Gottesbeweis:
https://israswiss.files.wordpress.com/2013/09/gc3b6dels_kette.png

Abbildung 6 Hollerith Maschine:
http://it-spots.de/wp-content/uploads/2009/06/102653125_706f4ffcd2_o.jpg

Abbildung 7 Enigma:
https://www.h-its.org/wp-content/uploads/2012/06/Enigma-Maschine.jpg