Theoretische Informatik

Geschichte und Bedeutung

– unter besonderer Berücksichtigung der Beiträge von Alan Turing

Vortrag
Im Rahmen der Vorlesung
„Theoretische Informatik“
von Prof. Dr. Rainer Schrader
gehalten im Wintersemester 2001/2002
an der Universität zu Köln

von Michael Bialowons

Version 1.0

Inhaltsverzeichnis

Kurze Geschichte der theoretischen Informatik

Zusammenfassung und Übersetzung des Artikels: John E. Savage, Brown University Providence; Alan L. Selman, University at Buffalo; Carl Smith, University of Maryland: History and Contributions of Theoretical Computer Science.

Ergebnisse der theoretischen Informatik (theoretical computer science) haben enormen Einfluß auf die Entwicklung von Programmiersprachen und andere Gebiete der Informatik (computer science) wie Kryptographie, Kommunikationsnetzwerke, Multimedia und graphische Systeme, Parallel-Computing, VLSI, Lernen. Darüberhinaus hat die theoretische Informatik auch die Biologie, Mathematik, Herstellung (manufacturing) und Astronomie beeinflußt.

In über 50 Jahren der Computerentwicklung wurden die Grundlagen der Disziplin durch die Entwicklung von Modellen des Rechnens (modells of computation) und daraus abgeleiteten Analysemethoden von theoretischen Informatikern gelegt. Nach dem frühzeitigen Erkennen der Bedeutung der Theorie der formalen Sprachen für die Praxis des Compilerbaus wurde die theoretische Informatik ein Eckstein der Hochschulausbildung in Informatik.

- in der Anfangszeit Entwicklung von Basiskonzepten wie: Entwurf fundamentaler Algorithmen, Identifizierung und Entwicklung wichtiger Unterdisziplinen, Klassifikation von Problemen durch ihre Komplexität
- heute Schwerpunkt auf Entwurf und Implementation sehr großer Computersysteme

Rolle der theroretischen Informatiker: Untersuchung der grundlegenden Probleme in diesem Bereich durch Modellierung, Analyse und Experimente (wird auch von angewandten Informatikern genutzt).

Was ist theoretische Informatik?
Theoretische Informatiker versuchen Computer-Phänomene zu verstehen:

- die Ausdruckskraft (expressibility) von Programmiersprachen,
- den Entwurf (design) und die Leistungsfähigkeit (performance) von Algorithmen
- generelle Grenzen der Berechenbarkeit (computation)

Sie fragen also: was ist Berechnung (computation)?; Was kann man berechnen? Wie? Mit welchem Aufwand?
Sie lernen von der Praxis und tragen zu ihrer Entwicklung bei. Schließlich versuchen sie, die Grundlagen (core activities) besser auf schwere Computerprobleme anzuwenden (address hard computational problems).

Manchmal dauert es Jahre, bis theoretische Konzepte sich in der Praxis durchsetzen. So gehen die für die Informatik wesentlichen Grundlagen des speicherprogrammierbaren Computers, zurück auf Alan Turing, der sie bereits in den 30er Jahren studierte und beschrieb.
Die Praxis der Computerprogrammierung konnte sich durch die Entwicklung der Automatentheorie durch Chomsky und andere in den 50er Jahren wesentlich weiterentwickeln. Auf der Grundlage der kontextfreien Grammatiken entwickelten Knuth und andere Algorithmen und Datenstrukturen für effizientes Erkennen (parse) von höheren Sprachen (high-level languages), was zur Entwicklung von Werkzeugen wie YACC? und damit zur Software-Revolution in den 60er Jahren führte. In den 70er Jahren entdeckten die Theoretiker bei der Untersuchung der in den Problemen selbst angelegten Komplexität (intrinsic complexity of computational problems) die große Klasse der NP-vollständigen Probleme.

Weitere Entdeckungen:

- harte Probleme in moderner Computer-Sicherheit (RSA public-key cryptosystem)
- Demonstration des Nutzens von mathematischer Logik und Automatentheorie zur Verifikation komplexer Computersysteme, z.B. nutzen Hardwarehersteller hierfür die sog. model-checking-technology.

Der Fortschritt in der Forschung der letzten 10 bis 15 Jahre verspricht einen starken Einfluß auch in der Zukunft. Die wesentlichen Ergebnisse:

- schnelle (polynomielle) Algorithmen mit festen Leistungsgrenzen (performance bounds) zur approximativen Lösung vieler NP-vollständigen Probleme
- randomisierte Algorithmen für schnelle Lösungen harter Probleme mit hoher Wahrscheinlichkeit (high probability).
- Einsatz von interaktiven Beweissystemen zur Verifikation von elektronischem Austausch (electronic exchange)

Ein Beispiel für den erklärenden Wert der theoretischen Informatik zeigt sich im modernen Web Browser: Er enthält das Konzept der abstrakten Maschine, das in den 70er Jahren entwickelt wurde. Beim benutzen eines Link (follow a link to data) ruft der Browser den passenden Interpreter (eine abstrakte Machine) zur Verarbeitung der Daten auf, z.B. um ein Bild anzuzeigen oder ein Java-Programm laufen zu lassen.

In der Zukunft werden Computersysteme groß und komplex sein und komplexe Interaktionen ausführen. Dieses zu verstehen ist eine enorme intellektuelle Herausforderung, die Anstrengungen von theoretischen und experimentellen Computerwissenschaftlern erfordert. Skalierbare Hard- und Softwaresysteme müssen entwickelt und einer Analyse unterzogen werden, bevor große Investitionen für ihren Einsatz erfolgen.
Zusammenfassend: „Wir brauchen mehr Grundlagenforschung von der Art des ´groundbreaking, high-risk/high-return` die die Ideen und Methoden neuer Paradigmen für die Zeit in zehn oder mehr Jahren liefert. Wir müssen klug investieren um die Früchte in den nächsten 40 Jahren ernten zu können.

Theorie in der Computer-Praxis

Theoretisches Forschungsgebiet	**Praktische Anwendung**	**Erläuterung**
Kryptographie und Sicheres Rechnen (secure computation)		
differential and linear cryptanalysis		Starke Verbesserung in der Beurteilung der Stärke herkömmlicher Verschlüsselungssysteme
factorization and discrete logarithm techniques based on the number field sieve	Neue Protokolle (z.B. für electronic cash)	Tieferes Verständnis von Grundlagen der public-key-cryptographie
Verbindungen zwischen Kryptographie und Maschinenlernen	Verbesserungen in Techniken zum Beweisen der Sicherheit von Kryptographie-Primitiven und Protokollen	?

Kommunikations-Netzwerke		
On-line Algorithmen, multicommodity flow Algorithmen	Zugangskontrolle, Routing in ATM-Netzwerken	Intensive Simulation dieser Algorithmen hat gezeigt, daß sie deutlich bessere Ergebnisse bringen als Standardansätze.
Theoretische Untersuchung von load balancing und web caching	Gründung der Fa. Akamai, (high visible new web caching company)	

Computer Geometrie		
Algorithmen zur Erzeugung von Delaunay triangulations und triangulations mit variierenden local properties	Mesh generation in computational fluid dynamics	
Voronoi Diagramme und Datenstrukturen für Nächster-Nachbar	Clustering-Algorithmen zur Sprach- und Bildkompression in Multimedia-Systemen für Personal-Computer	
Techniques for computing triangulations, line segmenta intersections and terrain visibility	Geographic information systems	
Visibility Graphs and visibility complex	Systems for computer vision and computer graphics	

Graph drawing algorithms	Advanced graphic user interfaces and visualization systems	

Parallele Computer Architekturen		
Mesh-connected-processors, hypercubes, cube-connected cycles, butterfly-networks	Design of parallel multiprocessor machines	
Algorithms for routing in networks including (multi-phase) randomized routing	“	

Software-Systeme		
Evolving algebras	Specify languages (z.B. C, Prolog, VHDL) Define real and virtual architectures (APE, PVM, Transputer) Validate standard language implementations (z.B. Prolog, Occam) Validate distributed protocols	
Epistemic logic	Analysis of existing and new authentication protocols	
Interaktive Beweissysteme wie ProofPower	Verify properties of critical systems	
Coordinating Communicating Systems (CCS)	Modeling, analysis and design of safety-critical systems	
Process calculi and related modal logics	Formally specify and analyze a cache coherence protocol for a multi-processor architecture; Prove correctness of a leader election protocoll for a point to point network; design and analyze a rendezvous-based scheduler to be used in an embedded software system	

Programmiersprachen		
Methods of structured operational semantics (with input from the lambda calculus and its model theory	Full-scale languages could be defined in such a way that properties (e.g. determinacy of evaluation and the lack of dangling pointers) of the language could be rigorously proven	
Semantic and syntactic theories of types	Language designs that are provably “type-sound”, leading to a significant increase in the reliability of a language and to greater efficiency in implementation	
Standard ML	Mechanized reasoning, program analysis, compiler construction	
Monads	Structuring denotational semantics, functional programming (Haskell), input-output and interaction with C, updateable arrays and references	

VLSI Design		
Minimum spanning tree, shortest-path algorithms	VLSI circuits layout algorithms and applications	
Models for single-layer routing	Graph partitioning, graph coloring	

Lerntheorie (Learning Theory)		
Computational learning theory community that learn subclasses of finite probabilistic automata	Handwriting recognition, part-of-speech-tagging, DNA sequence modelling, text correction	
Learning algorithms and techniques for deterministic automata	Reinforcement learning (new paradigm for machine learning)	
Learning algorithms for automata	Robot motion planning	

Beiträge zu anderen Disziplinen

Biologie		
Sparse dynamic programming techniques	New sequence alignment software for the comparison of two very long DNA sequences	

Mathematik		
Domain theory	Dynamical systems, measure and integration theory; fractals; finite-state discrete stochastic processes; iterated function systems; fractal image compression; neural nets; Ising model in statistical physics	
Fast algorith for polynomial decomposition	AXIOM, symbolic computation language developed by IBM	

Manufacturing		
A program *qhull* for computing convex hulls	Support structures for objects produced through layered manufacturing	Qhull reduced run times from minutes to seconds

Astronomie		
Network flow techniques	Determine telescope settings as part of the Sloan Digital Sky Survey	

Das Leben von Alan M. Turing

Überblick

Alan Mathison Turing (1912 – 1954)
Mathematiker, Logiker, Kryptoanalytiker, Computerkonstrukteur.

Herkunft aus der englischen Mittelschicht mit ´staatstragender` Bedeutung und teilweise noch viktorianischen Ansichten. Zweiter Sohn eines Verwaltungsbeamten der britischen Kolonialbehörde in Indien, Vorfahren der Mutter waren Ingenieure, Offiziere, Ärzte.

Bis Ende 1929	Besuch der Public-School in Sherborne, England
ab Anfang 1930 bis Mai 1934	Studium der Mathematik am King´s College der Universität Cambridge
März 1935	Wahl zum Fellow der Universität Cambridge
Von September 1936 bis Juli 1938	Studienaufenthalt an der Universität Princeton, USA
Mai 1938	Dissertation zum Erwerb des PhD
Bis August 1939	wissenschaftliche Tätigkeit am King´s College
ab September 1939 bis August 1945	Arbeit an der Entschlüsselung der Enigma-Maschine in Bletchley Park
September 1945 Bis Oktober 1948	Mitarbeit an der Konstruktion von Computern am National Physical Laboratory
Oktober 1948 Bis Juni 1954	Stellung an der Universität Manchester Mitarbeit an Computer-Projekten
März 1951	Wahl zum Fellow der Royal Society (FRS)
März 1952	Verurteilung wegen Homosexualität
Juni 1954	Freitod durch Vergiftung

Kindheit und Jugend

Aufgewachsen in englischen Pensionen und Privatschulen.
Frühe Faszinіation für Zahlen (vor dem Lesen), Einarbeitung in die Grundlagen der Naturwissenschaften als Schüler, tiefe Faszination für Chemie und Biologie.
Er verabscheut Kirchen („dort riecht es übel“). Im Internat gilt er als Eigenbrötler, fällt aber durch seine mathematische Begabung auf, liest *Einstein* und *Eddington*. Auf der Public-school trifft er Christopher Morcom, seinen ersten Freund. Dieser stirbt mit 19 Jahren an Tuberkulose. Turing schreibt der Mutter von Christopher noch lange Jahre immer wieder Briefe.

Studium und wissenschaftliche Tätigkeit

Ab 1931 Studium der Mathematik an der Universität Cambridge, Stipendium am *King´s College.* (King´s genoß besondere Privilegien innerhalb des Universitätssystems und war durch seinen Reichtum ausgezeichnet, dank des von John Maynard Keynes angehäuften Vermögens. Aber es schätzte auch moralische Autonomie)
Turing hört Vorlesungen u.a. von *Courant, Born* und *Schrödinger* (prominente deutsche Mathematiker und Physiker, die in den 30er Jahren durch den Nationalsozialismus aus Deutschland vertrieben wurden) und G.H. Hardy (Sadleirian chair).

Er liest *Mathematische Grundlagen der Quantenmechanik* von *John von Neumann* und fand es höchst interessant, weil „ ... von Neumann sich dem Gegenstand seiner Untersuchung soweit wie möglich durch logisches Denken näherte. Denn Wissenschaft war für Alan Turing selbständiges Denken und Sehen und nicht eine Ansammlung von Fakten. Wissenschaft war das Zweifeln an Axiomen. Sein Zugang zum Thema war der des reinen Mathematikers, der dem Denken frei die Zügel schießen läßt und erst nachträglich sieht, ob es zu einer Anwendung auf die physikalische Welt führt oder nicht.“ (Hodges, S. 93)

1933 tritt er dem Anti-War-Council bei, einer Vereinigung von Pazifisten, Kommunisten und Internationalisten gegen einen „nationalen Krieg“. Er beginnt *New Statesman* zu lesen und sich ein wenig mit politischen und wirtschaftlichen Fragen zu beschäftigen. „Seine Idee von der Gesellschaft war jedoch die eines Aggregats von Individuen, viel näher den Ansichten eines demokratischen Individualismus, vertreten von J.S.Mill, als jenen des Sozialismus. Sein Ideal war es, ein intaktes individuelles Selbst zu bewahren, autark und immun gegen Kompromiß oder Heuchelei.“ (Hodges, S. 87)

Er liest *Samuel Butler: Erewhon* und *G.B. Shaw: Back to Methuselah*.
„... Shaw wollte echte Charaktere auf die Bühne bringen, solche, die nicht nach ´gebräuchlichen Moralvorstellungen`, sondern nach innerer Überzeugung lebten. Aber er stellte auch harte Fragen darüber, welche Gesellschaft Raum hätte für solche wahren Individuen: Fragen, die großen Bezug hatten zu dem jungen Alan Turing.“ (Hodges, S. 87)

„ Die Quantenmechanik war ein schönes Beispiel dafür, wie sich die Erweiterung und Befreiung der Mathematik um ihrer selbst willen für die Physik bezahlt gemacht hatte. Es hatte sich als notwendig herausgestellt, eine Theorie von Zuständen und nicht von Zahlen und Meßgrößen zu entwerfen – und der ´Hilbert-Raum´ bot für diese genau den richtigen Symbolismus.“ (Hodges, S. 95)

„ In der Beschäftigung mit der Beziehung zwischen Mathematik und Naturwissenschaft begann Alan Turing, sich mit einem verwirrenden, schwierigen und für ihn persönlich bedeutsamen Aspekt des neuen Denkens auseinanderzusetzen.“ (Hodges, S. 95)

„ Die Bewegung in Richtung Abstraktion hatte andererseits so etwas wie eine Krise innerhalb der reinen Mathematik hervorgerufen. Wenn man sie sich als ein Spiel vorzustellen hatte, das beliebigen Regeln folgt, um das Spiel der Symbole zu lenken, was war dabei mit der Auffassung von absoluter Wahrheit geschehen? Im März 1933 erwarb Alan *Bertrand Russels* Buch *Introduction to Mathematical Philosophy*, das dieser zentralen Fragestellung gewidmet war. “ (Hodges, S. 96)

Ende Februar 1934 war ihm ein Beweis des zentralen Grenzwertsatzes gelungen. Dieser war jedoch bereits 1922 von dem Mathematiker Lindeberg bewiesen worden. „ Bei seiner eigenständigen Arbeitsweise hatte er nicht daran gedacht, zuerst einmal herauszufinden, ob sein Ziel schon erreicht worden war. Er wurde aber daraufhingewiesen, daß es dennoch mit einer entsprechenden Erklärung als eigenständige Arbeit für ein King´s Fellowship akzeptiert werden könnte.“ (Hodges, S. 103)

Ende Mai 1934 besteht Turing mit Auszeichnung seine Prüfungen. Ihm wird vom King´s ein Forschungsstipendium zuerkannt. Am Tag nach den Feierlichkeiten geht er mit einem Bekannten auf eine Fahrradtour nach Deutschland. Er fährt mit dem Zug bis Köln und von dort in einigen Tagen nach Göttingen, wo er eine Autorität der Mathematik konsultiert. Sie erleben den „Röhm-Vorfall“ der Hitler endgültig zur absoluten Macht verhilft. (Hodges, S. 105)

„ Bei manchen Studenten aus Cambridge mochte ein Blick auf das neue Deutschland und eine Berührung mit seinen Rohheiten ein großes antifaschistisches Engagement hervorrufen. Dieser Schritt kam für Alan Turing nicht in Frage. Er betrachtete die antifaschistische Sache immer mit Sympathie, aber nichts konnte ihn zu einem ´politischen` Menschen machen. Er hatte einen anderen Weg in die Freiheit gewählt; jenen der Hingabe an sein Handwerk. Sollten andere tun, was sie konnten; er würde etwas Richtiges, etwas Wahres erreichen. Er würde die Kultur fortführen, welche die Antifaschisten verteidigten.“ (Hodges, S. 106)

Im Sommer und Herbst 1934 arbeitet Turing an seiner Fellowship-Dissertation und legt sie einen Monat vor dem spätesten Abgabetermin (6. Dezember) vor. Der Titel der Arbeit war: On the Gaussian Error Function. Sie blieb unveröffentlicht, das Original-Typoscript befindet sich im KCC (Archiv in der Bibliothek des King´s College, Cambridge).

Am 16. März 1935 wird Turing durch Keynes, Pigou u.a. zum Fellow gewählt. „Die Jungen der Sherborne School kamen in den Genuß eines halben schulfreien Tages und ein Vierzeiler machte die Runde:

Turing
must have been alluring
to get made a don
so early on*

*Turing muß betörend gewesen sein, um schon so früh zum Don gemacht zu werden.“

... „ Fellow zu sein brachte 300 Pfund pro Jahr mit sich für einen Zeitraum von 3 Jahren, der normalerweise auf 6 Jahre verlängert wurde, und es gab keine Verpflichtungen. Er hatte ein Anrecht auf Unterkunft und Verpflegung, wenn er sich in Cambridge aufhalten wollte, und darauf, am Dozententisch zu speisen.“ (Hodges, S. 111)

„Die Wahl fiel zeitlich mit einer, von Alan so genannten `Entdeckung kleineren Maßstabs` zusammen, die seine erste veröffentlichungswürdige Arbeit bildete. Es handelte sich um ein ordentliches Resultat in der Gruppentheorie. ... Die Arbeit wurde eingereicht und später im selben Monat von der London Mathematical Society publiziert. Das Resultat war eine kleine Verbesserung einer Arbeit von Neumanns, die die Theorie der `fast periodischen Funktionen` durch deren Definition mit Bezug auf `Gruppen` entwickelte. Wie es der Zufall wollte, kam von Neumann im Verlauf dieses Monats nach Cambridge. Er verbrachte einen Sommer außerhalb von Princeton und hielt eine Vorlesungsreihe in Cambridge über das Thema der `fast periodischen Funktionen`. Alan traf ihn mit Sicherheit während des Trimesters, höchstwahrscheinlich infolge seiner Teilnahme an dem Kurs.“ (Hodges, S. 111, 112)

„John von Neumann war einer der bedeutendsten Mathematiker des 20. Jahrhunderts. Er war ein Mann, der intellektuellen mit finanziellem Erfolg ergänzte. Sein Auftreten war gebieterisch, er hatte einen pikanten Humor, eine Ausbildung als Ingenieur, umfassende Kenntnisse der Geschichte – und ein Gehalt von mehr als 10.000 Dollar, zusätzlich zu seinen beträchtlichen privaten Einkünften. Er war eine völlig andere Erscheinung als der zweiundzwanzigjährige Turing in seinem schäbigen Sportsakko, bei dem die Schärfe des Verstandes mit Schüchternheit und einer stockenden Sprechweise einherging, die schon mit einer Sprache Schwierigkeiten hatte – ganz zu schweigen von deren vier. Aber für die Mathematik spielte das keine Rolle, und es könnte durchaus das Resultat eines Treffens verwandter Geister gewesen sein, daß Alan am 24. Mai nach Hause schrieb: `... ich habe mich für das nächste Jahr um ein Gaststipendium für Princeton beworben.` “ (Hodges, S. 112)

„Es zeichnete sich jedenfalls immer deutlicher ab, daß Princeton das neue Göttingen war; ein Strom erstklassiger Mathematiker und Physiker floß hin und her über den Atlantik. Es war ein Aspekt der anhaltenden Verlagerung der Macht von Europa und insbesondere von Deutschland nach Amerika. Keiner, der wie Alan *etwas tun* wollte, konnte in Zukunft die Vereinigten Staaten ignorieren.“ (Hodges, S. 112, 113)

„Alan hatte nämlich etwas Neues entdeckt, etwas, das im Zentrum der Mathematik lag, etwas in seinem eigenen Zentrum. Es verdankte seinem Studiengang, dem Tripos, so gut wie gar nichts und beruhte lediglich auf dem, was überall zu finden war. Es war von vollkommener Alltäglichkeit und führte doch zu einer spektakulären Idee. ... Später erzählte er, es sei ihm auf einer Wiese bei Grantchester liegend klar geworden, wie Hilberts dritte Frage zu beantworten sei. Es muß im Frühsommer des Jahres 1935 gewesen sein. `Durch ein mechanisches Verfahren`, hatte Newman [einer seiner akademischen Lehrer] gesagt, und so träumte Alan Turing von Maschinen.“ (Hodges, S. 113)

„Fast an demselben Tag, an dem Alan seine Entdeckung Newmann verkündete, führte ein anderer den Nachweis zu Ende, daß das Hilbertsche Entscheidungsproblem unlösbar war. Das geschah in Princeton, wo der amerikanische Logiker Alonzo Church seinen Beweis am 15. April 1936 zur Publikation druckfertig gemacht hatte. Churchs entscheidende Idee, die Existenz eines ´unlösbaren Problems` nachzuweisen, war schon ein Jahr zuvor verkündet worden, aber erst zu diesem Zeitpunkt brachte er sie genau in die Form einer Antwort auf Hilberts Frage. Zwei Menschen waren gleichzeitig und unabhängig voneinander auf eine neue Idee gekommen. Zunächst war dies in Cambridge nicht bekannt ...“ (Hodges, S. 131)

„Doch was Church getan hatte, war etwas ganz anderes und in einem gewissen Sinn schwächer. Er hatte einen Formalismus entwickelt, der Lambda-Kalkül genannt wurde, und hatte – zusammen mit dem Logiker Stephen Kleene – entdeckt, daß dieser Formalismus dazu verwendet werden konnte, alle Formeln der Arithmetik in eine Standardform zu bringen. ...

Church lieferte verbale Argumente für die Behauptung, daß jedes ´effektive` Berechnungsverfahren als eine Formel des Lambda-Kalküls dargestellt werden könnte. Turings Konstruktion hingegen war direkter und lieferte eine von Grundprinzipien ausgehende Begründung, wodurch die Lücke in Chuchs Darlegung geschlossen wurde.“ (Hodges, S. 132)

Die Arbeit von Turing wurde am 28. Mai 1936 bei der London Mathematical Society zur Veröffentlichung in deren Proceedings eingereicht, jedoch konnte in England niemand die Arbeit begutachten. Es war tatsächlich nur Church, der dies sinnvollerweise hätte tun können, aus diesem Grund schrieb Newmann auch an ihn und bat ihn auch, sich für einen Aufenthalt von Turing in Princeton zu verwenden. Turing schreibt an seine Mutter, daß er den „ziemlich sicheren Entschluß“ gefaßt habe, nach Princeton zu gehen.

„Wenn er konventioneller gearbeitet hätte, hätte er sich nicht an das Hilbertsche Problem herangewagt, ohne vorher die gesamte Literatur dazu gelesen zu haben, einschließlich der Arbeiten von Church. Dann wäre ihm vielleicht niemand zuvorgekommen – aber dann hätte er vielleicht nie die neue Idee von der logischen Maschine mit ihrer Simulation von ´Denkzuständen` kreiert, die nicht nur das Hilbertsche Problem zum Abschluß brachte, sondern völlig neue Fragestellungen eröffnete. Das waren die Vor- und Nachteile des Arbeitens als ein ´eingefleischter Einzelgänger`, wie Newmann es nannte. Sowohl im Fall des Zentralen Grenzwertsatzes als auch beim Entscheidungsproblem war er der Kapitän Scott der Mathematik gewesen, der an großartiger zweiter Stelle lag. Und obwohl er selbst Mathematik und Wissenschaft sicher nicht als ein Spiel mit Gewinnern und Verlierern betrachtete, so war dies doch offensichtlich eine Enttäuschung. Es bedeutete Monate der Verzögerung und verschleierte die Originalität seiner eigenen Vorgehensweise. Es beeinträchtigte den Moment seines ersten Auftretens in der Welt.“ (Hodges, S. 134, 135)

Am 23. September 1936 schifft sich Turing in Southhampton nach Amerika ein, am 29. September kommt er in New York an und erreicht Princeton am Abend mit dem Zug.

Im Oktober schreibt er nach Hause: „Die mathematische Abteilung hier erfüllt voll die Erwartungen. Eine große Zahl der bedeutendsten Mathematiker ist hier. J.v. Neumann, Weyl, Courant, Hardy, Einstein, Lefschetz sowie Schwärme kleinerer Fische. Unglücklicherweise sind nicht annähernd so viele Leute aus der Logik hier wie im letzten Jahr. Church ist natürlich hier, aber Gödel, Kleene, Rosser und Bernays, die im letzten Jahr hier waren, sind weggegangen.“ (Hodges, S. 138)

Über seine Begegnungen mit Church schreibt Turing: „ Ich habe Church zwei- oder dreimal gesehen und ich komme mit ihm sehr gut aus. Er scheint von meiner Arbeit recht angetan zu sein und glaubt, daß sie ihm helfen wird, ein Arbeitsprogramm durchzuführen, an das er zur Zeit denkt. „ (Hodges, S. 140)

Gewissenhaft besucht er Churchs schwerfällige und mühsame Vorlesungen und macht sich Notizen von Chuchs Typentheorie, was sein anhaltendes Interesse an diesem Aspekt der Mathematischen Logik widerspiegelt. In einem Brief an seine Mutter gibt er einen ersten Hinweis bezüglich seines Interesses an der Kryptographie. Er entwickelt dazu Ideen und denkt, daß er sie ´für eine recht beträchtliche Summe an die Regeierung seiner Majestät` verkaufen könnte, bezweifelt aber die Moralität solcher Handlungen. „Wenn Alan nun so etwas wie einen ´kriegsartigen Zweck` im Spiel der Zeichen entdeckt hatte, dann sah er sich, zumindest in Ansätzen, mit dem Dilemma des Mathematikers konfrontiert. Hinter den beiläufigen, scherzhaften Zeilen an seine Mutter lag eine ernsthafte Frage.“ (Hodges, S. 142, 143)

Dazu bemerkte G.H.Hardy: „Es sind die langweiligen und elementaren Teile der angewandten Mathematik, so wie es auch die langweiligen und elementaren Teile der reinen Mathematik sind, die für Gut oder Böse arbeiten.“ (Hodges, S. 142)

Der Bezug zur universellen Maschine ist offensichtlich: „Verschlüsselung wäre ein sehr gutes Beispiel für ein auf Zeichen angewandtes ´genau festgelegtes Verfahren`, etwas, das von einer Turing-Maschine gemacht werden könnte. Es wäre für die Natur einer Verschlüsselung essentiell, daß der Verschlüsselnde sich wie eine Maschine verhielte, in Übereinstimmung mit den jeweils im voraus mit dem Empfänger der Nachricht vereinbarten Regeln.“ (Hodges, S. 141)

Turing erhält die Druckfahnen seiner Arbeit aus der Heimat zugeschickt, Church bietet ihm an, darüber eine Vorlesung abzuhalten. Ein erster Vortrag im Maths Club ist jedoch sehr schlecht besucht, eine Enttäuschung für Alan. Auch nach Veröffentlichung im Druck im Januar 1937 gibt es wenig Reaktionen. „Church rezensierte die Arbeit für das Journal of Symbolic Logic und brachte damit die Bezeichnung ´Turing-Maschine` in eine veröffentlichte Form. Aber nur zwei Personen baten um Separata?: Richard Braithwaite vom King´s College und Heinrich Scholz aus Münster.“ Von von Neumann hätte Alan ein paar Bemerkungen erwarten können, es kamen aber keine.

Mathematische Logik schien in den Augen vieler Mathematiker eher ein marginales Forschungsgebiet zu sein und es gab weitere Gründe, warum sich angewandte Mathematiker nicht mit Turings Arbeit beschäftigten: „Der Text fing interessant an, verlief sich aber bald (in typischer Turing-Manier) in einem Dickicht obskurer deutscher gotischer Lettern, wenn es darum ging, seine Instruktionstabellen für die universelle Maschine zu entwickeln.“ (Hodges, S. 146)

Ein weiterer Wissenschaftler, Emil Post, polnisch-amerikanischer Mathematiker am City College von New York hatte einige von Gödels und Turings Ideen in unveröffentlichter Form vorweggenommen. ... „Selbst wenn es Alan Turing also nicht gegeben hätte, seine Idee wäre bald in der einen oder anderen Form aufgetaucht. Das mußte so sein. Es war die notwendige Brücke zwischen der Welt der Logik und der Welt, in der Menschen handelten.“ (Hodges, S. 147, 148)

Anfang Februar 1937 verschickt Alan Separatdrucke seiner Arbeit an einige gute Freunde u.a. auch James Atkins, demgegenüber er auf ziemlich distanzierte Weise schilderte, „ ... daß er sogar an einen Plan gedacht habe, um seinem Leben ein Ende zu setzen. Darin spielten ein Apfel und elektrische Kabel eine Rolle. Vielleicht war das ein Fall von Depression nach dem Triumph; die Arbeit an *On Computable Numbers* wäre eine Liebesaffäre gewesen, die jetzt bis auf das Wegkehren der Scherben vorbei war.“ (Hodges, S. 152)

Der Dekan Eisenhart deutet die Möglichkeit für Alan an, das ´Procter-Stipendium` zu erhalten und ein weiteres Jahr in Princeton zu bleiben, Turing ist jedoch nicht besonders davon angetan. Stattdessen bewirbt er sich um eine Dozentur in Cambridge, die effektiv eine permanente Unterkunft in Cambridge bedeutet hätte, also die Lösung seiner Lebensprobleme und außerdem die fällige Anerkennung seiner Leistungen. Er erhält jedoch keine Berufung nach Cambridge sondern eine Ermutigung zu bleiben. Er bleibt und beschließt den Doktorgrad (PhD) zu erwerben. John von Neumann unterstützt Turing in Bezug auf das Procter-Stipendium durch Empfehlungsschreiben an den Vizekanzler, erwähnt jedoch nur die kleineren Arbeiten Turings, nicht jedoch *On Computable Numbers*. „Es wäre typisch für das, was als sein Mangel an praktischer Vernunft angesehen wurde, wenn er [Turing] zu

schüchtern gewesen sein sollte, dem ´Oberhäuptling` [von Neumann] seine Arbeit aufzudrängen.“ (Hodges, S. 154, 155)

Den Sommer verbringt er in Cambridge und arbeitet dort an der Verbesserung seiner Arbeit (Bernays hatte einige Fehler darin entdeckt) und an einem Beweis der Tatsache, daß seine eigene „Berechenbarkeit“ genau mit Churchs „effektiver Berechenbarkeit“ übereinstimmte. Eine dritte Definition derselben Art von Idee bestand in jener Zeit in der Idee der „rekursiven Funktion“, wodurch eine vollständige Präzisierung der des Konzepts der Definition einer mathematischen Funktion mittels anderer elementarer Funktionen erreicht wurde. Die Idee ging von Gödel aus und war implizit in seinem Beweis der Unvollständigkeit der Arithmetik enthalten. Es hatte sich aber herausgestellt, daß die allgemeine rekursive Funktion der berechenbaren genau entsprach. „Damit stellten sich Churchs Lambda-Kalkül und Gödels Methode der Definition arithmetischer Funktionen beide als gegenüber der Turing-Maschine gleichwertig heraus. Gödel selbst bestätigte später, daß das Konzept der Turing-Maschine die befriedigendste Definition eines ´mechanischen Verfahrens` sei. Zu der Zeit war es eine sehr erstaunliche und überraschende Tatsache, daß drei unabhängige Auffassungen von der Idee, etwas auf genau festgelegte Weise zu tun, in äquivaltenten Begriffen konvergiert waren.“ (Hodges, S. 156)

Im Sommer 1937 wird Turing in Cambridge durch einen King´s Fellow mit dem Philosophen Ludwig Wittgenstein bekanntgemacht, der wie auch Bertrand Russel eine Kopie von *On Computable Numbers* erhalten hatte.

Im Herbst 1937 entwirft Turing einen elektrischen Multiplizierer und baut die ersten drei oder vier Stufen, um ihn zum Laufen zu bringen. Er verwendet relaisbetriebene Schalter. Neu daran war, daß mit Binärzahlen gerechnet wurde, wie er sie schon in seiner Arbeit verwendet hatte und die Anwendung Boole´scher Algebra zur Minimierung der Anzahl der Elementaroperationen. „Als Übung auf dem Papier hätte das große Ähnlichkeit mit dem Entwurf einer ´Turing-Maschine` für dasselbe Problem gehabt. Aber um es in einer funktionierenden Maschinerie zu realisieren, bedurfte es einiger Mittel zur Einstellung verschiedener physischer ´Konfigurationen`. Dies wurde durch Schalter erreicht, denn das entscheidende an einem Schalter war ja, daß er in einem von zwei Zuständen sein konnte, ´Ein` oder ´Aus`, ´0` oder ´1`, ´wahr` oder ´falsch`. Die von ihm verwendeten Schalter wurden von Relais betrieben; und damit spielte zum ersten Mal Elektrizität eine direkte Rolle bei seinem Drang nach der Verbindung logischer Ideen mit etwas, das physikalisch funktionierte.“ (Hodges, S. 163)

„ Es war 1937 nicht geläufig, daß sich die logischen Eigenschaften von Kombinationen von Schaltern durch Boole´sche Algebra oder durch binäre Arithmetik darstellen ließen, aber für einen Logiker war es nicht schwer, das zu sehen. ... Turing-Maschinen erwachten zum Leben, denn die ersten Stufen seiner Relaismultipliziermaschine *funktionierten* tatsächlich.“ (Hodges, S. 164)

Im Frühjahr 1938 wollte Turing nach England zurückkehren unter der Voraussetzung, daß sein Fellowship erneuert werden würde. Sein Vater empfahl ihm jedoch brieflich, sich eine Stelle in den USA zu suchen. Aus irgendwelchen Gründen ließ sich das King´s College Zeit ihn über die Verlängerung in Kenntnis zu setzen. Alan fragte den Dekan Eisenhart nach einer Stelle, dieser wollte sich das auch merken. Dann bot ihm John von Neumann eine Forschungsassistentenstelle am IAS an. „ ... der ideale Start für die amerikanische akademische Laufbahn ... “ Alan schreibt am 17. Mai an seine Mutter: „ ´Ich bekam hier eine Stelle angeboten als von Neumanns Assistent mit 1500 Dollar pro Jahr, entschied mich aber, sie nicht zu nehmen.` Er hatte nämlich mit dem King´s telefoniert, um festzustellen ob das

Fellowship erneuert worden war, und da dies der Fall war, war seine Entscheidung klar.“ (Hodges, S. 169)

„Zunächst kommen wir zu dem Engländer Alan Turing, der seine Dissertation an der Universität Princeton schrieb. Dort wurde er mit von Neumann bekannt, der Turing so sehr schätzte, daß er ihn als Assistent für das Studienjahr 1938/39 einlud. Turing entschied jedoch, daß es für ihn wichtiger sei, nach England zurückzukehren und dort im Außenministerium eine Stelle anzunehmen, um so gegen die Nazis zu kämpfen, die die freie Welt bedrohten“ (Legendi, Szentivanyi: S. 48)

Am 17. Mai reicht er schließlich seine Dissertation ein, am 31. Mai gab es eine mündliche Prüfung die von Church, Lefschetz und H.F.Bohnenblust durchgeführt wurde. Er besteht eine exzellente Prüfung nicht nur auf dem Spezialgebiet der Mathematischen Logik sondern auch auf anderen Gebieten der Mathematik und in wissenschaftlichen Französisch und Deutsch. Absurd war, daß er gleichzeitig eine Doktorarbeit aus Cambridge begutachtete. Der Doktorgrad (PhD) wurde ihm am 21. Juni zuerkannt, er machte jedoch wenig Gebrauch von dem Titel, für den es in Cambridge keine Anwendung gab. Am 18. Juli kehrt er nach England zurück. (Hodges, S. 170, 171)

Das Enigma

Einige Begriffe
Code – gewöhnliche Verfahren der Textübermittlung, geheim oder nicht
Chiffre – für Dritte unverständliche Übermittlungsform
Kryptographie – Kunst des Schreibens in Chiffren
Kryptoanalyse – Entzifferung dessen, was in Chiffren verborgen wurde
Kryptologie – umfaßt sowohl das Aufstellen als auch das Entschlüsseln von Chiffren
GC CS – Government Code and Cypher School
Enigma – griechisches Wort für Rätsel, gleichzeitig Bezeichnung für die deutsche Verschlüsselungsmaschine in der Zeit des Nationalsozialismus

Alan hatte sich nicht getäuscht, die Regierung Seiner Majestät hatte mit Codes und Chiffren zu tun. Zunächst wurden Zivilisten aus Schulen und Universitäten rekrutiert, die im Auftrag der Marine an Hand eines deutschen Codebuches eine Vielzahl von Meldungen entschlüsselte (seit 1914). Ab 1922 kamen diese Aktivitäten zum Foreign Office, wurden dort dem Geheimdienst (Secret Service, auch SIS oder MI6 genannt) zugeschlagen und in GC CS umbenannt. Sie entschlüsselten russische, italienische und japanische Meldungen aber gegen Deutschland waren sie nicht mehr so erfolgreich. „Die Jahre nach dem ersten Weltkrieg waren die ´goldene Ära des modernen diplomatischen Codebrechens` genannt worden. Aber jetzt stellte die deutsche Nachrichtenübermittlung die GC and CS vor ein Problem, das ihre Möglichkeiten überstieg – die Enigma-Maschine.“ (Hodges, S. 173)

„Die Enigma-Maschine war das zentrale Problem, mit dem sich der britische Geheimdienst 1938 konfrontiert sah. Doch er hielt es für unlösbar. Innerhalb des existierenden Systems war es das vielleicht tatsächlich. Denn in dieser Abteilung von Altphilologen ... gabe es keinen Mathematiker.“ (Hodges, S. 173)

Es wurden Pläne gemacht, im Kriegsfalle etwa 60 Kryptoanalytiker einzustellen, darunter auch Alan Turing. Wahrscheinlich wurde er von einem seiner älteren Dons dem Leiter der GC and CS Alistair Denniston zur Mitarbeit empfohlen. Unmittelbar nach seiner Rückkehr im Sommer 1938 wurde er zu einem Lehrgang in das Hauptquartier der GC and CS mitgenommen. Daraufhin entschloß er sich, für die Regierung zu arbeiten. „Bei allem Mißtrauen gegen die ´Regierung SM` muß es aufregend gewesen sein, hinter die Kulissen sehen zu dürfen. Aber es bedeutete, daß er mit dem Versprechen, die Geheimnisse der Regierung zu wahren, zum ersten Mal einen Teil seines Denkens preisgegeben hatte.“ (Hodges, S. 174)

Universitätsleben

Der Film *Schneewittchen und die sieben Zwerge* kam im Oktober nach Cambridge und Alan sah ihn sich an. „Er war sehr von der Szene angetan, in der die böse Hexe einen an einem Faden baumelnden Apfel in ein kochendes Giftbräu tauchte und murmelte:

Dip the apple in the brew
Let the Sleeping Death seep through*

*Tauch den Apfel ins Gebräu / laß den Schlaftod einziehen.

Es gefiel ihm, das prophetische Verspaar wieder und immer wieder zu singen.“ (Hodges, S. 174, 175)

An der Fakultät hält Alan eine Vorlesung über Grundlagen der Mathematik und fertigt verschiedene Gutachten an. Er schafft sich so eine kleine Nische für sich. Er unterstützt einen jüdischen Jungen einer Flüchtlingsfamilie, damit dieser eine Ausbildung bekommt. Nebenbei arbeitet er auch am King´s (unter besonderer Geheimhaltung) bereits an der Entschlüsselung der Enigma, ohne jedoch sehr weit zu kommen.

„Zur gleichen Zeit nahm Alan an Wittgensteins Klasse über Grundlagen der Mathematik teil, und obwohl diese denselben Titel wie Alans Kurs trug, war sie doch davon völlig verschieden. Turings Kurs handelte von dem Schachspiel der mathematischen Logik, dem Auswählen der übersichtlichsten und minimalsten Menge von Axiomen, von denen auszugehen war, und davon, sie – gemäß dem exakten System von Regeln – zur Entfaltung in die Strukturen der Mathematik zu bringen und die technischen Beschränkungen dieses Verfahrens zu entdecken. Wittgensteins Kurs dagegen war über die *Philosophie* der Mathematik, darüber, was Mathematik *wirklich war*." (Hodges, S. 178)

„Beide [Turing und Wittgenstein] waren schroff und leger in ihrer spartanischen und krawattenlosen Erscheinung ... und sie waren einander ziemlich ähnlich in ihrer Intensität und Ernsthaftigkeit. Keiner von beiden ließ sich durch seine offizielle Stellung definieren. (Wittgenstein, der damals fünfzig war, war gerade zum Professor der Philosophie in der Nachfolge von G.E.Moore ernannt worden). Sie waren einzigartige Individuen, die sich ihre eigenen geistigen Welten schufen. Sie interessierten sich beide nur für grundlegende Fragen, auch wenn sie dabei verschiedene Richtungen einschlugen." (Hodges, S. 179)

Turing arbeitet weiter an der Berechnung von Nullstellen der Riemannschen Zeta-Funktion (Hilberts viertes Problem) und beanträgt bei der Royal Society Mittel zum Bau einer speziellen Berechnungsmaschine. Diese werden auch bewilligt.

„Ein derartiger räuberischer Vorstoß in die praktische Welt lief Gefahr, zum Gegenstand gönnerhafter Witze innerhalb der akademischen Kreise zu werden. Für Alan Turing selbst war die Maschine Symptom für etwas, das nicht durch Mathematik allein zu beantworten war. Er arbeitete an den zentralen Fragestellungen der der klassischen Zahlentheorie und leistete einen Beitrag dazu, aber das war nicht genug. Die Turing-Maschine, die Ordinallogiken, die Formalisierung von Denkvorgängen, Wittgensteins Untersuchungen, die elektrische Multipliziermaschine und nun diese Aneinanderreihung von Zahnrädern – all das wies auf einen herzustellenden Zusammenhang zwischen dem Abstrakten und dem Physischen hin. Es war nicht Naturwissenschaft, nicht ´angewandte Mathematik`, sondern eine Art angewandter Logik, etwas, das keinen Namen hatte." (Hodges, S. 183, 184)

Kriegsdienst in geheimer Mission

Am 4. September 1939 meldete sich Alan bei der GC and CS, die im August in das viktorianische Landhaus Bletchley Park evakuiert worden war. Alan wohnte in Shenley Brook End, etwa drei Meilen nördlich von Bletchley Park und fuhr jeden Tag mit dem Fahrrad dorthin. Manchmal half er in der Bar seiner Wirtin aus. Nur eine kleine Gruppe von Spezialisten beschäftigte sich mit der Entschlüsselung der Enigma, zu Ihnen gehörte Alan.

„Funktechnik war wurde in der Kriegsführung zu Lande, zu Wasser und in der Luft gebraucht, und ein Funkspruch an einen war eine Botschaft an alle. Deshalb mußten die Meldungen getarnt werden, und nicht nur diese oder jene ´Geheimbotschaft` wie bei Spionen oder Schmugglern, sondern das gesamte Kommunikationssystem. Das bedeutete Fehler,

Einschränkungen und stundenlange mühsame Arbeit an jeder Meldung, aber es gab keine andere Wahl.“ (Hodges, S. 189)

<Auf den Seiten 189ff folgt eine Einführung in die verschiedenen Methoden des Verschlüsselns sowie in die Arbeitsweise der Enigma-Maschine.>

Im Oktober läßt sich Alan für die Dauer des Krieges von seinem Fellowship suspendieren und obwohl seine Lehrveranstaltung über die Grundlagen der Mathematik im Vorlesungsverzeichnis angekündigt worden war, wurde sie nicht gehalten. In Bletchley Park wird der Seekrieg zu Alans besonderem Gebiet, er leitet die Entschlüsselung der Marinemeldungen in Baracke 8. „ Er arbeitete für die Admiralität, welche nur grollend die Marine-Kryptoanalyse an die GC and CS abgetreten hatte. Traditionellerweise erwartete die Royal Navy Autonomie. Man hätte von der Admiralität, der Besitzerin der größten Flotte der Welt, die Fähigkeit erwarten können, ihre Kriegsführung allein zu organisieren. Doch sie hatte gründlich dabei versagt, die Tatsache zu erkennen, daß Seestreitkräfte nicht nur von ihrer Kampfkraft abhingen, sondern von *Information*. Kanonen und Torpedos waren machtlos, wenn sie nicht zur richtigen Zeit am richtigen Ort waren.“ (Hodges, S. 217)

Im Gegensatz dazu waren die Deutschen nicht völlig ahnungslos. Immerhin konnte der B.Dienst (Beobachtungsdienst) seit 1938 eine Anzahl der englischen Meldungen lesen und diese Informationen mit großer Wirkung verwenden. Turing konstruiert die sog. Turing-Bomben (bombas), Maschinen die außerhalb von Bletchley Park stationiert werden und ab Mai 1940 die Entschlüsselungsarbeit übernahmen.

„ ... Es war eine Art Urlaub, sogar von der professionellen Mathematik, denn die hier geforderte Arbeit lag mehr auf der Linie genialer Anwendung elementarer Ideen als in einem Zurückdrängen der Grenzen wissenschaftlicher Erkenntnis.“ (Hodges, S. 224)

„Der Krieg, so hatte Churchill 1930 geschrieben, war ´... komplett verdorben. Es ist alles die Schuld der Demokratie und der Wissenschaft.` Aber dennoch verwendete er die Demokratie und die Wissenschaft, wenn es nötig war, und übersah jene nicht, die die Dechiffrierungen machten. Im Sommer 1941 stattete er Bletchley einen Besuch ab und hielt vor den Kryptoanalytikern, die sich auf dem Gras um ihn versammelt hatten, eine anfeuernde Rede. In Baracke 8 wurde ihm ein sehr nervöser Alan Turing vorgestellt. Der Premierminister pflegte von den Mitarbeitern in Bletchley zu sagen, sie seien ´die Gänse, die die goldenen Eier legen und niemals schnattern.` Alan war die Preisgans.“ (Hodges, S. 238)

Nachkriegszeit

<siehe Kippenhahn, S. 238 – 240>

Postscriptum

„Alan Turings Leichnam wurde am 12. Juni 1954 im Krematorium von Woking eingeäschert. Seine Mutter, sein Bruder und Lyn Newmann wohnten der Zeremonie bei. Die Asche wurde im Garten verstreut, am selben Ort wie die seines Vaters. Es gibt keinen Gedenkstein.“ (Hodges, S. 609)

Exkurs: Das Entscheidungsproblem

Hilbert findet 1899 ein System von Axiomen, von dem er beweisen konnte, das es zu allen Sätzen der euklidischen Geometrie führen würde, brauchte aber dazu die reellen Zahlen. Diese waren 1872 von Dedekind auf die ganzen Zahlen zurückgeführt worden – im technisch mathematischen Sinn also auf die "Arithmetik, so daß Hilbert von sich sagen konnte, er habe nichts weiter getan, als „alles auf die Widerspruchsfreiheit der arithmetischen Axiome zu reduzieren, die unbeantwortet geblieben ist". (Hodges, S. 97)

Hilbert stellte 1900 auf dem internationalen Kongreß der Mathematiker in Paris der mathematischen Welt 23 ungelöste Probleme. Das zweite davon betraf den Beweis der Widerspruchsfreiheit der „Peano-Axiome", von dem wie er gezeigt hatte, die Exaktheit und Strenge der Mathematik abhing. „Widerspruchsfreiheit" war das entscheidende Wort. (Hodges, S. 98)

„Eines der wichtigsten Probleme in der mathematischen Logik war das sogenannte ´Entscheidungsproblem`. Hilbert warf die Frage auf, ob man ein Verfahren finden kann, um zu entscheiden, ob irgendeine gegebene ´sinnvolle` Behauptung, die man mit der üblichen Bezeichnungsweise der symbolischen Logik ausdrückte, beweisbar ist. 1936 bewiesen sowohl Church als auch Turing, daß das nicht möglich ist. (Wir müssen erwähnen, daß dieses Ergebnis sich von Gödels Satz unterscheidet. Gödel zeigte, daß im Formalismus der Principia Behauptungen stecken, die nicht beweisbar sind, aber ihre Negationen ebenfalls nicht.)" (Legendi, Szentivanyi: S. 48)

Gottlob Frege versucht 1884 diese Fragestellung zu behandeln in seinem Buch: *Die Grundlagen der Arithmetik, eine logisch-mathematische Untersuchung über den Begriff der Zahl.* Durch die Einführung der Mengenlehre (Bertrand Russel, 1901) wurden Freges Arbeiten überholt. Russel wollte durch den Begriff der Gleichheit eine Menge-mit-einem-Element definieren, ohne auf den Begriff des Zählens zurückzugreifen. Die Zahl „Eins" wäre dann dadurch zu definieren, daß sie „die Menge aller Mengen-mit-einem-Element" sei. Doch er bemerkte, daß es zu logischen Widersprüchen kam, sobald man versuchte den Begriff „die Menge aller Mengen" zu verwenden.

<siehe Hodges, S. 99 mitte bis S. 100 mitte>

„Die harmlos klingende Forderung nach einem Nachweis dafür, daß die Mathematik ein vollständiges und widerspruchsfreies Ganzes bildet, hatte eine Büchse der Pandora an Problemen geöffnet. Mathematische Aussagen schienen einerseits noch immer so wahr zu sein, wie nur irgend etwas sein konnte; andererseits stellten sie sich nun als bloße Zeichen auf Papier dar, die zu verwirrenden Paradoxen führten, sobald man zu klären versuchte, was sie bedeuteten." (Hodges, S. 100)

<siehe Hodges, S. 100 unten bis S. 101 oben>

„Ende 1933 hatte Alan Turing mit Sicherheit gleich zwei fundamentale Probleme in Angriff genommen. Sowohl in der Quantenphysik als auch in der reinen Mathematik bestand die Aufgabe darin, das Abstrakte und das Physikalische, das Symbolische und das Wirkliche in Bezug zu setzen." (Hodges, S. 101)

<siehe Hodges, S. 107 bis S. 110>

„Hilberts Frage nach der Entscheidbarkeit hatte nichts mit dem Determinismus der Physik, der Chemie oder dem der biologischen Zellen zu tun. Es ging dabei um etwas Abstrakteres, nämlich um die Eigenschaft, im voraus derart festgelegt zu sein, daß es zu nichts Neuem kommen konnte. Außerdem sollten die Operationen auf Symbole und nicht auf Dinge mit einer bestimmten Masse oder chemischen Zusammensetzung anzuwendende Operationen sein.“ (Hodges, S. 113)

<auf den Seiten 113 bis einschließlich S. 130 findet sich eine ausführliche Beschreibung der Turingmaschine, wie AMT sie sich gedacht hat>

Exkurs: Die Arbeit der polnischen Kryptologen

„ ... das Zyklometer reichte nicht mehr aus. Die Polen bauten eine kompliziertere Maschine, der sie den Namen bomba (Bombe) gaben, wobei sie merkwürdigerweise nicht an eine Fliegerbombe dachten ... – sondern an eine Eisbombe. In solch einer bomba simulierten sie sechs Enigmas. Es wurden sechs bombas gebaut, keine ist erhalten geblieben; niemand weiß heute genau, wie die Maschine funktionierte.“ (Kippenhahn, S. 226)

„Am 25. Juli 1939 trafen sich Vertreter der polnischen, britischen und französischen Geheimdienste in Pyry bei Warschau. ... Die Polen übergaben den Alliierten die Ergebnisse ihrer Untersuchungen an der Enigma. Zu dieser Zeit waren die durch fünf Walzen ermöglichten Verschlüsselungen noch nicht gebrochen. Man beschloß, sich die Arbeit zu teilen. Die Polen sollten ihre mathematisch-theoretischen Arbeiten weiterführen, die Franzosen versuchten, über Kontaktleute Informationen aus Deutschland zu beschaffen. Die Briten schließlich übernahmen es, eine große Anzahl von *bombas* zu bauen, um den Code der fünf Walzen zu knacken. Außerdem übergaben die Polen den Franzosen zwei Exemplare ihrer Nachbauten der Enigma.“ (Kippenhahn, S. 226, 227)

Nach dem Überfall Hitlers auf Polen wurde das Chiffrierbüro in Warschau aufgelöst. Drei Mitarbeiter (Rejewski, Rozycki, Zygalski) machen sich auf die Flucht, über Rumänien landen sie zunächst in Paris. Hier arbeiten sie zusammen mit einigen Franzosen weiter an dem Nachbau der Enigmas und der bombas. Mitte Januar 1940 werden sie dort von Alan Turing besucht. Als die deutsche Armee in Frankreich einmarschiert müssen sie wiederum fliehen. Sie versuchen England zu erreichen. „Sie mußten Umwege über Spanien, Portugal und Gibraltar nehmen und wurden immer wieder verhaftet. Nach mehr als 8 Monaten erreichten sie ihr Ziel, schlossen sich der in England aufgestellten polnischen Exilarmee an und wurden beauftragt, Playfair-Chiffrierungen der SS zu entschlüsseln. Es ist nicht ganz klar, warum die beiden genialen Chiffrierexperten nicht auf die wirklich schwierigen Probleme angesetzt wurden. Irgendwie wollten es die Engländer nicht wahrhaben, daß die Polen mit der Enigma-Entschlüsselung so weit fortgeschritten waren. Das neu entstandene englische Projekt ´ULTRA` hatte fortan die Aufgabe, die mit der Enigma chiffrierten Funksprüche zu bearbeiten, und die Polen sind nie in dieses Unternehmen einbezogen worden. Seit August 1939 gab es nördlich von London auf dem Gut Bletchley Park eine große Abteilung mit Tausenden von Mitarbeitern, die damit beschäftigt waren, Enigma-Funksprüche zu entschlüsseln. Davon hat Rejewski erst dreißig Jahre nach dem Kriegsende etwas erfahren.“ (Kippenhahn, S. 230)

„Hier noch einmal die damalige Situation: Die Polen konnten die Funksprüche der Dreiwalzen-Enigma lesen, für die fünf Walzen zur Auswahl standen. Zu diesen waren zwei weitere Walzen hinzugekommen und später noch die Walze Nummer VIII, was die Entschlüsselung immer komplizierter und langwieriger machte. Dann aber änderten die Deutschen auch noch die Übermittlung des Spruchschlüssels. Im Mai 1940 verschwanden die hilfreichen sechs Zeichen am Anfang einer Nachricht. Es wurde immer mühsamer, alle denkbaren Einstellungen der Maschine durchzuprobieren.
Turing konstruierte nun *bombes*, die leistungsfähiger waren als die polnischen *bombas*.
Die diffizilen Apparate der Bomben erforderten Techniker, die sie warteten und reparierten. Man benötigte Funker, die rund um die Uhr in den einschlägigen Frequenzen auf Signale lauerten und die zahllosen Funksprüche aufnahmen. Dann erst konnten die wichtigsten Leute, die Entschlüßler, an ihre Arbeit gehen. Zusammen mit dem Hilfspersonal arbeiteten in Bletchley Park etwa zehntausend Menschen.“ (Kippenhahn, S. 233)

„Die erste von Turing entworfene Bombe wurde im Januar 1940 eingesetzt. ... Ende 1941 standen Bletchley Park zwölf solcher Maschinen zur Verfügung, im März 1943 waren es sechzig. Aber auch dann benötigten die Rechner manchmal bis zu drei Tage rund um die Uhr, um einen Tagesschlüssel zu finden. Im Frühjahr 1940, während des Norwegenfeldzuges der Deutschen, gelangen in Bletchley Park die ersten Entschlüsselungen. Ein Jahr später konnten die Briten schon einen wesentlichen Teil des Enigma-Funkverkehrs mitlesen.“ (Kippenhahn, 236, 237)