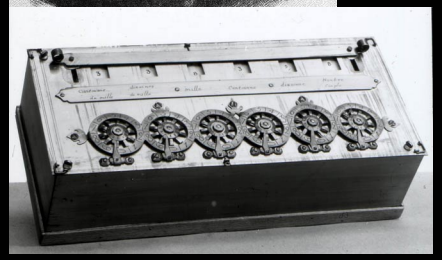
Computation:
The Mathematical Story

Christos H. Papadimitriou
UC Berkeley
Google "christos"

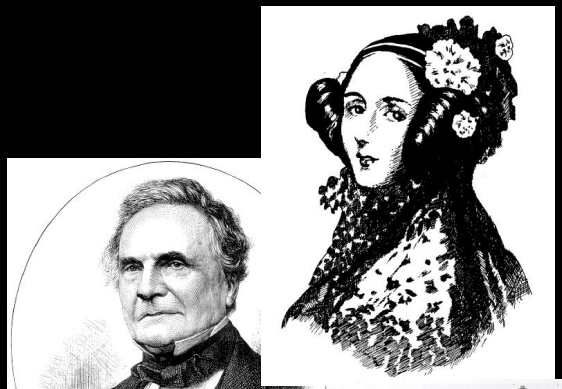
Outline

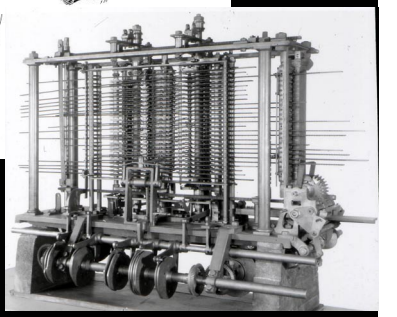
- The Foundational Crisis in Math (1900 – 31)
- How it Led to the Computer (1931 – 46)
- And to P *vs* NP (1946 – 72)

The prehistory of computation

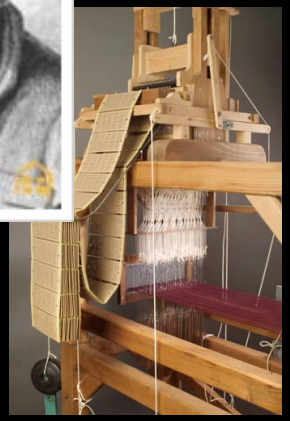


Pascal's Calculator 1650



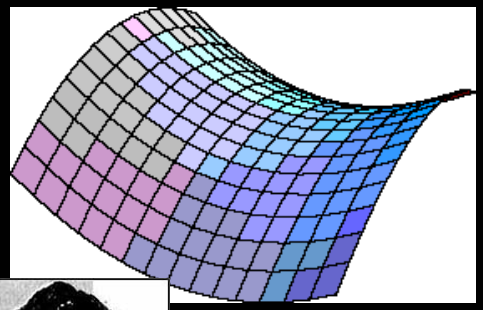


Babbage & Ada, 1850 the analytical engine



Jacquard's looms 1805

Trouble in Math



Non-euclidean geometries

Cantor, 1880: sets and infinity

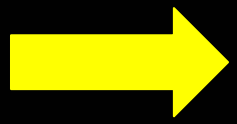
The quest for foundations

Hilbert, 1900:

"We must know,
we can know
we shall know!"

The two quests

An axiomatic system that comprises all of Mathematics



A machine that finds a proof for every theorem

The disaster

Gödel 1931

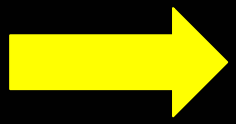
The Incompleteness Theorem

"sometimes, we cannot know"

Theorems that have no proof

Recall the two quests

~~Find an axiomatic system that comprises all of Mathematics~~



Find a machine that finds a proof for every theorem

?

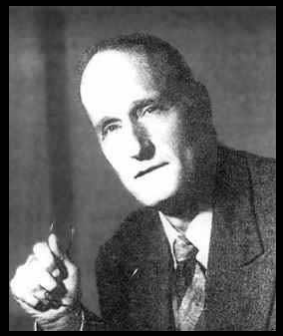
Also impossible?

but what is a machine?

The mathematical machines (1934 – 37)

Post

Church



Kleene

Turing

Universal Turing machine

Powerful and crucial idea
which anticipates software

…and radical too:
dedicated machines
were favored at the time

"If it should turn out that the basic logics of a machine designed for the numerical solution of differential equations coincide with the logics of a machine intended to make bills for a department store, I would regard this as the most amazing coincidence that I have ever encountered"

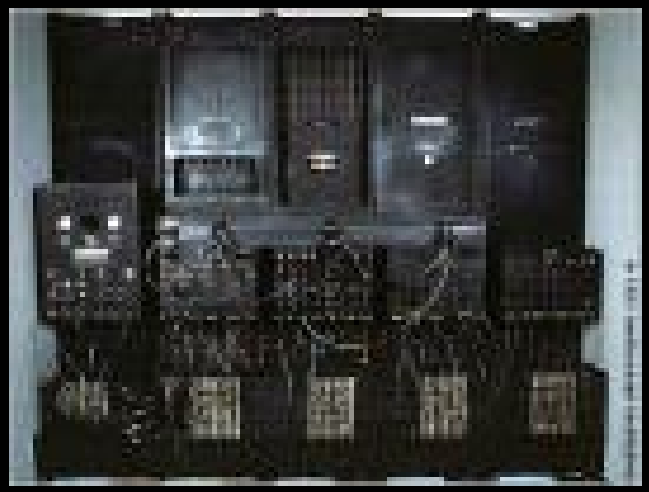
Howard Aiken, 1939

In a world without Turing…

WELCOME TO THE COMPUTER STORE!
First Floor: Web browsers, e-mailers
Second Floor: Database engines, Word processors
Third Floor: Accounting computers, Business machines
Basement: Game engines, Video and Music computers
SPECIAL TODAY: All number crunchers 40% off!

And finally…

von Neumann 1946
EDVAC and report



Johnny come lately

- von Neumann and the Incompleteness Theorem
- *"Turing has done good work on the theories of almost periodic functions and of continuous groups" (1939)*
- Zuse (1936 – 44) , Turing (1941 – 52), Atanasoff/Berry (1937 – 42), Aiken (1939 – 45), etc.
- The meeting at the Aberdeen, MD train station
- The "logicians" *vs* the "engineers" at UPenn
- Eckert, Mauchly, Goldstine, and the ***First Draft***

Madness in their method? the painful human story

G. Cantor

D. Hilbert

E. Post

K. Gödel

J. Von Neumann

A. M. Turing

Theory of Computation since Turing: Efficient algorithms

- Some problems can be solved in ***polynomial time*** (n, n log n, n^2, n^3, etc.)
- Others, like the traveling salesman problem and Boolean satisfiability, apparently cannot (because ***they involve exponential search***)
- Important dichotomy (von Neumann 1952, Edmonds 1965, Cobham 1965, others)

Polynomial algorithms deliver Moore's Law to the world

- A 2^n algorithm for SAT, run for 1 hour:

1956	1966	1976	1986	1996	2006
$n = 15$	$n = 23$	$n = 31$	$n = 38$	$n = 45$	$n = 53$

An n or n log n algorithm	n^3	n^7
× 100 every decade	× 5	× 2

NP-completeness
Cook, Karp, Levin (1971 – 73)

- Efficiently solvable problems: ***P***
- Exponential search: ***NP***
- Many common problems capture the full power of exponential search: ***NP-complete***
- Arguably the most influential concept to come out of Computer Science
- Is P = NP? Fundamental question and mathematical problem

Intellectual debt to Gödel/Turing?

- Negative results are an important intellectual tradition in Computer Science and Logic
- The Incompleteness Theorem and Turing's halting problem are the archetypical negative results
- ***The Gödel letter*** (discovered 1992)

Princeton, 20./III. 1956

Lieber Herr v. Neumann!

Ich habe mit größtem Bedauern von Ihrer Erkrankung gehört. Die Nachricht kam nun ganz unerwartet. Morgenstern hatte mir zwar schon im Sommer von einem Schwächeanfall erzählt den Sie einmal hatten, aber er meinte damals, dass dem keine größere Bedeutung beizumessen sei. Wie ich höre, haben Sie sich in den letzten Monaten einer radikalen Behandlung unterzogen u. ich freue mich, dass diese den gewünschten Erfolg hatte u. es Ihnen jetzt besser geht. Ich hoffe u. wünsche Ihnen, dass Ihr Zustand sich bald noch weiter bessert u. dass die normalen Ermüdungserscheinungen am Morgen, wenn möglich, zu einer vollständigen Heilung führen mögen.

Da Sie sich, wie ich höre, jetzt kräftiger fühlen, möchte ich mir erlauben, Ihnen über ein mathematisches Problem zu schreiben, über das mich ~~Ihre Ansicht~~ K. in unterredung mit: Man kann offenbar leicht eine Turingmaschine konstruieren, welche von jeder Formel F der engeren Funktionenkalküls u. jeder natürl. Zahl n zu entscheiden gestattet ob F einen Beweis der Länge n hat [Länge = Anzahl der Symbole]. Sei $\psi(F,n)$ die Anzahl der Schritte die die Maschine dazu benötigt u. sei $\varphi(n) = \max_F \psi(F,n)$. Die Frage ist, wie rasch $\varphi(n)$ für eine optimale Maschine wächst. Man kann zeigen $\varphi(n) \geq Kn$. Wenn es wirklich eine Maschine mit ~~$\varphi(n) \sim Kn$~~ $\varphi(n) \sim Kn$ (oder auch nur $\sim Kn^2$) gäbe, hätte das Folgerungen von der größten Tragweite. Es würde nämlich offenbar bedeuten, dass man trotz der Unlösbarkeit des Entscheidungsproblems die Denkarbeit der Mathematiker bei ja-oder-nein Fragen vollständig* durch Maschinen ersetzen könnte. ~~(abgesehen~~ Man müsste ja dann das n ja gerade wählen, dass, wenn die Maschine kein Resultat liefert es auch keinen

*abgesehen von der Aufstellung der Axiome

Sie hat über d[as] Problem nachzudenken. Nun scheint es mir aber durchaus im Bereich der Möglichkeit zu liegen, dass $\varphi(n)$ so langsam wächst

Dann 1.) scheint $\varphi(n) \geq Kn$ die einzige Abschätzung zu sein, die man durch eine Verallgemeinerung des Beweises für die Unlösbarkeit des Entscheidungsproblems erhalten kann; 2. bedeutet ja $\varphi(n) \sim Kn$ (oder $\sim Kn^2$) bloss, dass die Anzahl der Schritte gegenüber dem blossen Probieren von N auf $\log N$ (oder $(\log N)^2$) vermindert werden kann. So starke Verminderungen kommen aber bei andern finiten Problemen durchaus vor, z.B. bei der Berechnung eines quadratischen Restsymbols durch wiederholte Anwendung des Reziprozitätsgesetzes. Es wäre interessant zu wissen, wie es damit z.B. bei der Feststellung, ob eine Zahl Primzahl ist, steht u. wie stark im allgemeinen bei finiten kombinatorischen Problemen die Anzahl der Schritte gegenüber dem blossen Probieren vermindert werden kann.

Ich weiss nicht ob Sie gehört haben, dass "Post's problem" (ob es unter den Problemen $(\exists y)\varphi(y,x)$ mit rekursivem φ Grade der Unlösbarkeit gibt) von einem ganz jungen Mann namens Richard Friedberg in positivem Sinn gelöst wurde. Die Lösung ist sehr elegant. Leider will Friedberg nicht Mathematik, sondern Medizin studieren (scheinbar unter dem Einfluss seines Vaters).

Was halten Sie übrigens von den Bestrebungen, die Analysis auf die verzweigte Typentheorie zu begründen, die neuerdings wieder in Schwung gekommen sind? Es ist Ihnen wahrscheinlich bekannt, dass Paul Lorenzen dabei bis zur Theorie der Lebesgueschen Masse vorgedrungen ist. Aber ich glaube, dass in wichtigen Teilen der Analysis nicht eliminierbare imprädikative Schlussweisen vorkommen.

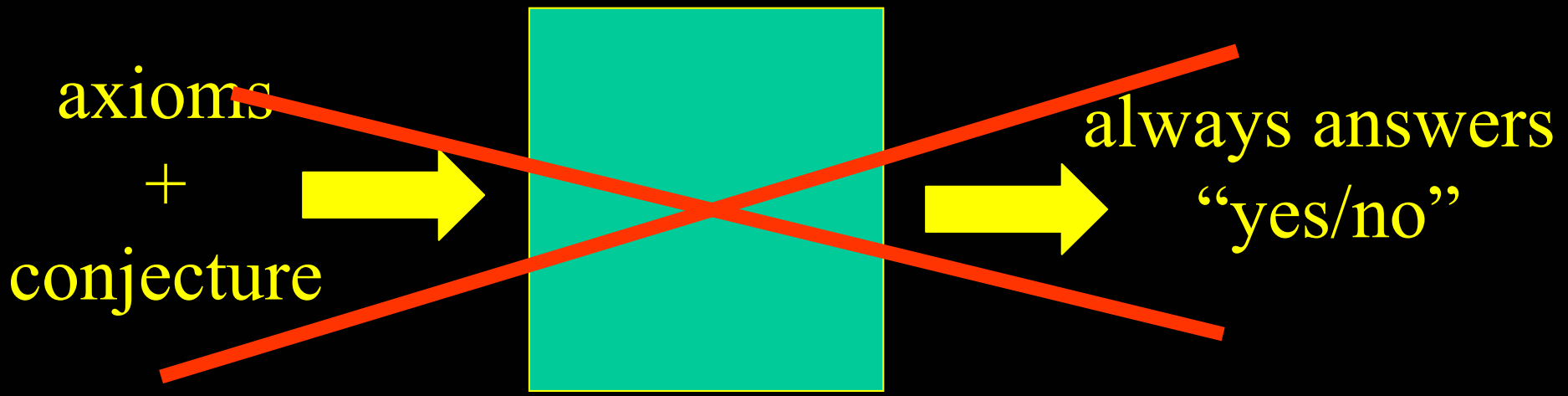
Ich würde mich sehr freuen, von Ihnen persönlich etwas zu hören; u. bitte lassen Sie es mich wissen, wenn ich irgend etwas für Sie tun kann.

Mit besten Grüssen u. Wünschen, auch an Ihre Frau Gemahlin

Ihr sehr ergebener Kurt Gödel

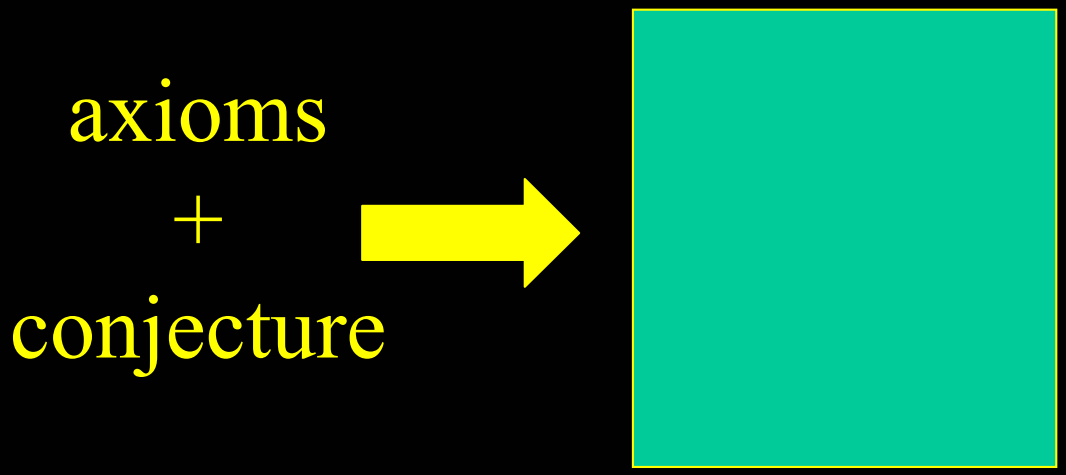
S. Ich gratuliere Ihnen bestens zu den [illegible]

Recall: Hilbert's Quest



Turing's halting problem

Gödel's revision



if there is a proof
of length n
it finds it
in time k^n

(this is trivial,
just try all proofs)

Hilbert's last stand

- Gödel asked von Neumann in the 1956 letter:

"Can this be done in time n ?

n^2 ?

n^c ?"

- This would ***still*** mechanize Mathematics…

Surprise!

- Gödel's question is equivalent to

"P = NP"

- He seems to be optimistic about it…

So…

- Hilbert's foundations quest and the Incompleteness Theorem have started an intellectual Rube Goldberg that eventually led to the computer
- Some of the most important concepts in today's Computer Science, including P *vs* NP, owe a debt to that tradition

And this is the story we tell in…

LOGICOMIX

A graphic novel of reason, madness and the birth of the computer

by…

LOGICOMIX: A graphic novel of reason, madness and the birth of the computer

By Apostolos Doxiadis and Christos Papadimitriou

Art: Alecos Papadatos and Annie Di Donna

Bloomsbury, 2007

Thank you!