

50003

Models of Computation
Imperial College London

Contents

1	Introduction	2
1.1	Course Structure	2
1.2	Algorithms	2
1.3	Decision Problems	4
1.3.1	Hilbert's Entscheidungsproblem	4
1.4	Algorithms	4
1.4.1	Algorithms Informally	4
1.4.2	The Halting Problem	5
1.4.3	Algorithms as Functions	5
1.4.4	Haskell Programs	5
1.5	Program Semantics	6
2	Credit	7

Chapter 1

Introduction

1.1 Course Structure



Dr Azelea Raad



Dr Herbert Wiklicky

First Half

- The while language
- Big & small step semantics
- Structural induction

Second Half

- Register Machines & gadgets
- Turing Machines
- Lambda Calculus

1.2 Algorithms

Euclid's Algorithm

Extra Fun! 1.2.1

Algorithm to find the greatest common divisor published by greek mathematician Euclid in ≈ 300 B.C.

```
-- continually take the modulus and compare until the modulus is zero
euclidGCD :: Int -> Int -> Int
euclidGCD a b
  | b == 0 = a
  | otherwise = euclidGCD b (a `mod` b)
```

Sieve of Eratosthenes

Extra Fun! 1.2.2

Used to find the prime numbers within a limit. Done by starting from the 2, adding the number to the primes, marking all multiples as non-prime, then repeating progressing to the next non-marked number (a prime) and repeating.

The sieve is attributed to Eratosthenes of Cyrene and was first published ≈ 200 B.C.

```
-- Filtering rather than marking elements
eraSieve :: Int -> [Int]
eraSieve lim = eraSieveHelper [2..lim]
  where
    eraSieveHelper :: [Int] -> [Int]
```

```
eraSieveHelper (x:xs) = x:eraSieveHelper (filter (\n -> n `mod` x /= 0) xs)
eraSieveHelper [] = []
```

Al-Khwarizmi

Extra Fun! 1.2.3

A persian polymath who first presented systematic solutions to linear and quadratic equations (by completing the square). He pioneered the treatment of algebra as an independent discipline within mathematics and introduced foundational methods such as the notion of balancing & reducing equal equations (e.g subtract/-cancel the same algebraic term from both sides of an equation)

His book title الجبر "*al-jabr*" resulted in the word *algebra* and subsequently algorithm.

Algorithms predate the computer, and have been studied in a mathematical/logical context for centuries.

- Very early attempts such as the Antikythera Mechanism (an analogue calculator for determining the positions of)
- Simple configurable machines (e.g automatic looms, pianola, census tabulating machines) invented in the 1800s.
- Basic calculation devices such as Charles Babbage's *Difference Engine* further generalised the idea of a calculating machine with a sequence of operations, and rudimentary memory store.
- Babbage's Analytical Engine is generally considered the world's first digital computer design, but was not fully implemented due to the limits of precision engineering at the time.
- English mathematician Ada Lovelace writes the first ever computer program (to calculate bernoulli numbers) on Babbage's analytical engine.

Note G

Extra Fun! 1.2.4

While translating a french transcript of a lecture given by Charles Babbage at the University of Turin on his analytical engine, Ada Lovelace added several notes (A-G), with the last including a description of an algorithm to compute the Bernoulli numbers.

Diagram for the computation by the Engine of the Numbers of Bernoulli. See Note G. (page 722 et seq.)

Number of Operation.	Variables used upon.	Variables receiving results.	Indication of change in the value on any Variable.	Statement of Results.	Data.										Working Variables.												Result Variables.					
					v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}	v_{13}	v_{14}	v_{15}	v_{16}	v_{17}	v_{18}	v_{19}	v_{20}	v_{21}	v_{22}	v_{23}	v_{24}	v_{25}			
					1	2	n																									
1	$\times v_1 \times v_2$	v_4	$v_4 = v_2$	$-2n$		2	n	2n	2n	2n																						
2	$-v_4 - v_1$	v_4	$v_4 = v_4$	$-2n-1$	1																											
3	$+v_4 + v_1$	v_4	$v_4 = v_4$	$-2n+1$	1																											
4	$+v_4 - v_1$	v_{11}	$v_{11} = v_4$	$\frac{2n-1}{2}$				0	0																							
5	$+v_{11} + v_2$	v_{11}	$v_{11} = v_{11}$	$\frac{1}{2} \cdot \frac{2n-1}{2}$		2																										
6	$-v_{11} - v_{11}$	v_{12}	$v_{12} = v_{11}$	$\frac{1}{2} \cdot \frac{2n-1}{2} = A_0$																												
7	$-v_4 - v_1$	v_{10}	$v_{10} = v_4$	$n-1 (=3)$	1		n																									
8	$+v_2 + v_2$	v_7	$v_7 = v_2$	$-2+0=2$		2																										
9	$+v_2 + v_2$	v_{11}	$v_{11} = v_2$	$\frac{2n}{2} = A_1$						2n	2																					
10	$\times v_{12} \times v_{11}$	v_{12}	$v_{12} = v_{11}$	$\frac{2n}{2} = A_1$																												
11	$+v_{12} + v_{12}$	v_{13}	$v_{13} = v_{12}$	$-\frac{1}{2} \cdot \frac{2n-1}{2} + B_1 \cdot \frac{2n}{2}$																												
12	$-v_{12} - v_1$	v_{10}	$v_{10} = v_1$	$n-2 (=2)$	1																											
13	$-v_4 - v_1$	v_7	$v_7 = v_4$	$-2n-1$	1																											
14	$+v_1 + v_2$	v_7	$v_7 = v_2$	$-2+1=3$																												
15	$-v_4 + v_2$	v_6	$v_6 = v_2$	$\frac{2n-1}{2}$																												
16	$\times v_6 \times v_{11}$	v_{11}	$v_{11} = v_6$	$\frac{2n}{2} = A_1$																												
17	$-v_4 - v_1$	v_6	$v_6 = v_4$	$2n-2$	1																											
18	$+v_1 + v_2$	v_7	$v_7 = v_2$	$-3+1=4$																												
19	$+v_2 + v_2$	v_6	$v_6 = v_2$	$\frac{2n-2}{2}$																												
20	$\times v_7 \times v_{11}$	v_{11}	$v_{11} = v_7$	$\frac{2n}{2} = A_1$																												
21	$\times v_{12} \times v_{11}$	v_{12}	$v_{12} = v_{11}$	$\frac{2n}{2} = A_1$																												
22	$+v_{12} + v_{12}$	v_{13}	$v_{13} = v_{12}$	$A_0 + B_1 \cdot A_1 + B_2 \cdot A_2$																												
23	$-v_{12} - v_1$	v_{10}	$v_{10} = v_1$	$n-3 (=1)$	1																											
Here follows a repetition of Operations thirteen to twenty-three.																																
24	$+v_{13} + v_{13}$	v_{13}	$v_{13} = v_{13}$	$n = 4+1=5$																												
25	$+v_1 + v_2$	v_7	$v_7 = v_2$	by a Variable-card.	1		n+1			0	0																					

Babbage's Machines

Extra Fun! 1.2.5

The *Difference Engine* was used as the basis for designing the fully programmable *Analytical Engine*.

- Held back by lack of funds, limitations of precision machining at the time.
- Contains an ALU for arithmetic operations, supports conditional branches and has a memory

- Part of the machine (including a printing mechanism) are on display at the science museum.

1.3 Decision Problems

Formulas

Definition 1.3.1

Well formed logical statements that are a sequence of symbols form a given formal language. e.g $(p \vee q) \wedge i$ is a formula, but $) \vee \wedge ji$ is not.

Given:

- A set S of finite data structures of some kind (e.g formulae in first order logic).
- A property P of elements of S (e.g the property of a formula that it has a proof).

The associated decision procedure is:

Find an algorithm such that for any $s \in S$, if s has property P the algorithm terminates with 1, otherwise with 0.

1.3.1 Hilbert's Entscheidungsproblem

Is there an algorithm which can take any statement in first-order logic, and determine in a finite number of steps if the statement is provable?

First Order Logic/Predicate Logic

Definition 1.3.2

An extension of propositional logic that includes quantifiers (\forall, \exists), equality, function symbols (e.g $\times, \div, +, -$) and structured formulas (predicate functions).

This problem was originally presented in a more ambiguous form, using a logic system more powerful than first-order logic.

'*Entscheidungsproblem*' means 'decision problem'

Many tried to solve the problem, without success. One strategy was to try and disprove that such an algorithm can exist. In order to answer this question properly a formal definition of algorithm was required.

1.4 Algorithms

1.4.1 Algorithms Informally

Common features of Algorithms:

- | | |
|----------------------|---|
| Finite | Description of the procedure in terms of elementary operations. |
| Deterministic | If there is a next step, it is uniquely determined - that is on the same data, the same steps will be made. |
| Terminate? | Procedure may not terminate on some input data, however we can recognize when it terminates and what the result is. |

In 1935/35, Alan Turing (Cambridge) and Church (Princeton) independently gave negative solutions to Hilbert's Entscheidungsproblem (showed such an algorithm could not exist).

1. They gave concrete/precise definitions of what algorithms are (Turing Machines & Lambda Calculus).
2. They regarded algorithms as data, on which other algorithms could act.
3. They reduced the problem to the *Halting problem*.

This work led to the Church-Turing Thesis, that shows everything computable is computed by a Turing Machine. Church's Thesis extended this to show that General Recursive Functions were the same type as those expressed by lambda calculus, and Turing showed that lambda calculus and the Turing machine were equivalent.

Algorithms Formalised

Any formal definition of an algorithm should be:

- Precise** No ambiguities, no implicit assumptions, Should be phrased mathematically.
- Simple** No unnecessary details, only the few axioms required. Makes it easier to reason about.
- General** So all algorithms and types of algorithms are covered.

1.4.2 The Halting Problem

The *Halting problem* is a *decision problem* with:

- The set of all pairs (A, D) such that A is an algorithm, and D is some input datum on which the algorithm operates.
- The property $A(D) \downarrow$ holds for $(A, D) \in S$ if algorithm A when applied to D eventually produces a result (halts).

Turning and Church showed that there is no algorithm such that:

$$\forall (A, D) \in S \left[\begin{array}{ll} H(A, D) & = \quad 1 \quad A(D) \downarrow \\ & 0 \quad \text{otherwise} \end{array} \right]$$

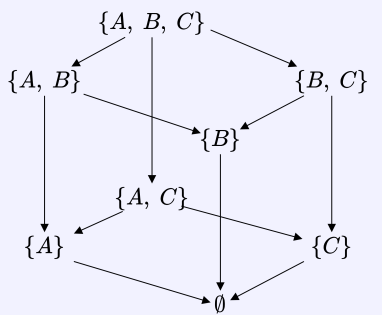
The final step for Turing/Church's proof was to construct an algorithm encoding instances (A, D) of the halting problem as statements such that:

$$\Phi_{A,D} \text{ is provable} \leftrightarrow A(D) \downarrow$$

1.4.3 Algorithms as Functions

It is possible to give a mathematical description of a computable function as a special function between special sets.

In the 1960s Strachey & Scott (Oxford) introduced *denotational semantics*, which describes the meaning (denotation) of an algorithm as a function that maps input to output.

Domains	Definition 1.4.1
<p>Domains are special kinds of partially ordered sets. Partial orders meaning there is an order of elements in the set, but not every element is comparable.</p> <p>Partial orders are reflexive, transitive and anti-symmetric. You can easily represent them on a Hasse Diagram.</p> <div style="text-align: center;"><pre>graph BT; Empty["{}"] --> A["{A}"]; Empty --> B["{B}"]; Empty --> C["{C}"]; A --> AB["{A, B}"]; A --> AC["{A, C}"]; B --> AB["{A, B}"]; B --> BC["{B, C}"]; C --> AC["{A, C}"]; C --> BC["{B, C}"]; AB --> ABC["{A, B, C}"]; AC --> ABC["{A, B, C}"]; BC --> ABC["{A, B, C}"];</pre></div> <p>Diagram of \subseteq for sets $\subseteq \{A, B, C\}$</p>	

Scott solved the most difficult part, considering recursively defined algorithms as continuous functions between domains.

1.4.4 Haskell Programs

Example using a basic implementation of power.

```
-- Precondition: n >= 0
power :: Integer -> Integer -> Integer
power x 0 = 1
```

```

power x n = x * power x (n-1)

-- Precondition: n >= 0
power' :: Integer -> Integer -> Integer
power' x 0 = 1
power' x n
  | even n = k2
  | odd n  = x * k2
where
  k  = power' x (n `div` 2)
  k2 = k * k

O(n)
power 7 5
  ~> 7 * (power 7 4)
  ~> 7 * ( 7 * (power 7 3))
  ~> 7 * ( 7 * (7 * (power 7 2)))
  ~> 7 * ( 7 * (7 * (7 * (power 7 1))))
  ~> 7 * ( 7 * (7 * (7 * (7 * (power 7 0)))))
  ~> 7 * ( 7 * (7 * (7 * (7 * 1))))
  ~> 16807

```

O(log(n)) steps

```

power' 7 5
  ~> 7 * (power' 7 2)2
  ~> 7 * ((power' 7 1)2)2
  ~> 7 * ((7 * (power' 7 0)2)2)2
  ~> 7 * ((7 * (1)2)2)2
  ~> 16807

```

These two functions are equivalent in result however operate differently (one much faster than the other).

1.5 Program Semantics

Denotational Semantics	Definition 1.5.1
<ul style="list-style-type: none"> • A program's meaning is described computationally using denotations (mathematical objects) • A denotation of a program phrase is built from its sub-phrases. 	
Operational Semantics	Definition 1.5.2
Program's meaning is given in terms of the steps taken to make it run.	

There are also *axiomatic semantics* and *declarative semantics* but we will not cover them here.

Chapter 2

Credit

Image Credit

Front Cover Analytical Engine - Science Museum London

Content

Based on the *Models of Computation* course taught by Dr Azelea Raad and Dr Herbert Wiklicky.

These notes were written by Oliver Killane.