1 Machines & Models

16 February 2021

Sebastian Wild

version 2021-02-16 10:31

Outline

What is an algorithm?

An algorithm is a sequence of instructions.

think: recipe

More precisely:

e. g. Java program

1. mechanically executable
   ⇝ no "common sense" needed
2. finite description ≠ finite computation!
3. solves a problem, i. e., a class of problem instances

$x + y$, not only 17 + 4

input → [algo] → output

typical example: *bubblesort*

not a specific program but underlying idea

What is a data structure?

A data structure is

1. a rule for encoding data (in computer memory), plus
2. algorithms to work with it (queries, updates, etc.)

typical example: binary search tree

1.1 Algorithm analysis

Good algorithms

Our goal: Find good (best?) algorithms and data structures for a task.

Good "usually" means

can be complicated in distributed systems

- fast running *time*
- moderate memory *space* usage

Algorithm analysis is a way to

- compare different algorithms,
- predict their performance in an application

Running time experiment

Why not simply run and time it?

- results only apply to
  - single *test* machine
  - tested inputs
  - tested implementation
  - ...

  $\neq$ ***universal truths***
- instead: consider and analyze algorithms on an abstract machine
  - ⇝ provable statements for model
  - ⇝ testable model hypotheses

survives Pentium 4

⇝ Need precise model of machine (costs), input data and algorithms.

Data Models

Algorithm analysis typically uses one of the following simple data models:

- **worst-case performance:**
  consider the *worst* of all inputs as our cost metric
- **best-case performance:**
  consider the *best* of all inputs as our cost metric
- **average-case performance:**
  consider the average/expectation of a *random* input as our cost metric

Usually, we apply the above for *inputs of same size* n.

$\rightsquigarrow$ performance is only a **function of** n.

1.2 The RAM Model

Clicker Question

What is the cost of *adding* two d-digit integers?
For example, for $d = 5$, what is $45\,235 + 91\,342$?

- **A** constant time
- **B** logarithmic in d
- **C** proportional to d
- **D** quadratic in d
- **E** no idea what you are talking about

`sli.do/comp526`

Click on "Polls" tab

Clicker Question

What is the cost of *adding* two d-digit integers?
For example, for $d = 5$, what is $45\,235 + 91\,342$?

- **A** constant time ✓ if fit into an int (64 bit)
- **B** ~~logarithmic in d~~
- **C** proportional to d ✓ if #bits >> 64 (BigInteger)
- **D** ~~quadratic in d~~
- **E** no idea what you are talking about ✓

sli.do/comp526

Click on "Polls" tab

Machine models

The machine model decides

- what algorithms are possible
- how they are described (= programming language)
- what an execution *costs*

Goal: Machine model should be
detailed and powerful enough to reflect actual machines,
abstract enough to unify architectures,
simple enough to analyze.

Random Access Machines

Random access machine (RAM)

more detail in §2.2 of *Sequential and Parallel Algorithms and Data Structures* by Sanders, Mehlhorn, Dietzfelbinger, Dementiev

- unlimited *memory* $\texttt{MEM}[0], \texttt{MEM}[1], \texttt{MEM}[2], \ldots$
- fixed number of *registers* $R_1, \ldots, R_r$ (say $r = 100$)
- memory cells $\texttt{MEM}[i]$ and registers R_i store w-bit integers, i. e., numbers in $[0..2^w - 1]$
  w is the word width/size; typically $w \propto \lg n \rightsquigarrow 2^w \approx n$
  w = 64 128
  machine grows with input!?
- Instructions:
  - load & store: $R_i := \texttt{MEM}[R_j]$ $\texttt{MEM}[R_j] := R_i$
  - operations on registers: $R_k := R_i + R_j$ (arithmetic is *modulo* 2^w!)
    also $R_i - R_j,\ R_i \cdot R_j,\ R_i \operatorname{div} R_j,\ R_i \bmod R_j$
    C-style operations (bitwise and/or/xor, left/right shift)
    $R_j = 0$
  - conditional and unconditional jumps
- cost: number of executed instructions

we will see further models later

$\rightsquigarrow$ The RAM is the standard model for sequential computation.

Pseudocode

Typical simplifications for convenience:

- more abstract *pseudocode* to specify algorithms
  code that humans understand (easily)
- count *dominant operations* (e. g. array accesses) instead of all operations

In both cases: can go to full detail if needed.

restart at noon

.. 1 more min

1.3 Asymptotics & Big-Oh

Why asymptotics?

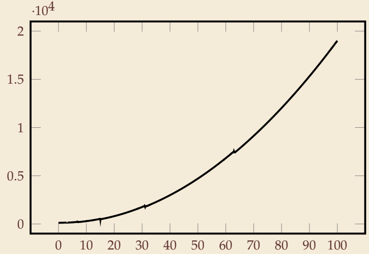
Algorithm analysis focuses on (the limiting behavior for infinitely) **large** inputs.

- abstracts from unnecessary detail
- simplifies analysis
- often necessary for sensible comparison

Asymptotics = approximation around ∞

Example: Consider a function $f(n)$ given by

$2n^2 - 3n\lfloor \log_2(n+1) \rfloor + 7n - 3\lfloor \log_2(n+1) \rfloor + 120$



Why asymptotics?

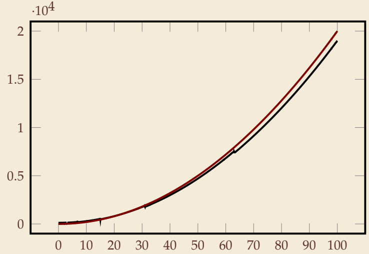
Algorithm analysis focuses on (the limiting behavior for infinitely) **large** inputs.

- abstracts from unnecessary detail
- simplifies analysis
- often necessary for sensible comparison

Asymptotics = approximation around ∞

Example: Consider a function $f(n)$ given by

$$2n^2 - 3n\lfloor \log_2(n+1)\rfloor + 7n - 3\lfloor \log_2(n+1)\rfloor + 120 \quad \sim \quad \underset{\smile}{\mathbf{2n^2}}$$



Asymptotic tools – Formal & definitive definition

- **"Tilde Notation:"** $f(n) \sim g(n)$ iff $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$

  if, and only if

  „f and g are *asymptotically equivalent*"

preserves constant factors

Asymptotic tools – Formal & definitive definition

- **"Tilde Notation:"** $f(n) \sim g(n)$ iff $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$ (if, and only if)

  „f and g are *asymptotically equivalent*"

- **"Big-Oh Notation:"** $f(n) \in O(g(n))$ (also write '=' instead) iff $\left|\frac{f(n)}{g(n)}\right|$ is bounded for $n \geq n_0$ ($< \infty$) ($g(n)$ could be 0)

  iff $\limsup_{n\to\infty} \left|\frac{f(n)}{g(n)}\right| < \infty$ (need supremum since limit might not exist!)

Variants:

- $f(n) = \Omega(g(n))$ ("Big-Omega"; $\in$) iff $g(n) = O(f(n))$
- $f(n) = \Theta(g(n))$ ("Big-Theta"; $\in$) iff $f(n) = O(g(n))$ **and** $f(n) = \Omega(g(n))$

Asymptotic tools – Formal & definitive definition

- **"Tilde Notation:"** $f(n) \sim g(n)$ iff $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$ (iff: if, and only if)

  „f and g are *asymptotically equivalent*"

- **"Big-Oh Notation:"** $f(n) \in O(g(n))$ (also write '=' instead) iff $\left|\frac{f(n)}{g(n)}\right|$ is bounded for $n \geq n_0$

  iff $\lim_{n\to\infty} \sup \left|\frac{f(n)}{g(n)}\right| < \infty$ (need supremum since limit might not exist!)

  Variants:
  - $f(n) = \Omega(g(n))$ ("Big-Omega") iff $g(n) = O(f(n))$
  - $f(n) = \Theta(g(n))$ ("Big-Theta") iff $f(n) = O(g(n))$ **and** $f(n) = \Omega(g(n))$

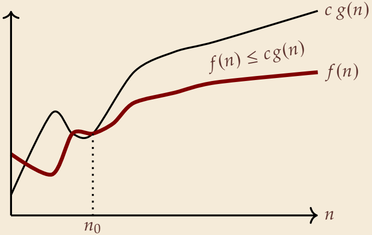
- **"Little-Oh Notation:"** $f(n) = o(g(n))$ iff $\lim_{n\to\infty} \left|\frac{f(n)}{g(n)}\right| = 0$

  $f(n) = \omega(g(n))$ if $\lim = \infty$

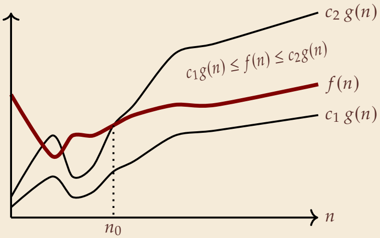
Asymptotic tools – Intuition

- $f(n) = O(g(n))$: $f(n)$ is **at most** $g(n)$ up to constant factors and for sufficiently large n

“ $f \le g$ ”



- $f(n) = \Theta(g(n))$: $f(n)$ is **equal to** $g(n)$ up to constant factors and for sufficiently large n



Plots can be misleading!

Example

Clicker Question

Assume $f(n) \in O(g(n))$. What can we say about $g(n)$?

- **A** $g(n) = O(f(n))$
- **B** $g(n) = \Omega(f(n))$
- **C** $g(n) = \Theta(f(n))$
- **D** Nothing (it depends on f and g)

sli.do/comp526

Click on “Polls” tab

Clicker Question

Assume $f(n) \in O(g(n))$. What can we say about $g(n)$?

- **A** ~~$g(n) = O(f(n))$~~
- **B** $g(n) = \Omega(f(n))$ ✓
- **C** ~~$g(n) = \Theta(f(n))$~~
- **D** ~~Nothing (it depends on f and g)~~

`sli.do/comp526`

Click on “Polls” tab

Clicker Question

Assume $f(n) \in O(g(n))$. What can we say about $g(n)$?

- **A** ~~$g(n) = O(f(n))$~~
- **B** $g(n) = \Omega(f(n))$ ✓ (if $f(n) \neq 0$)
- **C** ~~$g(n) = \Theta(f(n))$~~
- **D** Nothing (it depends on f and g) ✓

sli.do/comp526

Click on "Polls" tab

Asymptotics – Example 1

Basic examples:

- $20n^3 + 10n\ln(n) + 5 \sim 20n^3 = \Theta(n^3)$
- $3\lg(n^2) + \lg(\lg(n)) = \Theta(\log n)$
- $10^{100} = O(1)$

$$\frac{3 \cdot 2\,\lg(n) + \lg(\lg(n))}{\lg n} \xrightarrow[n\to\infty]{} 6$$

$$\lim_{n\to\infty} \frac{20n^3 + 10n\ln n + 5}{20n^3} = \lim_{n\to\infty} \frac{20n^3}{20n^3} + \frac{10n\ln n + 5}{20n^3} = 1 + \lim_{n\to\infty} \frac{10n\ln n + 5}{20n^3} = 1 + 0$$

$$20 < \infty \Rightarrow f(n) = O(n^3)$$

Use *wolfram alpha* to compute/check limits.

Clicker Question

Is $(\sin(n) + 2)n^2 = \Theta(n^2)$?

A Yes

B No

sli.do/comp526

Click on "Polls" tab

Clicker Question

Is $(\sin(n) + 2)n^2 = \Theta(n^2)$?

A Yes ✓

B ~~No~~

sli.do/comp526

Click on "Polls" tab

Asymptotics – Frequently used facts

- Rules:
  - $c \cdot f(n) = \Theta(f(n))$ for constant $c \neq 0$
  - $\Theta(f + g) = \Theta(\max\{f, g\})$ largest summand determines order of growth

    $\approx \Theta$ class
- Frequently used orders of growth:
  - logarithmic $\Theta(\log n)$ Note: $a, b > 0$ constants $\rightsquigarrow$ $\Theta(\log_a(n)) = \Theta(\log_b(n))$
  - linear $\Theta(n)$
  - linearithmic $\Theta(n \log n)$
  - quadratic $\Theta(n^2)$
  - polynomial $O(n^c)$ for constant c
  - exponential $O(c^n)$ for constant c Note: $a > b > 0$ constants $\rightsquigarrow$ $b^n = o(a^n)$

Asymptotics – Example 2

Square-and-multiply algorithm
for computing x^m with $m \in \mathbb{N}$

Inputs:

- m as binary number (array of bits)
- n = #bits in m
- x a floating-point number

```
1 double pow(double base, boolean[] exponentBits) {
2     double res = 1;
3     for (boolean bit : exponentBits) {
4         res *= res;
5         if (bit) res *= base;
6     }
7     return res;
8 }
```

- Cost: C = # multiplications
- $C = n$ (line 4) + #one-bits binary representation of m (line 5)

$\rightsquigarrow$ $n \le C \le 2n$

Clicker Question

We showed $n \leq C(n) \leq 2n$; what is the most precise asymptotic approximation for $C(n)$ that we can make?

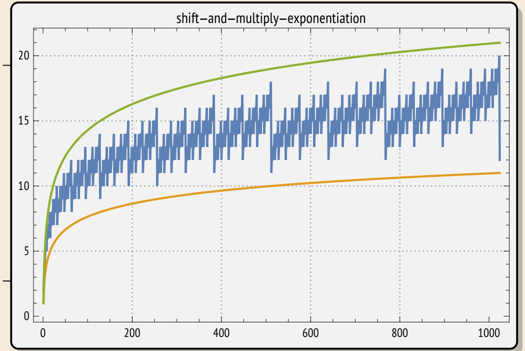
Write e. g. `O(n^2)` for $O(n^2)$ or `Theta(sqrt(n))` for $\Theta(\sqrt{n})$.

`sli.do/comp526`

Click on "Polls" tab

Asymptotics – Example 2

Square-and-multiply algorithm
for computing x^m with $m \in \mathbb{N}$



Inputs:

- m as binary number (array of bits)
- n = #bits in m
- x a floating-point number

- Cost: C = # multiplications
- $C = n$ (line 4) + #one-bits binary representation of m (line 5)

$\rightsquigarrow$ $n \le C \le 2n$

$\rightsquigarrow$ $C = \Theta(n) = \Theta(\log m)$

Note: Often, you can pretend Θ is "like $\sim$ with an unknown constant"
but in this case, no such constant exists!