Intro to Algorithms HW 2

Greg Stewart

February 2, 2018

Q1

Compute 2^{2^n} in linear time.

```
function power_of_power_of_two(n):
  input: the power n to raise the 2 in the exponent to
  output: the answer

  result = 2
  for i in 0..n:
    result = result * result

  return result
```

Since we assume multiplication of arbitrary size integers takes unit time, the above algorithm is $O(n)$. If we don't make that assumption, then every multiplication in the for loop takes $O(m^2)$ time, where m is the number of bits. The numbers being multiplied are n-digits, though, so overall the complexity becomes $O(n) \cdot O(n^2) = O(n^3)$.

Q2

(a) N is an n-bit number. How many bits is $N!$?

Multiplication of 2 m-bit numbers results in a number of $2m$ bits. Given a number N, the number of bits is $n = log_2 N$. With a factorial, the number N is multiplied with all numbers before it:

$$N! = N \cdot (N-1) \cdot (N-2) \cdots 1$$

Since multiplication roughly results in adding the bit-lengths of the numbers being multiplied, we can write the resulting bit-length of $N!$ as

$$m = \log(N+1) + \log(N) + \log(N-1) + \cdots + \log(1)$$

N could be any arbitrary number, so what this amounts to is on the order of

$$m = \log(N)^N$$

Which we can rewrite as

$$m = N \log(N)$$

Recalling that the number of bits in N is n, we finally arrive at the answer

$$m = N \cdot n$$

This is linear, of course, so the resulting $O()$ notation is

$$O(n)$$

.

(b) Give an algorithm to compute $N!$ and analyze the running time.

```
function factorial(n):
  if n = 1 or 0: return 1
  answer = 1
  for i in 1..n+1:
    answer = answer*i
  return answer
```

For the trivial case, this is $O(1)$. In general, however, this requires n multiplications, where n is the number to be factorialized. The bit complexity of multiplication is $O(n^2)$, and this operation occurs n times, so we end up with

$$O(n^3)$$

Q3 Find the GCD of 1492 and 1776 using

(a) the prime factorization method and using Euclid's method

Euclid's Method: We use the extended method for simplifying part (b)

a	b	$r = a \mod b$	combination
1776	1492	284	1776 - 1492
1492	284	72	1492 - 5(284)
284	72	68	284 - 3(72)
72	68	4	72 - 68
68	4	0	-

So gcd(1776, 1492) = 4.

Prime Factorization: Factor both and obtain the common prime factor.

$$1492 = 2(746) = 2^2(373)$$
$$1776 = 2^4(111) = 2^4 \cdot 3(37)$$

From the factorization it is obvious that the only common factor is 2^2, so gcd = 4,

(b) express the GCD as an integer linear combination of two inputs

To do this, we work backwards from the GCD, using the table from Euclid's Method.

$$\begin{aligned}
4 &= 72 - 68 \\
&= (1492 - 5(284)) - (284 - 3(72)) \\
&= (1492 - 5(1776 - 1492)) - ((1776 - 1492) - 3(1492 - 5(284))) \\
&= (1492 - 5(1776 - 1492)) - ((1776 - 1492) - 3(1492 - 5(1776 - 1492))) \\
&= 1492 - 5(1776) + 5(1492) - (1776 - 1492 - 3(1492) + 15(1776 - 1492) \\
&= 6(1492) - 5(1776) - 1776 + 1492 + 3(1492) - 15(1776) + 15(1492) \\
&= 25(1492) - 21(1776)
\end{aligned}$$

With the final expression being the linear combination of the inputs.