

IT-math F2003 : Supplementary Material

Episodes 10–11, April 8–22, 2003

Growth Rates of Functions

1. DEFINITION. Let f and g be functions from \mathbb{N} to \mathbb{R} (or from \mathbb{R}_+ to \mathbb{R}). Define
- (i) $f(n) = O(g(n))$ (also written $f = O(g)$) if there is a real number $C > 0$ such that there is an $m \geq 0$ such that for all $n \geq m$ one has¹ $|f(n)| \leq C \cdot |g(n)|$;
 - (ii) $f(n) = \Omega(g(n))$ (also written $f = \Omega(g)$) if there is a real number $C > 0$ such that for almost all n one has $C \cdot |f(n)| \geq |g(n)|$;
 - (iii) $f(n) = \Theta(g(n))$ (also written $f = \Theta(g)$) if we have both $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$;
 - (iv) $f(n) = o(g(n))$ (also written $f = o(g)$) if for any real number $c > 0$ we have for almost all n that $|f(n)| < c \cdot |g(n)|$.

2. OBSERVATION. $f = O(g)$ if and only if $g = \Omega(f)$.

PROOF. Follows at once from the definitions. ■

3. PROPOSITION. (a) Both binary relations $f = O(g)$ and $f = \Omega(g)$ are reflexive and transitive;
(b) The binary relation $f = \Theta(g)$ is an equivalence relation.

PROOF. (a). O is clearly reflexive: one has $|f(n)| \leq 1 \cdot |f(n)|$ for all $n \geq 0$, so that $f = O(f)$.

For transitivity, assume $f = O(g)$ and $g = O(h)$. Thus we have $C_1, C_2 > 0$ and $m_1, m_2 \geq 0$ such that for all $n \geq m_1$ one has $|f(n)| \leq C_1 \cdot |g(n)|$ and for all $n \geq m_2$, $|g(n)| \leq C_2 \cdot |h(n)|$. Therefore², as soon as $n \geq \max\{m_1, m_2\}$, one has

$$|f(n)| \leq C_1 \cdot |g(n)| \leq C_1 \cdot C_2 \cdot |h(n)|.$$

Since $C_1 \cdot C_2 > 0$, this shows $f = O(h)$, so that O is transitive.

Reflexivity and transitivity of Ω follow at once from the reflexivity and transitivity of O in view of Observation 2.

(b). Θ is clearly reflexive: for any function $f : \mathbb{N} \rightarrow \mathbb{R}$ (or $f : \mathbb{R}_+ \rightarrow \mathbb{R}$) we have $f = O(f)$ and $f = \Omega(f)$ by (a), so $f = \Theta(f)$.

Transitivity of Θ again follows from that of O and Ω : If we have $f = \Theta(g)$ and $g = \Theta(h)$ then $f = O(g)$ and $g = O(h)$, which by (a) implies $f = O(h)$. Similarly, $f = \Omega(g)$ and $g = \Omega(h)$ get us $f = \Omega(h)$ by (a), so that $f = \Theta(h)$ as required.

Finally, Θ is symmetric: $f = \Theta(g)$ means by definition that $f = O(g)$ and $f = \Omega(g)$, hence by 2 $g = \Omega(f)$ and $g = O(f)$, so we have $g = \Theta(f)$.

Thus the binary relation $f = \Theta(g)$, being reflexive, transitive, and symmetric, is an equivalence relation. ■

4. EXERCISE. If $\alpha > \beta > 0$ are real numbers then $n^\beta = o(n^\alpha)$. ■

¹The expression ‘there is an m such that for all $n \geq m$...’ is often abbreviated by ‘for all sufficiently large n ...’ or by ‘for almost all n ...’.

²What follows is an elaboration of the following principle, which we are going to use later on without too many words: if two (in)equalities both hold for almost all n , then they hold *together* for almost all n as well, as do their consequences (in this instance, a third inequality).

The Complexity of Euclid's Algorithm

5. PROPOSITION. *Euclid's Algorithm for finding $\gcd(m, n)$ ($m, n \in \mathbb{N}_+$) performs $O(\log \max\{m, n\})$ many operations of division with remainder.*

PROOF. Let us recall Euclid's Algorithm. Without loss of generality, we may assume $m > n$. We define a sequence r_0, r_1, r_2, \dots by putting $r_0 = m, r_1 = n$, and letting each successive r_i be the remainder of integer division of r_{i-2} by r_{i-1} :

$$\begin{aligned} r_0 &= m \\ r_1 &= n \\ r_2 &= r_0 \bmod r_1 \\ &\dots \\ r_{k+1} &= r_{k-1} \bmod r_k \\ &\dots \end{aligned}$$

Recall that r_i gets smaller and smaller: $r_{i+1} < r_i$. The process stops when you get $r_{N+1} = 0$. Then $r_N = \gcd(m, n)$:

$$\begin{aligned} \gcd(m, n) &= r_N = r_{N-2} \bmod r_{N-1} \\ 0 &= r_{N+1} = r_{N-1} \bmod r_N \end{aligned}$$

Observe that N is the number of operations of integer division performed by the algorithm. We would like to estimate N in terms of m and n . In order to do that we first observe that $r_{k+2} \leq \frac{1}{2}r_k$ for all $k \leq N-1$: Indeed, since $r_k = q_{k+1} \cdot r_{k+1} + r_{k+2}$ and $r_{k+1} < r_k$, we have $q_{k+1} \geq 1$, so that $2 \cdot r_{k+2} \leq q_{k+1} \cdot r_{k+1} + r_{k+2} = r_k$.

Next we claim that $r_{2i} \leq \left(\frac{1}{2}\right)^i \cdot m$. This is clear for $i = 0$ and follows for larger i by induction since we have just shown that $r_{2(i+1)} \leq \frac{1}{2}r_{2i}$. Therefore $r_k \leq r_{2\lceil k/2 \rceil} \leq \left(\frac{1}{2}\right)^{\lceil k/2 \rceil} \cdot m$.

Now, since $r_N \geq 1$, we have $1 \leq \left(\frac{1}{2}\right)^{\lceil N/2 \rceil} \cdot m$, or, equivalently, $2^{\lceil N/2 \rceil} \leq m$, hence $\lceil N/2 \rceil \leq \log_2 m$, so $N \leq 2 \cdot \log_2 m = 2 \cdot \log_2 \max\{m, n\}$. In particular, $N = O(\log_2 \max\{m, n\})$ as required. ■

Technical Lemmas on O , Ω , Θ , and o

6. EXERCISE. *Suppose $c \in \mathbb{R}$ and $c \neq 0$. Then $c \cdot f = \Theta(f)$.* ■

7. LEMMA. (a) *If $f = o(g)$ then $f = O(g)$;*
 (b) *If $f = o(g)$ then $f \neq \Omega(g)$.*

PROOF. (a). If $f = o(g)$ then we have $|f(n)| \leq 1 \cdot |g(n)|$ for almost all n . But this is enough to conclude that $f = O(g)$.

(b). Reasoning towards contradiction, let us assume $f = o(g)$ and $f = \Omega(g)$. Since $f = \Omega(g)$, there must exist $C > 0$ such that $|f(n)| \geq C \cdot |g(n)|$ for almost all n . Since $f = o(g)$, One also has $|f(n)| < C \cdot |g(n)|$ for almost all n (for that same C). Thus $|f(n)| < C \cdot |g(n)| \leq |f(n)|$ for almost all n , which is the required contradiction. ■

8. LEMMA. (a) *If $f = o(g)$ and $h = o(g)$, then³ $f + h = o(g)$;*
 (b) *If $f = O(g)$ and $h = O(g)$, then $f + h = O(g)$.*

³The function $f + h$ is defined by $(f + h)(n) = f(n) + h(n)$.

PROOF. (a). Fix $c > 0$. Since $f = o(g)$ and $h = o(g)$, one has $|f(n)| < \frac{c}{2} \cdot |g(n)|$ and $|h(n)| < \frac{c}{2} \cdot |g(n)|$ for almost all n . Hence

$$|f(n) + h(n)| \leq |f(n)| + |h(n)| < \frac{c}{2} \cdot |g(n)| + \frac{c}{2} \cdot |g(n)| = c \cdot |g(n)|$$

for almost all n , which shows $f + h = o(g)$.

(b). Since $f = O(g)$ and $h = O(g)$, there are $C_1, C_2 > 0$ such that $|f(n)| < C_1 \cdot |g(n)|$ and $|h(n)| < C_2 \cdot |g(n)|$ for almost all n . Therefore

$$|f(n) + h(n)| \leq |f(n)| + |h(n)| < C_1 \cdot |g(n)| + C_2 \cdot |g(n)| = (C_1 + C_2) \cdot |g(n)|$$

for almost all n . We conclude $f = O(g)$. ■

9. LEMMA. Suppose $h = o(g)$.

- (a) If $f = O(g)$ then $f + h = O(g)$;
- (b) If $f = \Omega(g)$ then $f + h = \Omega(g)$;
- (c) If $f = \Theta(g)$ then $f + h = \Theta(g)$.

PROOF. (a). Since $f = O(g)$, there exists a $C > 0$ with $|f(n)| \leq C \cdot |g(n)|$ for almost all n . Since $h = o(g)$, one has $|h(n)| < C \cdot |g(n)|$ for almost all n . Therefore for almost all n there holds

$$|f(n) + h(n)| \leq |f(n)| + |h(n)| < C \cdot |g(n)| + C \cdot |g(n)| = 2C \cdot |g(n)|,$$

which shows $f + h = O(g)$.

(b). By $f = \Omega(g)$, there exists a $C > 0$ with $|f(n)| \geq C \cdot |g(n)|$ for almost all n . Since $h = o(g)$, the inequality $|h(n)| < \frac{C}{2} \cdot |g(n)|$ also holds for almost all n . Thus we have

$$|f(n) + h(n)| \geq |f(n)| - |h(n)| > C \cdot |g(n)| - \frac{C}{2} \cdot |g(n)| = \frac{C}{2} \cdot |g(n)|,$$

which spells out $f + h = \Omega(g)$.

(c). Follows at once from (a) and (b). ■

10. LEMMA. (a) If $f = o(g)$ and $g = O(h)$, then $f = o(h)$;

(b) If $f = O(g)$ and $g = o(h)$, then $f = o(h)$.

PROOF. (a). Fix $c > 0$. Since $g = O(h)$, there exists a $D > 0$ such that $|g(n)| \leq D \cdot |h(n)|$ for almost all n . Since $f = o(g)$, one has $|f(n)| < \frac{c}{D} \cdot |g(n)|$ for almost all n . Therefore

$$|f(n)| < \frac{c}{D} \cdot |g(n)| \leq \frac{c}{D} \cdot D \cdot |h(n)| = c \cdot |h(n)|$$

for almost all n , showing $f = o(h)$.

(b). Fix $c > 0$. Since $f = O(g)$, there exists a $D > 0$ such that $|f(n)| \leq D \cdot |g(n)|$ for almost all n . Since $g = o(h)$, one has $|g(n)| < \frac{c}{D} \cdot |h(n)|$ for almost all n . Therefore

$$|f(n)| < D \cdot |g(n)| \leq D \cdot \frac{c}{D} \cdot |h(n)| = c \cdot |h(n)|$$

for almost all n , showing $f = o(h)$. ■

Polynomials, Logarithms, Exponents, and Factorials

11. PROPOSITION. If $f(n) = a_k n^k + a_{k-1} n^{k-1} + \dots + a_0$ is a polynomial in n and $a_k \neq 0$, then $f(n) = \Theta(n^k)$.

PROOF. let $g(n) = a_{k-1} n^{k-1} + \dots + a_0$, so that $f(n) = a_k n^k + g(n)$. Since $a_k \neq 0$, we have $a_k n^k = \Theta(n^k)$ by Exercise 6. By Exercise 4 and Lemma 8(a), we have $g(n) = o(n^k)$. Therefore by Lemma 9(c) we get $f(n) = a_k n^k + g(n) = \Theta(n^k)$ as required. ■

12. PROPOSITION. For $k \in \mathbb{N}$ and any real $a > 1$ we have

- (a) $n^k = o(a^n)$;
- (b) $n^k = o(a^{(n^\varepsilon)})$ for any real $\varepsilon > 0$.

PROOF. (a). Fix an arbitrary real $c > 0$. Let $\delta = a - 1$. Observe that $\delta > 0$. For sufficiently large natural n we have

$$\begin{aligned} n^k &< \frac{c}{a} \cdot \binom{n}{k+1} \cdot \delta^{k+1} \quad (\text{by Exercise 4, as the r.h.s. is a polynomial in } n \text{ of degree } k+1) \\ &< \frac{c}{a} \cdot \left(1 + \binom{n}{1} \cdot \delta + \cdots + \binom{n}{k+1} \cdot \delta^{k+1} + \cdots + \binom{n}{n} \cdot \delta^n\right) \\ &\hspace{15em} (\text{here we have just added a few positive terms}) \\ &= \frac{c}{a} \cdot (1 + \delta)^n = \frac{c}{a} \cdot a^n = c \cdot a^{n-1} \quad (\text{by the Binomial Theorem}). \end{aligned}$$

Therefore if $n \in \mathbb{R}$ and n is sufficiently large, we have $n^k \leq \lceil n \rceil^k < c \cdot a^{\lceil n \rceil - 1} \leq c \cdot a^n$. So $n^k = o(a^n)$.

(b). Again, fix an arbitrary $c > 0$. By (a) we have $m^{k/\varepsilon} \leq m^{\lceil k/\varepsilon \rceil} < c \cdot a^m$ for almost all m (recall that this means there exists an m_0 such that the inequality holds for all $m \geq m_0$). Now put $n = m^{1/\varepsilon}$ (so that $m = n^\varepsilon$). Then $n^k = m^{k/\varepsilon} < c \cdot a^m = c \cdot a^{(n^\varepsilon)}$ as soon as $n^\varepsilon = m \geq m_0$, or equivalently, provided $n \geq m_0^{1/\varepsilon}$, which holds for almost all n . Thus $n^k = o(a^{(n^\varepsilon)})$. ■

13. PROPOSITION. Let $\varepsilon, a \in \mathbb{R}, a > 1, \varepsilon > 0$.

- (a) $\log_a n = o(n^\varepsilon)$;
- (b) $(\log_a n)^M = o(n^\varepsilon)$ for any $M > 0$.

PROOF. (a). Fix an arbitrary real $c > 0$. Since $a^{\varepsilon \cdot c} > 1$, we have $m = o((a^{\varepsilon \cdot c})^m)$ by (a), so $m < (a^{\varepsilon \cdot c})^m$ for almost all m . Hence for almost all m one has

$$\log_a m < \log_a a^{\varepsilon \cdot c \cdot m} = \varepsilon \cdot c \cdot m.$$

Divide this by $\varepsilon > 0$ to get

$$\log_a m^{1/\varepsilon} = \frac{1}{\varepsilon} \log_a m < c \cdot m.$$

Now let $n = m^{1/\varepsilon}$. Then $\log_a n < c \cdot n^\varepsilon$ for almost all n (this is argued as in the proof of Proposition 12(a)). So $\log_a n = o(n^\varepsilon)$.

(b). Fix some $c > 0$. By (a), $\log_a n < c^{1/M} \cdot n^{\varepsilon/M}$ for almost all n . Take this to the M th power: you get $(\log_a n)^M < c \cdot n^\varepsilon$, so $(\log_a n)^M = o(n^\varepsilon)$. ■

14. PROPOSITION. If the numbers $a, b \in \mathbb{R}$ are such that $a > b > 1$, then $b^n = o(a^n)$.

PROOF. Let $c > 0$. If $n > \log_{a/b}(\frac{1}{c})$ then $\log_{a/b}(\frac{1}{c}) < n = \log_{a/b}(\frac{a}{b})^n$, hence $\frac{1}{c} < (\frac{a}{b})^n$ (for $\frac{a}{b} > 1$), hence $b^n < c \cdot a^n$ for almost all n . This shows $b^n = o(a^n)$. ■

15. PROPOSITION. $\log n! = \Theta(n \cdot \log n)$.

PROOF. Since $n! \leq n^n$, we have $\log n! \leq \log n^n = n \cdot \log n$, so $\log n! = O(n \cdot \log n)$.

To establish $\log n! = \Omega(n \cdot \log n)$, observe that

$$\begin{aligned} \log n! &= \log 1 + \log 2 + \cdots + \log n \geq \underbrace{\log \left\lfloor \frac{n}{2} \right\rfloor + \log \left(\left\lfloor \frac{n}{2} \right\rfloor + 1 \right) + \cdots + \log n}_{\lfloor n/2 \rfloor \text{ terms}} \\ &\geq \left\lfloor \frac{n}{2} \right\rfloor \cdot \log \left(\frac{n}{2} \right) \geq \left(\frac{n}{3} \right) \cdot \log \left(\frac{n}{2} \right) = \left(\frac{n}{3} \right) \cdot (\log n - \log 2) = \left(\frac{n}{3} \right) \cdot \log n - \left(\frac{n}{3} \right) \cdot \log 2 \end{aligned}$$

holds as soon as $\lfloor n/2 \rfloor \geq n/3$, i.e. for almost all n . We have $\binom{n}{3} \cdot \log n = \Omega(n \cdot \log n)$ by Exercise 6, and it is easily seen that $-\binom{n}{3} \cdot \log 2 = o(n \cdot \log n)$, therefore by Lemma 9(b) we get $\binom{n}{3} \cdot \log n - \binom{n}{3} \cdot \log 2 = \Omega(n \cdot \log n)$, hence $\log n! = \Omega(n \cdot \log n)$. ■