Asymptotic Arguments

A powerful technique using complexity and density

Jiwu Jang

Ross Mathematics Program

July 19, 2023

Outline

Limit superior

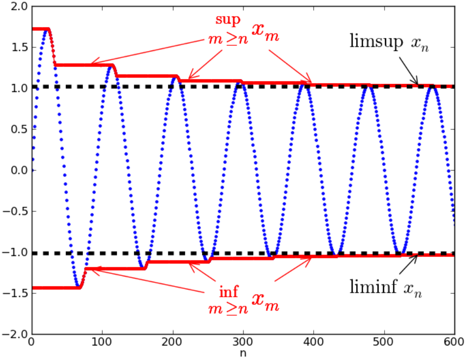

Figure: A graph showing the sup, inf, lim sup, and lim inf of a sequence.

Limit superior

Definition (Limit superior)

Let $\{x_n\}$ be a bounded sequence in $\mathbb{R}$. Let L be the set of all real numbers which are the limit of some subsequence of $\{x_n\}$. Since L is bounded, L has a maximum. This maximum is called the limit superior, denoted as:

$$\limsup_{n\to\infty} (x_n)$$

Bachmann-Landau notation

Important notations in asymptotic analysis (and problem solving):

- Big-O notation
- Little-o notation
- On the order of ($\sim$)

Big-O notation

Definition (Big-O)

Let $A \subseteq \mathbb{R}$ and $c \in \mathbb{R}$. Let $f, g : A \to \mathbb{R}$.
If $\exists M > 0$ such that $\limsup_{x \to c} \left| \frac{f(x)}{g(x)} \right| < M$, then we say that

$$f(x) = O(g(x)) \text{ as } x \to c$$

If the context is clear enough, we just write $f(x) = O(g(x))$ without specifying c.

Remark

In computational complexity theory, usually $x \to \infty$ is assumed.

Little-o notation

Definition (Little-o)

Let $A \subseteq \mathbb{R}$ and $c \in \mathbb{R}$. Let $f, g : A \to \mathbb{R}$.
If $\lim_{x \to c} \frac{f(x)}{g(x)} = 0$, then we say that

$$f(x) = o(g(x)) \text{ as } x \to c$$

If the context is clear enough, we simply write $f(x) = o(g(x))$ without specifying c.

Remark

For analytic purposes, either $x \to 0$ or $x \to \infty$ is assumed.

On the order of $(\sim)$

Definition (Asymptotic equality $(\sim)$)

Let $A \subseteq \mathbb{R}$ and $c \in \mathbb{R}$. Let $f, g : A \to \mathbb{R}$.
If $\lim_{x \to c} \frac{f(x)}{g(x)} = 1$, then we say that

$$f(x) \sim g(x) \text{ as } x \to c$$

If the context is clear enough, we just write $f(x) \sim g(x)$ without specifying c.

Remark

For analytic purposes, usually $x \to \infty$ is assumed.

Useful bounds

The following theorems are useful in asymptotic analysis.

Theorem (Prime number theorem)

Let $\pi(n)$ be the number of primes at most n. Then

$$\pi(n) \sim \frac{n}{\log n}$$

https://mathworld.wolfram.com/PrimeNumberTheorem.html

Useful bounds

Theorem (Dirichlet's theorem on arithmetic progressions)

For any two positive integers a and d with $\gcd(a, d) = 1$, there are infinitely many primes of the form $a + nd$, where $n \in \mathbb{N}$.

Exercise

Prove that there are infinitely many primes of the form $4n + 3$.

Problem (Harder)

Prove that there are infinitely many primes of the form $4n + 1$.

Useful bounds

Theorem (Strong form of Dirichlet)

For $\gcd(c, d) = 1$*, let* $\pi_d(n, c)$ *be the number of primes congruent to* c *modulo* d *less than* n*. Then,*

$$\pi_d(n, c) \sim \frac{n}{\varphi(d) \log n}$$

Exercise

Prove that $\frac{1}{3} + \frac{1}{7} + \frac{1}{11} + \frac{1}{19} + \frac{1}{23} + \frac{1}{31} + \frac{1}{43} + \frac{1}{47} + \frac{1}{59} + \frac{1}{67} + \dots$ *is a divergent series.*

Useful bounds

Theorem (Stirling's approximation)

For $n \in \mathbb{N}$, we have

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

or equivalently,

$$\log(n!) \sim n \log n - n + \frac{1}{2}\log n + \frac{1}{2}\log(2\pi)$$

Exercise

Prove that $\binom{3n}{n} \sim \dfrac{(27/4)^n\sqrt{3}}{2\sqrt{\pi n}}$.

Proving infinitude

Problem (Infinitude of primes)

Prove that there are infinitely many primes.

- The traditional way: suppose the set of primes was finite, then consider $n = p_1 p_2 \dots p_k + 1$.
- The Ross way: prove that $\gcd(2^{2^n} + 1, 2^{2^m} + 1) = 1$ for all $m, n \in \mathbb{N}$ where $m \neq n$, and conclude.
- The asymptotic way: $\pi(n) \sim \frac{n}{\log n}$, so $\pi(n) \to \infty$ as $n \to \infty$.

Remark

Totally overkill (and possibly circular), but this illustrates the usefulness of asymptotics: we can use analytic techniques to kill number theoretic problems.

Upper & lower density

Definition (Upper density)

Let $A \subseteq \mathbb{N}$. Define the upper asymptotic density $\overline{d}(A)$ of A (also called the "upper density") by

$$\overline{d}(A) = \limsup_{n \to \infty} \frac{|\{1, 2, \ldots, n\} \cap A|}{n}$$

Definition (Lower density)

Let $A \subseteq \mathbb{N}$. Define the lower asymptotic density $\underline{d}(A)$ of A (also called the "lower density") by

$$\underline{d}(A) = \liminf_{n \to \infty} \frac{|\{1, 2, \ldots, n\} \cap A|}{n}$$

Natural density

Definition (Natural density)

Let $A \subseteq \mathbb{N}$. If $\overline{d}(A) = \underline{d}(A)$, then define the natural density as

$$d(A) := \overline{d}(A) = \underline{d}(A)$$

Definition (Union bound)

For $n \in \mathbb{N}$ and sets $A_1, A_2, \ldots, A_k \subseteq \{1, 2, \ldots, n\}$, where $A_i := \{k \mid k \leq n \wedge P_i(k) = T\}$, where $P_i : \mathbb{N} \to \{T, F\}$ is a predicate. Let $A = A_1 \cap A_2 \cap \cdots \cap A_k$. We want to find the density

$$d(A) := \frac{|A|}{n}$$

which is equivalent to finding the number of elements that simultaneously satisfy all conditions P_i for all $1 \leq i \leq k$.

Union bound

Directly finding $d(A)$ is hard in most cases, but finding an upper bound $u_i \geq d(A_i)$ is usually easier. That is, we may do

$$d(A) \geq 1 - \sum_i d(A_i) \geq 1 - \sum_i u_i$$

Hence, to prove that $d(A) > 0$ as $n \to \infty$ (e.g., there are infinitely many n with some property), it suffices to show that $\sum_i u_i < 1$.

Proving infinitude

Problem (Ukraine TST 2007/12)

Prove that there are infinitely many positive integers n for which all the prime divisors of $n^2 + n + 1$ are not more than $\sqrt{n}$.

If we manually try to construct such n, the problem becomes much harder. This problem is in the spirit of trying to think of the cases that don't work, instead of trying to construct solutions from the beginning. (Actually, it is possible to manually construct solutions, but that solution has little to no motivation. On the other hand, density arguments are quite naturally motivated.)

Proving infinitude

Proof.

It suffices to show that there exist infinitely many $n \in \mathbb{N}$ such that $p \leq n^2$ for all primes p with

$$p \mid n^8 + n^4 + 1 = \left(n^4 - n^2 + 1\right)\left(n^2 - n + 1\right)\left(n^2 + n + 1\right)$$

Impose the condition that $n \equiv 1 \pmod 3$, then all prime factors of $\left(n^2 - n + 1\right)\left(n^2 + n + 1\right)$ are less than n^2, since $n^2 + n + 1 \equiv 0 \pmod 3$. It suffices to show infinitude of $n \equiv 1 \pmod 3$ such that all prime factors of $n^4 - n^2 + 1$ are less than n^2. When does there exist $p > n^2$ with $p \mid n^4 - n^2 + 1$? We can use double-counting to count how many n fail for some p. □

Proving infinitude

Proof.

For fixed p, it suffices to find the number of solutions to $n^4 - n^2 + 1 \equiv 0 \pmod{p}$ for $p > n^2$. But this is just $(n^2 - \frac{1}{2})^2 + \frac{3}{4} \equiv 0 \pmod{p}$, so $(2n^2 - 1)^2 \equiv -3 \pmod{p}$, thus there are at most 2 solutions for $2n^2 - 1$, and then we have at most 2 solutions for each case, thus in total, we have at most 4 solutions. Take the union bound to upper-bound the number of failing $n \in \{1, 4, 7, \dots, 3N-2\}$ by

$$\sum_{p<3N} 4 = O\left(\frac{N}{\log N}\right)$$

Thus, the density of failing n is strictly less than 1, so we have infinitely many positive integers n for which all the prime divisors of $n^2 + n + 1$ are not more than $\sqrt{n}$. $\square$

Szemerédi's theorem

Conjecture (Erdős, Turán, 1936)

If $d(E) > 0$*, then* E *contains arithmetic progressions of arbitrary length, that is,* $\forall k \in \mathbb{N}$*,* $\exists a \in E$ *and* $b \in \mathbb{N}$ *such that*

$$\{a + mb \mid 0 \leq m \leq k\} \subseteq E$$

Szemerédi's theorem

Let $E \subseteq \mathbb{Z}$. Define the upper density of E as

$$\overline{d}(E) := \limsup_{N \to \infty} \frac{|E \cap \{-N, \ldots, N\}|}{2N+1}$$

Theorem (Szemerédi, 1975)

If $\overline{d}(E) > 0$, then E contains arithmetic progressions of arbitrary length.

The proof is in "Ergodic behavior of diagonal measures and a theorem of Szemerédi" by H. Furstenberg.

Other interesting densities

Definition (Logarithmic density)

Let $A \subseteq \mathbb{N}$. Then, the *logarithmic density* of A is defined as

$$\delta(A) := \lim_{x\to\infty} \frac{1}{\log x} \sum_{n\in A,\ n\le x} \frac{1}{n}$$

provided that the limit is well-defined.

Definition (Banach density)

The *Banach density* $d^*(A)$ is defined as

$$d^*(A) = \lim_{N-M\to\infty} \frac{|A \cap \{M, M+1, \ldots, N\}|}{N-M+1}$$

given that the upper and lower densities coincide.

Closer: A problem from the IMO

Problem (IMO 2008/3)

Prove that there are infinitely many positive integers n such that n^2+1 has a prime divisor greater than $2n+\sqrt{2n}$.

Can you solve this problem using density? (Hint: It uses the exact same argument as Ukraine TST 2007/12.)

Happy problem solving!