A pretty proof that an exponential function is superpolynomial

Noah Stephens-Davidowitz
Cornell University

November 20, 2024

Abstract

We give a proof that we find to be rather elegant of the basic fact that $2^n \geq n^C$ for all sufficiently large n.

1 Introduction

We are interested in the fact that the exponential function grows faster than any polynomial. That is, we are interested in the fact that for any positive integer C, there exists $n_C > 0$ such that[1]

$$2^n \geq n^C, \text{ for all } n \geq n_C. \tag{1}$$

This is of course a widely used and quite basic fact, and there are many very nice and simple ways to prove it. E.g., a very slick proof simply uses repeated application of L'Hôpital's rule to argue that $\lim_{x\to\infty} \frac{x^C}{2^x} = 0$ for all constants C, which is of course equivalent to Equation (1). To prove Equation (1) combinatorially, one can note that $2^n \geq \binom{n}{C'}$ for any positive integers n and C', since 2^n counts the total number of subsets of a set with n elements, while $\binom{n}{C'}$ counts just some of these subsets. Applying the trivial inequality $\binom{n}{C'} \geq (n/C')^{C'}$ (valid for $n \geq C'$), and taking, say, $C' := C+1$ and $n \geq n_C := (C+1)^{C+1}$ gives

$$2^n \geq (n^{C+1}/(C+1))^{C+1} = n^C \cdot n/(C+1)^{C+1} \geq n^C \ ,$$

as needed.

The proofs described above are perfectly satisfactory, as are many other proofs. There is no need for any other proof, and it would be completely ridiculous for anyone to spend any additional time thinking about this. As such, there was a lively discussion on Twitter [Twi22] a few years ago among (otherwise perfectly respectable) mathematicians and computer scientists, giving different proofs of this and debating what counts as a truly "clean" proof of this basic fact.[2]

In this short note, we waste yet more time thinking about this basic fact that we already understand quite well. Specifically, we give yet another proof of Equation (1), simply because we find this new proof to be quite beautiful. The idea is to take the logarithm of both sides of

[1] The fact that we restrict our attention to positive integers n and C is not particularly important. Clearly the result holds more generally over the reals. But, for one of the proofs that we discuss below, it is convenient to take n and C to be positive integers.

[2] Of particular note in that discussion is a proof by Gowers, which is not nearly as simple as some of the others, but has the benefit of being "directly combinatorial." In particular, Gowers shows an explicit injection from the set $[n]^C$ of C-tuples to the power set of $[n]$ to for $n \geq n_C$.

Equation (1) *twice*, and to notice that after doing this, the inequality moves from "obvious but maybe not immediate" to completely trivial. (The author does not know of any prior work containing the proof that we give below, though one must imagine that such a proof has been discovered many times.)

2 The proof

We claim that the result follows from simple algebraic manipulation together with the seemingly much weaker and indisputably trivial inequality

$$2^y \geq y \;, \tag{2}$$

which is valid for all $y \in \mathbb{R}$.[3]

Indeed, let $n \geq n_C := 2^{4C}$ be large enough so that $x := \log\log n$ satisfies $x \geq x_C := \log(C) + 2$. Then,

$$\log\log(2^n) = 2^x = 2 \cdot 2^{x-1} \geq 2(x-1) = x + (x-2) \geq x + \log C = \log\log(n^C) \;.$$

Equation (1) then follows from the fact that the logarithm is monotonically increasing.

3 A little discussion and a note on taking the logarithm one time, two times, or three times

The above proof works by applying the change of variables $x := \log\log n$ and considering the inequality $\log\log(2^n) \geq \log\log(n^C)$. This shows that in order to prove Equation (1), it suffices to prove that for any constant C' (and specifically for $C' := \log C$) that there exists $x_{C'}$ such that

$$2^x \geq x + C', \text{ for all } x \geq x_{C'} \;. \tag{3}$$

In other words, by making this change of variables and twice taking the logarithm of both sides, we have managed to reduce the question of whether an exponential grows faster than *any* polynomial to the seemingly much simpler question of whether the exponential 2^x is larger than x by an arbitrarily large additive constant. The simple algebraic manipulation in the proof above just amounts to proving that taking $x_{C'} := C' + 2$ suffices for Equation (3) (though once one has reduced to Equation (3), there are many more-or-less equally simple ways to finish the proof).

Given the description above, it is natural to ask what happens if one "takes *one* logarithm instead of two." In particular, we can apply the change of variables $w := \log n$. Then, by considering the inequality $\log(2^n) \geq \log(n^C)$, we see that in order to prove Equation (1), it suffices to prove that there exists w_C such that

$$2^w \geq Cw, \text{ for all } w \geq w_C. \tag{4}$$

[3] One might complain that the use of Equation (2) is simply passing the buck. But, Equation (2) can be proven in many very elementary ways. For example, one can note that it is immediate for, say, $y \leq 1$ and then show that $2^y - y$ is an increasing function for $y \geq 1$ by differentiating. Or, more-or-less equivalently, one can simply note that Equation (2) follows from the even more trivial inequality $2x \geq x + 1$ for $x \geq 1$. Or, one can notice that for $y \geq 1$, $2^{\lfloor y \rfloor}$ counts the number of subsets of a set of size $\lfloor y \rfloor$ and since there are $\lfloor y \rfloor$ singleton subsets and one subset of size zero, this implies that $2^y \geq 2^{\lfloor y \rfloor} \geq \lfloor y \rfloor + 1 > y$.

The new inequality with the multiplicative constant in Equation (4) is nearly as easy to prove as the analogous inequality with the additive constant in Equation (3) (unsurprisingly, since it is easy to prove that they are equivalent).[4] But, it is somehow a bit less shocking that Equation (4) implies Equation (1). So, the proof loses some of its shine in this light, and we therefore prefer the "two logarithm" version of the proof that goes through Equation (3) to the "one logarithm" version that goes through Equation (4). (Versions of this "one-logarithm proof" are rather common.)

Of course, if two logarithms are (arguably) better than one, then it becomes natural to ask whether three logarithms are better than two. So, let $z := \log\log\log n$ and notice that by taking the logarithm of both sides of Equation (1) three times, we see that it suffices to prove that for every constant C' (and specifically $C' := \log C$ as above) there exists $z_{C'}$ such that

$$2^z \geq \log(2^z + C'), \text{ for all } z \geq z_{C'}. \tag{5}$$

Unfortunately, Equation (5) is not quite as simple as Equations (3) and (4), simply because $\log(2^z + C')$ does not simplify nicely (unlike $\log(2^{Cw})$ and $\log(C2^x)$). If one is willing to accept the basic inequality $\log(2^z + C') \leq z + C''/2^z$ for, say, $C'' := 2C'$, then we see that it actually suffices to prove that

$$2^z \geq z + C''/2^z \ ,$$

for sufficiently large z, which is of course quite easy to prove. A more elementary approach simply notices that for $z \geq \log C'$, $\log(2^z + C') \leq z + 1$, which reduces proving Equation (5) to proving Equation (3) in the special case when $C' = 1$. Finishing from there is of course quite simple, though it seems difficult to argue that this "three-logarithm proof" is simpler than the one- or two-logarithm proofs.

Of course, if one is willing to forget about simplicity, then one sees that after taking $k + 2$ logarithms, proving Equation (1) amounts to proving that

$$2^r \geq \log^{(k)}(f^{(k)}(r) + C') \ ,$$

for sufficiently large r, where we write $\log^{(k)}$ for the iterated logarithm and $f^{(k)}(x)$ for the iterated exponential. (E.g., $f^{(3)}(x) := 2^{2^{2^x}}$.) Using the inequality $\log^{(k)}(f^{(k)}(r) + C') \leq r + C''/f^{(k)}(r)$ for some appropriate constant C'', we see that in order to prove Equation (1), it suffices to show that $2^r - r$ is eventually larger than $C''/f^{(k)}(r)$. In other words, in order to prove that an exponential is superpolynomial, it suffices to beat Equation (2) simply by an additive $C''/f^{(k)}(y)$ for our favorite choice of a constant k. This is rather striking, though certainly there is no need to bring large towers of twos into this discussion.

Acknowledgments. Thanks to Huck Bennett, Sasha Golovnev, and Bobby Kleinberg for tolerating my overly enthusiastic ramblings about this. Thanks to Bobby Kleinberg and Michael Ngo for identifying stupid typos in earlier versions of this work. Apologies to the speaker whose talk I missed because I slept through my alarm after staying up all night writing this silliness.

[4]For completeness, we note that one can prove Equation (4) by, e.g., noting that for $w \geq 4C$ (and thus $n = 2^w \geq 2^{4C}$, just like the above), we have

$$2^w = (2^{w/2})^2 \geq (w/2)^2 = (w/4) \cdot w \geq Cw \ ,$$

as needed.

References

[Twi22] A Twitter thread on proofs that the exponential function is superpolynomial. https://x.com/NoahSD/status/1485747144808189954, 2022.