Non-regularity Proofs

Peter Dixon

February 26 2021

1 Admin Stuff

Current topic: Computability and Turing machines (Ch. 28-34)

HW5 is all on regular languages.

HW6 will cover the end of regular languages (non-regularity proofs) and the beginning of Turing machines.

2 A Nonregularity Proof

One last bit of regular language stuff.

On Monday, you saw a proof that $\{0^n 1^n\}$ is not regular. We're going to do one more.

We look at "first extensions":

- An extension of x is a string that puts x in the language ($xy \in L$)
- A_x is all extensions of x
- $A_x^{(1)}$ is the first extension of x
- $A^{(1)}$ is the first extension of every string

We're going to prove that $\{0^p \mid p \text{ is prime}\}$ is not regular. To do that, we're going to prove a more general statement:

- Any tally language (subset of $\{0^*\}$) that has arbitrarily large gaps between elements is not regular
- $\{0^p \mid p \text{ is prime}\}$ has arbitrarily large gaps between elements.

Let's define "arbitrarily large gaps". Let I be an infinite set of numbers. We'll define n^I to be "the next thing after n in I", and $GAPS_I$ to be $\{n^I - n \mid n \in I\}$.

Ex. If I is the set of all even numbers, $I = \{0, 2, 4, \ldots\}$. $GAPS_I$ contains $\{2-0, 4-2, 6-4, \ldots\} = \{2\}$.

Now we want to prove: If $GAPS_I$ is infinite, then $B_I = \{0^i \mid i \in I\}$ is not regular. We'll connect $GAPS_I$ to extensions.

Pick some $0^n \in B_I$. The first extension is λ (because $0^n\lambda = 0^n \in B_I$) . The second extension is the smallest string y such that $0^n y \in B_I$. y is the gap between n and n^I (the next thing in I). In other words, $A^{(2)} = \{0^i \mid i \in GAPS_I\}$. Since $GAPS_I$ is infinite, $A^{(2)}$ is infinite, so B_I is not regular.

Now for part 2. We want to show there's arbitrarily large gaps between prime numbers.

That means we need to show: for any m, there is a prime number p such that the next largest prime is m greater than p.

To show THAT, we're going to show there are prime numbers p, q such that $q \geq p + m$ and everything between p and q is not prime.

We're gonna make a really big prime.

Take p to be the largest prime smaller than $m! + 1$. (That's $m * (m-1) * \cdots * 2 * 1 + 1$.)

- Nothing between p and $m!+1$ is prime, because p is the largest such prime.
- Nothing between $m! + 1$ and $m! + m$ is prime, because $m! + k$ is divisible by k (if a and b are divisible by k then $a + b$ is too)
- So, the next prime q after p is at least $m! + m$, so $q - p \geq m$.

So, $\{0^p \mid p \text{ is prime}\}$ is not regular.