CSC110 Fall 2022 Assignment 2: Logic, Constraints, and Wordle!

Jaeyong Lee

October 12, 2022

Part 1: Conditional Execution

Complete this part in the provided `a2_part1_q1_q2.py` and `a2_part1_q3.py` starter files. Do **not** include your solutions in this file.

Part 2: Proof and Algorithms, Greatest Common Divisor edition

1. This can be explained using the following property of division: $\forall n, d \in \mathbb{Z}^+, d|n \Rightarrow d \leq n$

   According to this property of division, if d divides n, then d is lesser than or equal to n. From the precondition of the function, we know that m is lesser than or equal to n. Since d must divide both n and m to be considered a common divisor, we can conclude that the possible divisors must only go from 1 to the lower of the two integers m and n, which is m in the case of this function.

2. This can be explained using the following property of division: $\forall n \in \mathbb{Z}, 1|n$. Essentially, what this property tells us is that for every integer n, 1 divides n. Therefore, the set common_divisors will never be empty since 1 is a common divisor of every integer, meaning we don't have to check for a case in which common_divisors is empty before calling max(common_divisors).

3. *Proof.* $\forall n, m, d \in \mathbb{Z}, d|m \land m \neq 0 \Rightarrow (d|n \iff d|n \,\%\, m)$

   Suppose $d|m \land m \neq 0$. We wish to show that $(d|n \iff d|n \,\%\, m)$. Since this is a bi-conditional, we will split the proof into two separate parts.

   Part 1: $d|n \Rightarrow d|n \,\%\, m$

   Assume $d|n$. We wish to show that $d|n \,\%\, m$. We define $n \,\%\, m$ to be equal to the unique integer r that satisfies $0 \leq r < |m|$ and $\exists q \in \mathbb{Z}, n = qm + r$. From this, we know that $n = qm + n \,\%\, m$, which can be rearranged to $n - qm = n \,\%\, m$.

   Writing this as $n \,\%\, m = n + (-qm)$ shows that we can use the given property $\forall n, m, d, a, b \in \mathbb{Z}, d|n \land d|m \Rightarrow d|(an + bm)$ to show that $n \,\%\, m = an + bm$ when we let a = 1 and b = -q.

   From the given property, we know that $d|(an + bm)$ when $d|n$ and $d|m$. We've assumed $d|n$ and $d|m$ to be true in our proof. We have shown $d|(an + bm)$ to be equivalent to $d|n \,\%\, m$. Therefore, we have proven $d|n \Rightarrow d|n \,\%\, m$.

   Part 2: $d|n \,\%\, m \Rightarrow d|n$

   Assume $d|n \,\%\, m$. We want to show that $d|n$.
   $d|n$ can be expressed as $\exists k_1 \in \mathbb{Z}, n = dk_1$
   $d|n \,\%\, m$ can be expressed as $\exists k_2 \in \mathbb{Z}$, $n \,\%\, m = dk_2$

Lastly, we assumed from the very beginning that $d|m$, which can be expressed as $\exists k_3 \in \mathbb{Z}, m = dk_3$ From part one of the proof, we know that $n = qm+n\%m$. This can now be rewritten as $n = qdk_3+dk_2$. $n = d(qk_3+k_2)$. Now, we know that qk_3+k_2 will produce some integer because q, k_3, k_2 are all defined to be integers. Let $(qk_3 + k_2) = k_1$. Now, we can write that $n = dk_1$, which is what we wanted to originally show.

Therefore, since we've proven $d|n \Rightarrow d|n \,\%\, m$ and $d|n \,\%\, m \Rightarrow d|n$, we can conclude that the biconditional conclusion of the original statement is true, thus proving the whole original statement to be true.

□

4. if n % m is equal to zero, then we know that the greatest common divisor between n and m must be m because numbers greater than m will not be a common divisor of m due to the following property: $\forall n, d \in \mathbb{Z}^+, d|n \Rightarrow d \leq n$. This essentially states that for some number d to divide some number n, d must be lesser than or equal to n. So, we can conclude that numbers greater than m cannot divide m and therefore cannot be considered a potential gcd between two integers m and n. Any integers lower than m that may be a common divisor between m and n are not helpful as we are looking for the greatest common divisor.

   In terms of the range for possible_divisors, we define it to be range(1, r+1). This can be explained using the following statement: $\forall n, m, d \in \mathbb{Z}, d|m \land m \neq 0 \Rightarrow (d|n \iff d|n \,\%\, m)$. What this tells us is that for some integer d to be a possible common divisor of both m and n, d must also divide r, which is defined to be $n \,\%\, m$. Thus, we know that d must be less than or equal r from the following property: $\forall n, d \in \mathbb{Z}^+, d|r \Rightarrow d \leq r$. Therefore, possible_divisors will be in range(1, r+1).

```
def gcd(n: int, m: int) -> int:
    """Return the greatest common divisor of m and n.

    Preconditions:
    - 1 <= m <= n
    """
    r = n % m

    if r == 0:
        return m
    else:
        possible_divisors = range(1, r+1)
        common_divisors = {d for d in possible_divisors if divides(d, n) and divides(d, m)}
        return max(common_divisors)
```

Part 3: Wordle!

Complete this part in the provided `a2_part3.py` starter file. Do **not** include your solutions in this file.