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

Vrinda Subhash

October 10, 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 approach uses range(1, m + 1) instead of range(1, n + 1) because m is less than (or equal to) n. One of the properties of divisibility we learned in Lecture 9, is that for all n and d that are positive integers, if d divides n, then d is less than or equal to n. Using this property, we know that the greatest common divisor must be less than or equal to m and n. Since n might be greater than m, range(1, n + 1) might give us a list of invalid possible_divisors (as they might be greater than m which goes against the divisibility property).

2. We know the common_divisors will not be an empty collection because possible_divisors includes 1 in the range(1, m + 1). Using the divisibility property from Lecture 9 that states that every integer is divisible by 1, we know that common_divisors will at least contain the value 1, therefore it cannot be an empty collection, and the max function can be called on it.

3. *Proof.* Want to show: $\forall n, m, d \in \mathbb{Z}, d|m \land m \neq 0 \implies (d|n \iff d|n\%m)$
   Let n, m, d $\in \mathbb{Z}$
   I can assume: $d|m \land m \neq 0$
   I want to show that $d|n \iff d|n\%m$
   To show that, I need to prove:
   (1) $d|n \implies d|n\%m$
   (2) $d|n\%m \implies d|n$
   Proving (1):
   Assume $d|n$.
   We known $d|m$ since it was one of our assumptions.
   Want to show: $d|n\%m$.
   (a) Since $d|n, \exists a \in \mathbb{Z}$ such that n = da
   (b) Since $d|m, \exists b \in \mathbb{Z}$ such that m = db
   d is the gcd.
   By Quotient Remainder Theorem:
   $0 \leq r < |m|$ and $\exists c \in \mathbb{Z}$ such that
   $n\%m = r \rightarrow mc + r = n$
   Substituting values from (a) and (b) for n and m:
   $(db)c + r = da$
   $dbc + r = da$
   $r = da - dbc$

$r = d(a - bc)$
$(a - bc) \in \mathbb{Z}$ because $a, b, c \in \mathbb{Z}$
This shows that $d|r$ because $\exists p \in \mathbb{Z}$ such that r = dp.
$r = n\%m$
Therefore: $d|n\%m$
Proving (2):
Assume $d|n\%m$.
We know $d|m$ since it was one of our assumptions.
Want to show: $d|n$
Since $d|m, \exists b \in \mathbb{Z}$ such that $m = bd$.
This means m is a multiple of d.
Since $d|n\%m, n\%m$ is a multiple of d.
By Quotient Remainder Theorem:
$0 \leq r < |m|$ and $\exists c \in \mathbb{Z}$ such that
$n\%m = r \rightarrow mc + r = n$
mc is a multiple of d because $m = bd$, and $c \in \mathbb{Z}$.
r is a multiple of d because $r = n\%m$ and $d|n\%m$.
$\exists x \in \mathbb{Z}$ such that $mc = dx$
$\exists y \in \mathbb{Z}$ such that $r = dy$
$mc + r = n$ can be rewritten as:
$dx + dy = n$
$d(x + y) = n$
This shows that n is a multiple of d.
Therefore: $d|n$
I have now proven (1) and (2) which proves that $d|n \iff d|n\%m$.
Therefore: $\forall n, m, d \in \mathbb{Z}, d|m \wedge m \neq 0 \implies (d|n \iff d|n\%m)$. $\square$

4. If the mod of two numbers is 0, the gcd is the value you divided by, which is why I added "return m" after the first branch of the if-statement. The other change I made is changing the range of possible_divisors to be range(1, r + 1) because the remainder will be a multiple of the gcd, and the remainder will be greater than or equal to the gcd, so when looking for the gcd, you know it will be in the range(1, r+1). And r is less than m which is what makes the range(1, r+1), smaller than range(1, m+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.