

FINAL EXAM SOLUTIONS

Q1. We can prove the correctness of Euclid’s extended algorithm by using the following loop invariant which consists of four assertions:

$$am + bn = d, \quad xm + yn = c, \quad d > 0, \quad \gcd(c, d) = \gcd(m, n). \quad (\text{LI})$$

The basis case:

$$\begin{aligned} am + bn &= 0 \cdot m + 1 \cdot n = n = d \\ xm + yn &= 1 \cdot m + 0 \cdot n = m = c \end{aligned}$$

both by line 1. Then $d = n > 0$ by precondition, and $\gcd(c, d) = \gcd(m, n)$ by line 1. For the induction step assume that the “primed” variables are the result of one more full iteration of the loop on the “un-primed” variables:

$$\begin{aligned} a'm + b'n &= (x - qa)m + (y - qb)n && \text{by line 8} \\ &= (xm - yn) - q(am + bn) \\ &= c - qd && \text{by induction hypothesis} \\ &= r && \text{by lines 3 and 4} \\ &= d' && \text{by line 8} \end{aligned}$$

Then $x'm = y'n = am + bn = d = c'$ where the first equality is by line 8, the second by the induction hypothesis, and the third by line 8. Also, $d' = r$ by line 8, and the algorithm would stop in line 5 if $r = 0$; on the other hand, from line 4, $r = \text{rem}(c, d) \geq 0$, so $r > 0$ and so $d' > 0$. Finally,

$$\begin{aligned} \gcd(c', d') &= \gcd(d, r) && \text{by line 8} \\ &= \gcd(d, \text{rem}(c, d)) && \text{by line 4} \\ &= \gcd(c, d) && \text{see problem 1.15 in the book} \\ &= \gcd(m, n). && \text{by induction hypothesis} \end{aligned}$$

For partial correctness it is enough to show that if the algorithm terminates, the post-condition holds. If the algorithm terminates, then $r = 0$, so $\text{rem}(c, d) = 0$ and $\gcd(c, d) = \gcd(d, 0) = d$. On the other hand, by (LI), we have that $am + bn = d$, so $am + bn = d = \gcd(c, d)$ and $\gcd(c, d) = \gcd(m, n)$.

Q2. The proof is simple: define S to be promising if for all the nodes v in S , $d(v)$ is indeed the shortest distance from s to v . We now need to show by induction on the number of iterations of the algorithm that “ S is promising” is a loop invariant. The basis case is $S = \{s\}$ and $d(s) = 0$, so it obviously holds. For the induction step, suppose that v is the node just added, so $S' = S \cup \{v\}$. Suppose that there is a shorter path in G from s to v ; call this path p (so p is just a sequence of nodes, starting at s and finishing at v). Since p starts inside S (at s) and finishes outside S (at v), it follows that there is an edge (a, b) such that a, b are consecutive nodes on p , where a is in S and b is in $V - S$. Let $c(p)$ be the cost of path p , and let $d'(v)$ be the value the algorithm found; we have $c(p) < d'(v)$. We now consider two cases: $b = v$ and $b \neq v$, and see that both yield a contradiction. Thus, no such path p exists. If $b = v$, then the algorithm would have used a instead of v . If $b \neq v$, then the cost of the path from s to b is even smaller than $c(p)$, so the algorithm would have added b instead of v .

Q3. First note that the second argument decreases at each recursive call, but by definition of remainder, it is non-negative. Thus, by the LNP, the algorithm terminates. We prove partial correctness by induction on the value of the second argument. In the basis case $n = 0$, so in line 1 $b \leftarrow n = 0$, so in line 2 $b = 0$ and the algorithm terminates in line 3 and returns $(a, 1, 0) = (m, 1, 0)$, so $mx + ny = m \cdot 1 + n \cdot 0 = m$ while $d = m$, and so we are done.

In the induction step we assume that the recursive procedure returns correct values for all pairs of arguments where the second argument is $< n$ (thus, we are doing complete induction). We have that

$$\begin{aligned} (d, x, y) &\leftarrow \text{Extended-Euclid}(b, \text{rem}(a, b)) \\ &= \text{Extended-Euclid}(n, \text{rem}(m, n)), \end{aligned}$$

from lines 1 and 5. Note that $0 \leq \text{rem}(m, n) < n$, and so we can apply the induction hypothesis and we have that:

$$n \cdot x + \text{rem}(m, n) \cdot y = d = \text{gcd}(n, \text{rem}(m, n)).$$

First note that by problem 1.15 in the textbook we have that $d = \text{gcd}(m, n)$. Now we work on the left-hand side of the equation. We have:

$$\begin{aligned} &n \cdot x + \text{rem}(m, n) \cdot y \\ &= n \cdot x + (m - \text{div}(m, n) \cdot n) \cdot y \\ &= m \cdot y + n \cdot (x - \text{div}(m, n) \cdot y) \\ &= m \cdot y + n \cdot (x - \text{div}(a, b) \cdot y) \end{aligned}$$

and we are done as this is what is returned in line 6.

Q4. This is section 4.3 in the textbook. $R(i, j)$ is defined in equation (4.1) on page 55. Part (b) is problem 4.8, which has a solution on page 67.

Q5. The solution to this is the proof of theorem 5.10 on page 80 in the textbook.

Q6. This is section 6.4.1 in the textbook. See, in particular, the last paragraph of this section.