Week 13 Tutorial Solutions

2.2a Thinking about number theory

Claim: There is no such value. Proof: Suppose (towards a proof by contradiction) that there *is* an integer x such that both congruences are true. Then from the first congruence, we know that $x = 7 + 9p = 1 + 3(2 + 3p)$ for some integer p, so $remainder(x, 3) = 1$. From the second congruence, we know that $x = 5 + 12q = 2 + 3(1 + 4q)$ for some integer q, so $remainder(x, 3) = 2$. Thus $1 = remainder(x, 3) = 2$. But $1 \neq 2$: contradiction! So our assumption must be false, and instead such an x does *not* exist. □

16 Proof by Contradiction

a) Suppose not. That is, suppose $\sqrt{2} + \sqrt{6} \geq \sqrt{15}$. Then we get the following:

$$\begin{aligned}
\sqrt{2} + \sqrt{6} &\geq \sqrt{15} \\
2 + 2\sqrt{12} + 6 &\geq 15 && \text{(both sides were positive; square them)} \\
2\sqrt{12} &\geq 7 \\
48 &\geq 49 && \text{(both sides were positive; square them)}
\end{aligned}$$

This is a contradiction, so our initial supposition must be false. Thus we have shown $\sqrt{2} + \sqrt{6} < \sqrt{15}$.

b) Assume towards contradiction that there are a *finite* number of integers of the form $4k + 3$. Then there must be some largest of them. *(For claims where it isn't obvious, one should first show that there is at least one before claiming there's a largest - in this case we could say* $43 = 4 \cdot 10 + 3$ *so there's at least one.)* Let that largest be $m = 4y + 3$. Now consider $m + 4$. It is larger than m, so it does not have the $4k + 3$ form. Yet $m + 4 = (4y + 3) + 4 = 4(y + 1) + 3$, so it *does* have the $4k + 3$ form - contradiction! Thus our assumption is false and there are actually infinitely many integers of that form.

c) Suppose not. That is, suppose there *is* a rational number r such that $r^3 + r + 1 = 0$. Then let $r = \frac{a}{b}$, where a and b are integers in lowest terms, and we get

$$\begin{aligned}
r^3 + r + 1 &= 0 \\
\frac{a^3}{b^3} + \frac{a}{b} + 1 &= 0 \\
a^3 + ab^2 + b^3 &= 0
\end{aligned}$$

Now, consider each of the following three cases:

Case 1: a and b are both even. But then r isn't in lowest terms; contradiction.

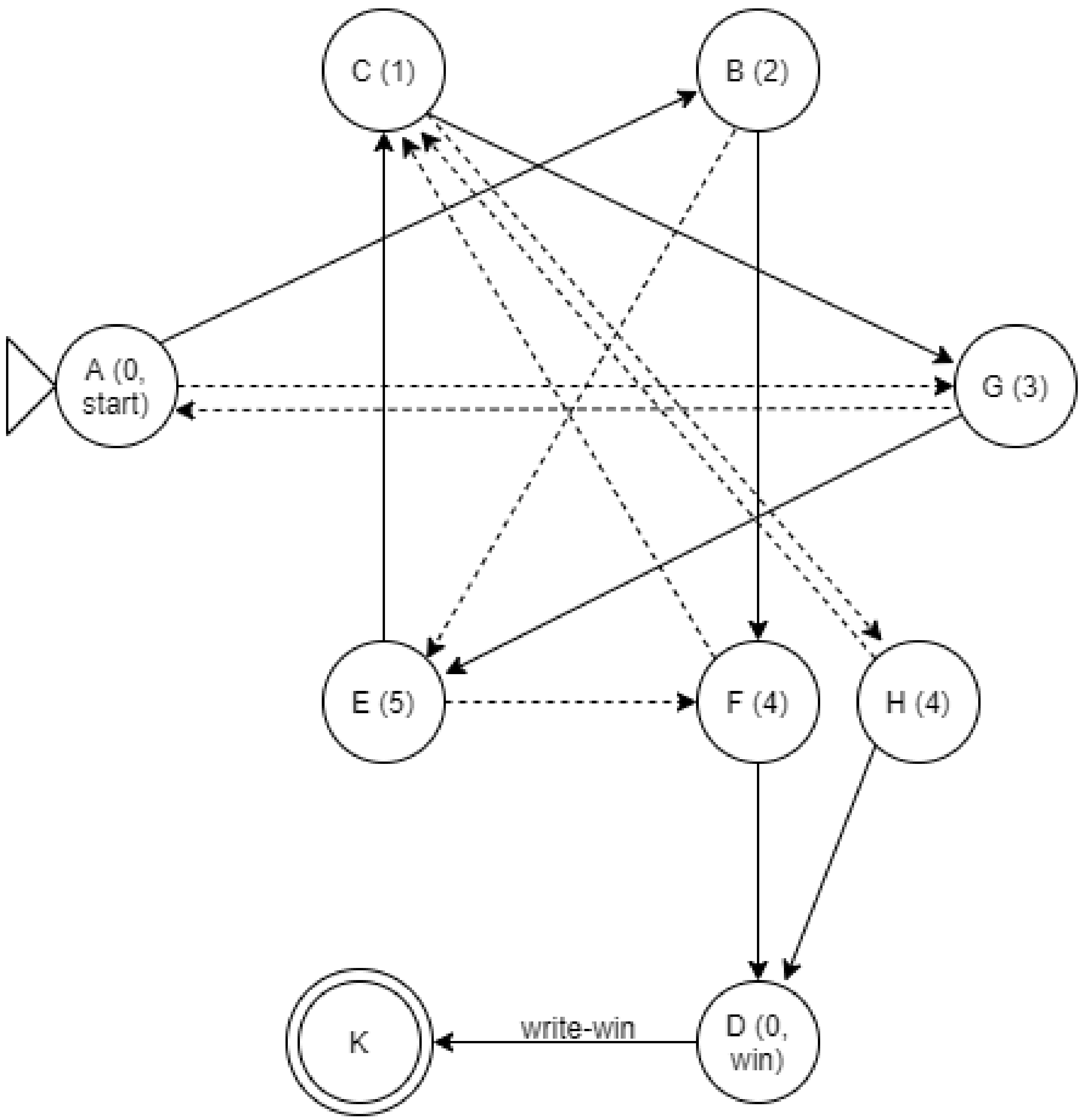
Case 2: exactly one of a and b is odd. Then two of the terms in $a^3 + ab^2 + b^3$ are even and the third is odd, so they can't sum to zero; contradiction.

Case 3: a and b are both odd. Then all three terms are odd, so they can't sum to zero; contradiction.

In all three cases, we have a contradiction, so our supposition (the negated claim) can't be true. Thus $r^3 + r + 1 = 0$ does *not* have any rational roots; QED

18.1 Recovering a State Diagram From a Transition Function

1. The original state diagram:



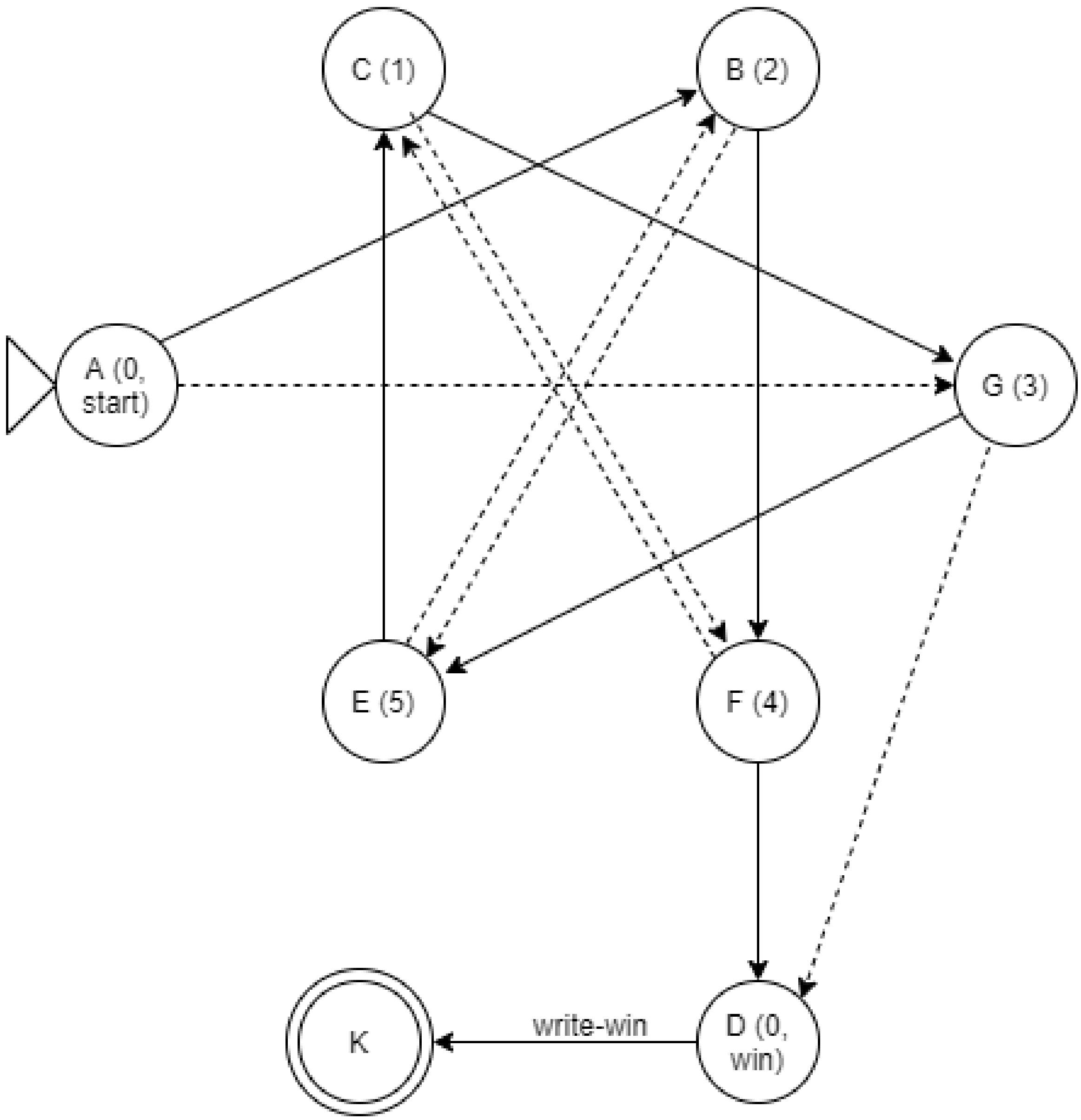
   (For readability, unlabeled solid arrows are action "2", and dashed arrows are action "3". Each state has in parentheses the current remainder upon division by 6.)

2. There are two incorrect transition arrows. $\delta(E, 3)$ should be $\{B\}$ because E is 5, B is 2, and $5 + 3 \equiv 2 \pmod 6$. $\delta(G, 3)$ should be $\{D\}$, since getting back to remainder zero

should begin the end-game sequence.

3. We don't need to keep both of H and F, since they both have the same outgoing transitions (because they both represent the remainder 4). *(Note that we* do *need to keep both A and D, since for remainder 0 we need to distinguish between whether the game has just begun (and so nobody has won), or the game is now ending.)*

4. The diagram with those two arrows fixed and the extra state removed:



18.2 A Simple State Diagram

a) `states:   3         4            fail`
   `actions:   password   unauthorized`

b) $S = \{start, 1, 2, 3, 4, 5, done, error, finished, fail\}$

$A = \{requestpage, login, shippage, notfound, password, unauthorized\}$

c) $\delta(1, requestpage) = \emptyset$

$\delta(3, password) = \{4\}$

$\delta(start, requestpage) = \{1, 2, 5\}$

d) $10 \cdot 6 = 60$

e) $1, 2, 5$ can be combined into a single state. You could almost certainly combine "done" and "finished"; you could probably also combine "error" and "fail", though it depends on how this information is likely to be used (e.g. do we want later processing to be able to report different specific errors). *(This problem is a bit open-ended and open to interpretation.)*

Magic Word

All three actions are possible from any state, but for readability, all arrows returning to the start state have been omitted from the diagram below (so e.g. there is an implicit arrow from "mam" back to the start state with label "l").