Foundations of Computer Science HW 3

Greg Stewart

February 16, 2018

Q1

4.13(h) If $n \in \mathbb{Z}$, then $n^2 - 3$ is not divisible by 4.

Suppose that $n^2 - 3$ *is* divisible by 4. Then $n^2 - 3 = 4k$ for $k \in \mathbb{Z}$, so

$$n^2 = 4k + 2$$

There are two cases to consider here—when n is even, and when n is odd.

For n odd, we know that n^2 is odd, but the right hand side of the above inequality is even, so we immediately have a contradiction.

For n even, $n = 2l$ for $l \in \mathbb{Z}$ so we end up with the expression

$$4l^2 = 4k + 2$$

From the left hand side, $4l^2 \mod 4 = 0$ and from the right, $(4k+2) \mod 4 = 2$, and since these remainders are different, the equality is impossible, so we have another contradiction.

As both cases lead to contradiction, it must be true that $n^2 - 3$ is not divisible by 4.

4.13(l) When dividing n by d, the quotient q and remainder $0 \leq r < d$ are unique.

Suppose there is also q' and r' such that $0 \leq r < b$ and $-b < -r' \leq 0$ for $a = bq + r = bq' + r'$. we can rearrange these inequalities so $-b < r - r' < b$. The two equations for a can also be arranged so $bq' - bq = r - r'$, whcih means $r - r'$ is divisible by b. For $r - r' \neq 0$, this implies $b \leq r - r'$, which is clearly a contradiction. We must have that $r = r'$ and $q = q'$, so r and q are unique.

Q2

4.28(b) $A = \{7k, k \in \mathbb{N}\}$ and $B = \{3k, k \in \mathbb{N}\}$. Prove that $A \cap B \neq \emptyset$

In set A, all of the elements are multiples of 7, and in B, all elements are multiples of 3. $A \cap B$ contains all the elements that A and B share, so what must be shown is that there is at least one element that is divisible by both 7 and 3. $3 \cdot 7 = 21$, and obviously 21 is divisible by both 3 and 7, so it is contained within both sets. Thus $A \cap B$ contains, at the very least, the number 21. Thus $A \cap B \neq \emptyset$.

4.28(c) $A = \{4k - 3, k \in \mathbb{N}\}$ and $B = \{4k + 1, k \in \mathbb{N}\}$. Prove or disprove $A = B$.

While in general, $4k - 3$ and $4k + 1$ will give equivalent elements for $n \geq 2$, the important value for k here is a base case—the first element of $\mathbb{N}$. When $k = 1$, we have in A

$$4(1) - 3 = 1$$

while in B we have

$$4(1) + 1 = 5$$

. So the first element of A, a_0, is less than the first in B, b_0. Since there is a value $x \in A$ for which $x \notin B$, $A \not\subseteq B$, so $A \neq B$.

Q3

5.3(c) $P(2)$ is T and $P(n) \implies (P(n^2) \wedge P(n-2))$ is T for $n \geq 1$.

Using the implication, we have

$$P(2) \implies (P(4) \wedge P(0))$$

$$P(4) \implies (P(16) \wedge P(2))$$

$$P(16) \implies (P(256) \wedge P(14)$$

$$P(256) \implies (P(65536) \wedge P(254)) \text{ and } P(14) \implies (P(196) \wedge P(12))$$

As is becoming obvious, each new implication in the chain leads to every even n below n^2 giving $P(n)$ as true. This is due to the $P(n-2)$ part of the predicate. The evenness comes from starting with $P(2)$—each n^2 is even, so every subsequent n^2 is of course even, and if n is even then $n-2$ is also even. So finally, we have the conclusion that $P(n)$ is true for all n even.

Q4

5.10(d) Prove by induction: $3^n > n^2$.

For the base case $n = 1$, we have

$$3^1 = 3 > 1^2 = 1$$

which is obviously true. Let's assume that $3^n > n^2$ for some n. Then for $n+1$ we have

$$\begin{aligned} 3^{n+1} &> (n+1)^2 \\ 3 \cdot 3^n &> n^2 + 2n + 1 \\ &> 3n^2 > n^2 + 2n + 1 \end{aligned}$$

The last step above is true for sufficiently large n, which we must solve for.

$$\begin{aligned} 3n^2 &> n^2 + 2n + 1 \\ 3n^2 - n^2 - 2n - 1 &> 0 \\ 2n^2 - 2n - 1 &> 0 \end{aligned}$$

Solving for n we get $n = \frac{1+\sqrt{3}}{2} \approx 1.4$, so this is true for all $n \geq 2$, and since we have the base case as true, we can say that $3^n > n^2$ for all $n \geq 1$.

Q5

5.14 Prove by induction that every $n \geq 1$ is a sum of distinct powers of 2.

Take the base case, $n = 0$. $0 \cdot 2^0 = 0 = n$ so this is true for the base case. It's clearly also true for $n = 1$: $2^0 = 1 = n$. Assume that for some n, for all m such that $0 \leq m \leq n$, $P(m)$ is true—m can be written as a sum of distinct powers of 2.

Consider the $n+1$ case. Let 2^k be the largest power of 2 less than or equal to $n+1$. $2^k \geq 1$ for any $k \in \mathbb{N}$, so

$$n + 1 - 2k \leq n + 1 - 1 = n$$

, which, using the assumption, means that $n+1-2^k$ is also the sum of distinct powers of 2. If A is the set of these powers of 2, and a_i are the elements in A, then

$$n+1 = 2^k + \sum_i a_i$$

Since all the powers of 2 in A are distinct by the assumption, it must be shown that $2^k \notin A$. Assume that $2^k \in A$. Then the sum of powers of 2 in S is $n+1-2^k$, which leads to

$$\begin{aligned} 2^k &\leq n+1-2^k \\ 2 \cdot 2^k &\leq n+1 \\ 2^{k+1} &\leq n+1 \end{aligned}$$

So 2^k is *not* the largest power of 2 which is less than or equal to $n+1$, so $2^k \notin A$. Therefore $n+1$ can be expressed as a sum of distinct powers of 2, so $P(n) \implies P(n+1)$ and any natural number can be written as a sume of distinct powers of 2.

Q6

5.16 Let A be a finite set of size $n \geq 1$; prove by induction that $|\mathscr{P}(A)| = 2^n$

For the base case, take $|A| = 0$, so $A = \emptyset$, and the empty set is its only subset, so $|\mathscr{P}(A)| = 1 = 2^0$.

Assume that for $|A| = n$, it is true that $|\mathscr{P}(A)| = 2^n$. Let B be a set with one more element than A, so we can say $B = A \cup \{b\}$. The subsets of B can be separated into two categories—some include b, and some do not. In the latter case, they are exactly the subsets of A, so there are 2^n of these. The former is all of these subsets plus b, which we can write as $C \cup b$ where $C \in \mathscr{P}(A)$. There are 2^n possibilities for Z, so so there are 2^n examples of $Z \cup b$. Thus,

$$|\mathscr{P}(B)| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$$

So by induction it's true that $|\mathscr{P}(A)| = 2^n$.

Q7

5.30 Prove you can make any postage greater than 12 cents using only 4 and 5 cent stamps.

We need a few base cases here. $12 = 3 \cdot 4 + 0 \cdot 5$. $13 = 2 \cdot 4 + 1 \cdot 5$. $14 = 1 \cdot 4 + 2 \cdot 5$. $15 = 0 \cdot 4 + 3 \cdot 5$.

Okay, let's assume that for $n \geq 15$, we have that

$$k \cdot 4 + l \cdot 5 = n$$

For $n+1$, there are two cases. In the first case, $k > 0$, so all we need to do is subtract one from k and add one to l, i.e.

$$(k-1) \cdot 4 + (l+1) \cdot 5 = n+1$$

For the $k = 0$ case, we must subtract 3 from l and add 4 to k to get the next number, so

$$(k+4) \cdot 4 + (l-3) \cdot 5 = n+1$$

So $P(n) \implies P(n+1)$ for all $n \geq 12$.

Q8

5.47(a) Robot moves one diagonal step at a time. Prove no move sequence can move the robot one square to the right of its initial position.

Let (x, y) be the position of the robot on the grid, and let $(0, 0)$ be its starting position. A brief inspection reveals that after the first step, the robot's position could be any of $(1, 1)$, $(1, -1)$, $(-1, 1)$, or $(-1, -1)$. In the next step, there are of course more possible positions, including back at $(0, 0)$, but none of these are the position $(1, 0)$, to the right of the intiial position. Going in any direction for more steps seems to reveal a relationship between x and y—$x + y$ is always even, and we call this predicate $P(n)$. We prove this by induction.

The $n = 0$ step is true because for $P(0)$ we have $0 + 0 = 0$, which is even. Now assume that $P(n)$ is even, so we know $x + y$ is even. Consider $P(n + 1)$. There are four possible moves for the robot, so there are four cases to look at.

First, $P(n + 1) = (x + 1, y + 1)$. The sum is $x + 1 + y + 1 = x + y + 2$ and since $x + y$ is even, the sum is even too, so $P(n + 1)$ is even.

For the move to $(x + 1, y - 1)$, the sum is just $x + y$, which we know is even, so $P(n + 1)$ is even.

Now for $(x - 1, y + 1)$, the sum is again just $x + y$ so $P(n + 1)$ is even.

Finally, for $(x - 1, y - 1)$, the sum is $x + y - 2$, which is even, so $P(n + 1)$ is even.

In all the cases, $P(n + 1)$ is even, so the robot can never be on a square whose coordinates sum to an odd number, as is the case with $(1, 0)$, so it's impossible for the robot to ever end up there.

5.47(b) A move changed! The (x+1,y+1) move is now (x+1, y+2). Prove the robot can go to any coordinate (m, n).

Let's call the predicate $P(k)$: the robot can reach any square (m, n) in a finite sequence of moves. By inspection, one can see that all of the squares surrounding the initial position are reachable by the robot in a finite number of moves, and these can be shown easily. The formula for the next location (m, n) is

$$(m, n) = a(x + 1, y + 2) + b(x + 1, y - 1) + c(x - 1, y + 1) + d(x - 1, y - 1)$$

So aside from the trivial cases, we have surrounding the initial position:

$$\begin{aligned}
(1, 0) &\implies (a, b, c, d) = (1, 1, 1, 0) \\
(0, -1) &\implies (a, b, c, d) = (1, 1, 2, 0) \\
(-1, 0) &\implies (a, b, c, d) = (1, 0, 2, 0) \\
(0, 1) &\implies (a, b, c, d) = (1, 0, 1, 0) \\
(1, 1) &\implies (a, b, c, d) = (2, 1, 2, 0)
\end{aligned}$$

What this means is that, from any position on the grid, a square adjacent or diagonally adjacent to that position can be reached in a finite number of moves. Since all eight surrounding squares can be reached from the (m, n) position, this means that, in the next move, any surrounding square can be reached from the $(m + 1, n + 1)$ position in a finite number of moves. As every step only involves a finite number of moves, to reach any square only a finite number of moves is needed, so any square can be reached from the origin by a finite sequence of moves.