

CSC236 Fall 2016  
Assignment #1: induction  
due October 7th, 10 p.m.

The aim of this assignment is to give you some practice with various forms of induction. For each question below you will present a proof by induction. For full marks you will need to make it clear to the reader that the base case(s) is/are verified, that the inductive step follows for each element of the domain (typically the natural numbers), where the inductive hypothesis is used and that it is used in a valid case.

Your assignment must be typed to produce a PDF document (hand-written submissions are not acceptable). You may work on the assignment in groups of 1, 2, or 3, and submit a single assignment for the entire group on [MarkUs](#)

1. Consider the Fibonacci-esque function  $g$ :

$$g(n) = \begin{cases} 1, & \text{if } n = 0 \\ 3, & \text{if } n = 1 \\ g(n-2) + g(n-1) & \text{if } n > 1 \end{cases}$$

Use complete induction to prove that if  $n$  is a natural number greater than 1, then  $2^{n/2} \leq g(n) \leq 2^n$ . You may **not** derive or use a closed-form for  $g(n)$  in your proof.

**Sample solution:** Proof, using complete induction.

**inductive step:** Let  $n$  be a typical natural number greater than 1 and assume  $H(n)$  : Every natural number  $i \in \{2, \dots, n-1\}$  satisfies  $2^{i/2} \leq g(i) \leq 2^i$ .

**show that inductive conclusion follows:** We'll derive  $C(n)$ :  $2^{n/2} \leq g(n) \leq 2^n$ .

**Base cases:**  $1 < n < 4$ :  $g(2) = 4$  and  $g(3) = 7$  # by the definition of  $g(2)$  and  $g(3)$ .

$$2^{2/2} = 2 \leq 4 = g(2) \leq 4 = 2^2 \quad \text{and} \quad 2^{3/2} = 2\sqrt{2} \leq 7 = g(3) \leq 8 = 2^3$$

$C(2)$  and  $C(3)$  follow from our assumptions in this case.

**Case  $n \geq 4$ :** By assumptions  $H(n-2)$  and  $H(n-1)$  #  $n \geq 4$  implies  $2 \leq n-2, n-1 < n$ :

$$2^{(n-2)/2} \leq g(n-2) \leq 2^{n-2} \quad \text{and} \quad 2^{(n-1)/2} \leq g(n-1) \leq 2^{n-1}.$$

Substituting these inequalities into the definition of  $g(n)$  # by definition of  $g(n)$ ,  $n \geq 4 > 0$ :

$$\begin{aligned} g(n) &= g(n-2) + g(n-1) \geq 2^{(n-2)/2} + 2^{(n-1)/2} = (1 + \sqrt{2})2^{(n-2)/2} \geq 2 \times 2^{(n-2)/2} = 2^{n/2} \\ g(n) &= g(n-2) + g(n-1) \leq 2^{n-2} + 2^{n-1} = (1 + 2)2^{n-2} \leq 2^2 \times 2^{n-2} = 2^n \end{aligned}$$

$C(n)$  follows from our assumptions in this case.

In all cases  $H(n)$  implies  $C(n)$ .

2. Suppose  $B$  is a set of binary strings where each binary string is of length  $n$ .  $n$  is positive (greater than 0), and no two strings in  $B$  differ in fewer than 2 positions. Use simple induction to prove that  $B$  has no more than  $2^{n-1}$  elements.

**Sample solution:** Proof, using simple induction.

**verify base:** There are two binary strings of length 1: "0" and "1", and they differ from each other in exactly one position (i.e. fewer than 2). That means that the only sets of binary strings of length 1 that contain no pairs that differ in fewer than 2 positions are {"1"}, {"0"}, and {}, which each have no more than  $1 = 2^{1-1}$  elements, verifying the claim in this case.

**inductive step:** Let  $n$  be a typical natural number greater than 0. Assume  $H(n)$ : any set of binary strings of length  $n$  containing no pairs that differ in fewer than 2 positions must have no more than  $2^{n-1}$  elements.

**derive conclusion  $C(n)$ :** We must show that from  $H(n)$  follows  $C(n)$ : any set of binary strings of length  $n + 1$  containing no pairs that differ in fewer than 2 positions must have no more than  $2^n$  strings.

Let  $B$  be an arbitrary set of binary strings of length  $n + 1$  that contains no pairs that differ in fewer than 2 positions.

Let  $B_1$  be the subset of  $B$  consisting of those elements with 1 in the first position, and  $B_2$  be the subset of  $B$  consisting of those elements of  $B$  with 0 in the first position.  $B_1$  and  $B_2$  partition  $B$ , since every element of  $B$  has either a 1 or a 0 in the first position, and no element of  $B$  has both a 1 and a 0 in the first position.

From  $B_1$  construct  $B'_1$ , consisting of the strings of  $B_1$  with the leading 1 removed. Similarly, from  $B_2$  construct  $B'_2$ , consisting of the strings of  $B_2$  with the leading 0 removed.

Sets  $B'_1$  and  $B'_2$  contain strings of length  $n$ , and contain no pairs that differ in fewer than 2 positions, since removing the leading 1s or 0s cannot change the number of positions in which elements differ. By assumption  $H(n)$ , both  $B'_1$  and  $B'_2$  have no more than  $2^{n-1}$  elements each. Elements of  $B_1$  are in 1-1 correspondence with those of  $B'_1$ , since you can transform one into the other by prepending a leading 1, or removing a leading 1. Similarly elements of  $B_2$  are in 1-1 correspondence with those of  $B'_2$ .  $|B_1| = |B'_1|$  and  $|B_2| = |B'_2|$ , since they are in 1-1 correspondence.

$|B| = |B_1| + |B_2| \leq 2^{n-1} + 2^{n-1} = 2^n$ , since  $B_1$  and  $B_2$  partition  $B$ . This is what  $C(n)$  claims.

3. Define  $T$  as the smallest set of strings such that:

(a) "b"  $\in T$

(b) If  $t_1, t_2 \in T$ , then  $t_1 + \text{"ene"} + t_2 \in T$ , where the  $+$  operator is string concatenation.

Use structural induction to prove that if  $t \in T$  has  $n$  "b" characters, then  $t$  has  $2n - 2$  "e" characters.

**Sample solution:** Proof, using structural induction.

**verify basis:** "b"  $\in T$  # from definition. "b" has 1 character "b" and  $2(1) - 2 = 0$  "e" characters. This verifies the claim for the basis.

**inductive step:** Let  $t_1, t_2 \in T$  and assume  $H(\{t_1, t_2\})$ : If  $t_1$  has  $n_1$  "b" characters and  $t_2$  has  $n_2$  "b" characters, then  $t_1$  has  $2n_1 - 2$  "e" characters and  $t_2$  has  $2n_2 - 2$  "e" characters.

**show that inductive conclusion follows from assumptions:** We'll derive  $C(t_1 + \text{"ene"} + t_2)$ : If  $t_1 + \text{"ene"} + t_2$  has  $n_{1,2}$  "b" characters, then it has  $2n_{1,2} - 2$  "e" characters.

$t_1 + \text{"ene"} + t_2 \in T$  # by definition of  $T$ , where  $+$  is string concatenation.

Let  $n_1, m_1$  be the number of "b" (respectively "e") characters in  $t_1$ , and  $n_2, m_2$  be the number of "b" (respectively "e") characters in  $t_2$ .  $t_1 + \text{"ene"} + t_2$  has  $n_1 + n_2$  "b" characters # Concatenating "ene" doesn't increase the number of "b" characters.

Let  $n_{1,2}$  be the number of "b" characters in  $t_1 + \text{"ene"} + t_2$ . Then  $n_{1,2} = n_1 + n_2$  # since no "b" characters are added by concatenating "ene".

$t_1 + \text{"ene"} + t_2$  has  $2n_1 - 2 + 2n_2 - 2 + 2$  "e" characters # by assumptions  $H(t_1), H(t_2)$ , and two "e" characters in "ene".

Summing up  $t_1 + \text{"ene"} + t_2$  has

$$2n_1 - 2 + 2n_2 - 2 + 2 = 2(n_1 + n_2) - 2 - 2 + 2 = 2(n_1 + n_2) - 2 = 2n_{1,2} - 2$$

... "e" characters. Conclusion  $C(t_1 + \text{"ene"} + t_2)$  follows in this case.

4. On [page 79](#) of the Course Notes the quantity  $\phi = (1 + \sqrt{5})/2$  is shown to be closely related to the Fibonacci function. You may assume that  $1.61803 < \phi < 1.61804$ . Complete the steps below to show that  $\phi$  is irrational.

- (a) Show that  $\phi(\phi - 1) = 1$ .

**Sample solution:** Substituting the expression for  $\phi$ :

$$\phi(\phi - 1) = \left( \frac{1 + \sqrt{5}}{2} \right) \left( \frac{\sqrt{5} - 1}{2} \right) = \frac{4}{4} = 1$$

- (b) Rewrite the equation in the previous step so that you have  $\phi$  on the left-hand side, and on the right-hand side a fraction whose numerator and denominator are expressions that may only have integers, + or -, and  $\phi$ . There are two different fractions, corresponding to the two different factors in the original equation's left-hand side. Keep both fractions around for future consideration.

**Sample solution:** I can choose to divide 1 by either  $\phi$  or  $\phi - 1$ , yielding:

$$\phi = \frac{1}{\phi - 1} \quad \phi = \frac{1 + \phi}{\phi}$$

- (c) Assume, for a moment, that  $\phi$  is the ratio of two natural numbers. Let  $m, n \in \mathbb{N}$  such that  $\phi = n/m$ . Re-write the right-hand side of both equations in the previous step so that you end up with fractions whose numerators and denominators are expressions that may only have integers, + or -,  $m$  and  $n$ .

**Sample solution:** Substitute  $n/m$  for  $\phi$  on the right-hand side, and then simplify:

$$\phi = \frac{1}{\phi - 1} \longrightarrow \phi = \frac{m}{n - m} \quad \phi = \frac{1 + \phi}{\phi} \longrightarrow \frac{m + n}{n}$$

- (d) Use your assumption from the previous part to construct a non-empty subset of the natural numbers that contains  $m$ . Use the Principle of Well-Ordering, plus one of the two expressions for  $\phi$  from the previous step to derive a contradiction.

**Sample solution:** Let  $F \subseteq \mathbb{N}$  be defined by:

$$F = \{m' \in \mathbb{N} \mid \exists n' \in \mathbb{N}, \phi = n'/m'\}.$$

By assumption in (c),  $F$  is non-empty, since it has at least one member,  $m$ . By PWO  $F$  has a smallest element, let it be  $m_0$ , with its corresponding  $n_0$  so that  $m_0, n_0 \in \mathbb{N}$  and  $\phi = n_0/m_0$ .

Rewriting the equation for  $\phi$  and using the assumption  $1.61803 < \phi < 1.61804$  yields:

$$\begin{aligned}\phi &= \frac{n_0}{m_0} \\ \phi m_0 &= n_0 \quad \# \text{multiply both sides by } m_0 \\ m_0 &< n_0 < 2m_0 \quad \# \text{multiply } 1.61803 < \phi < 1.61804 \text{ by } m \\ 0 &< n_0 - m_0 < m_0 \quad \# \text{subtract } m_0 \text{ from both inequalities.}\end{aligned}$$

$n_0 - m_0 \in \mathbb{N}$  #integers closed under  $-$  and difference is non-negative.

$n_0 - m_0 \in F$ , since  $\phi = n_0/m_0 = m_0/(n_0 - m_0)$  and  $n_0 - m_0 < m_0$ .

Contradiction  $\rightarrow \leftarrow$ .  $m_0$  is the smallest element of  $F$ , by construction.

- (e) Combine your assumption and contradiction from the previous step into a proof that  $\phi$  cannot be the ratio of two natural numbers. Extend this to a proof that  $\phi$  is irrational.

**Sample solution:** Proof (by contradiction) that  $\phi$  is irrational.

Assume, for the sake of contradiction, that  $\phi$  is rational.

Let  $z_1, z_2 \in \mathbb{Z}, \phi = z_1/z_2$  # by definition of  $\phi$  is rational

Let  $n, m \in \mathbb{N}, m/n = \phi$ . # Since  $\phi = z_1/z_2 > 0$  the numerator and denominator have the same sign. If  $z_1, z_2 > 0$ , let  $n = z_1, m = z_2$ . Otherwise, if  $z_1, z_2 < 0$ , let  $n = -z_1, m = -z_2$ .

Contradiction  $\rightarrow \leftarrow$ . From the previous part, there are no natural numbers  $m, n$  such that  $\phi = m/n$ .

$\phi$  is irrational, since assuming otherwise leads to a contradiction.

5. Consider the function  $f$ , where  $3 \div 2 = 1$  (integer division, like  $3//2$  in Python):

$$f(n) = \begin{cases} 1 & \text{if } n = 0 \\ f^2(n \div 3) + 3f(n \div 3) & \text{if } n > 0 \end{cases}$$

Use complete induction to prove that for every natural number  $n$  greater than 2,  $f(n)$  is a multiple of 7. NB: Think carefully about which natural numbers you are justified in using the inductive hypothesis for.

**Sample solution:** Proof by complete induction.

**inductive step:** Let  $n$  be a typical natural number greater than 2, and assume  $H(n)$ : that  $f(i)$  is a multiple of 7 for natural numbers  $2 < i < n$ .

**show that inductive conclusion follows:** We'll derive  $C(n)$ :  $f(n)$  is a multiple of 7.

**Base case**  $2 < n < 6$ :  $n > 0$ , so by the definition of  $f(n)$ :

$$f(n) = f^2(n \div 3) + 3f(n \div 3) = f^2(1) + 3f(1) = 28 \quad \#f(1) = 4 \text{ from definition}$$

28 is a multiple of 7, so  $C(n)$  follows in this case.

**Base case**  $6 \leq n < 9$ :  $n > 0$ , so by the definition of  $f(n)$ :

$$f(n) = f^2(n \div 3) + 3f(n \div 3) = f^2(2) + 3f(2) = 28 \quad \#f(2) = 4 \text{ from definition}$$

28 is a multiple of 7, so  $C(n)$  follows in this case.

**Case**  $n \geq 9$ :  $n > n \div 3 > 2$ , so by assumption  $H(n \div 3)$  we know that  $f(n \div 3)$  is a multiple of 7.

Let  $k \in \mathbb{N}$  be a natural number such that  $f(n \div 3) = 7k$ .

$$f(n) = f^2(n \div 3) + 3f(n \div 3) = 49k^2 + 21k = 7(7k^2 + 3k)$$

$7(7k^2 + 3k)$  is a multiple of 7, so the conclusion  $C(n)$  is verified in this case.