CS 81, Logic and Computability
HW 1: Practice with Proofs
Helped by Grutors Trishan Armruther and James Catron

- There are some challenging problems here so please start early. While this problem set is intended to review proof concepts from discrete math, the challenge level may depend on which offering of discrete math you took. So, as always, please seek help from Prof. George and the grutors as needed; we're very happy to help!
- Before getting started on this assignment, please read Handout 1. It discusses methods of proof and standards for writing clear and precise proofs. Your solutions will be graded both on correctness and clarity.
- As an added incentive to read Handout 1, you may appeal to any results from Handout 1 when solving the problems below. Of course, you may also use basic math facts (e.g., about logarithms, exponents, etc.).

Challenge 1: Proof by Contrapositive [5 Points]

Use proof by contrapositive to prove that if x is an integer and x^2 is not divisible by 4, then x is odd. (*Note:* This is very short, but remember that contrapositive is not the same as contradiction.)

Challenge 2: Proof by Contradiction [20 Points]

Use proof by contradiction to prove each of the following claims.

1. If a and b are positive real numbers then $\frac{a+b}{2} \geq \sqrt{ab}$. (The term on the left-hand-side is called the *arithmetic mean* and the term on the right-hand-side is called the *geometric mean.*)
2. $\log_2 3$ is irrational.

Challenge 3: Proofs Using Axioms [20 Points]

Recall from Handout 1 that a *field* is a set F (which can be finite or infinite) with the two operations called *addition* and *multiplication* denoted by operators $+$ and $\times$, respectively. These operations are required to satisfy the following properties (or "axioms"):

Axioms 1.

(A1) $a + b = b + a$ *and* $a \times b = b \times a$ *(commutative laws)*

(A2) $a + (b + c) = (a + b) + c$ *and* $a \times (b \times c) = (a \times b) \times c$ *(associative laws)*

(A3) $a \times (b + c) = (a \times b) + (a \times c)$ *(distributive law)*

(A4) There exists two different unique elements 0 *and* 1 *in* F *such that* $a + 0 = a$ *and* $a \times 1 = a$ *(identity elements)*

(A5) For each $a \in F$ *there exists an element denoted* $-a$ *in* F *such that* $a + (-a) = 0$ *(additive inverse)*

(A6) For each $a \in F$ *such that* $a \neq 0$*, there exists an element denoted* a^{-1} *in* F *such that* $a \times (a^{-1}) = 1$ *(multiplicative inverse)*

For example, the set of real numbers under real addition and multiplication is a field denoted $(\mathbb{R}, +, \times)$. However, there are many other fields and in some the addition and multiplication operators have entirely different meanings than the arithmetic addition and multiplication that we're used to!

Use these axioms to prove each of the following statements about an arbitrary element a in an arbitrary field. Divide each proof into separate lines and indicate which axiom you are using to get from one line to the next, following the style shown in Handout 1.

Once you've proved something, you can use that result in your proof just as you would use an axiom. Said another way, once you've proved something, it's a theorem. And, theorems are just as good as axioms! For example, once you've proved that $a \times 0 = 0$, you can then cite that result as "Theorem: $a \times 0 = 0$" when proving something else! (By the way, you're welcome to use the theorem that we proved about unique additive inverses from Handout 1!)

Our sample solutions use around 5-6 lines per proof. It's OK if yours are a bit longer or shorter, but much longer or shorter suggests that something may be going awry!

1. $a \times 0 = 0$
2. $-a = -1 \times a$

Challenge 4: Balanced Parentheses! [30 Points]

This problem explores two different characterizations of the set of all strings of balanced parentheses. First, a brief word about *strings*. A string is a sequence of zero or more symbols over some fixed alphabet. A string of length zero is denoted ϵ. In this course, we will only consider strings of finite length. A *set of strings* can be of finite size or infinitely large, even though all of the strings are of finite length. For example, let's consider the set of strings of balanced parentheses. The empty string, ϵ, is in that set. So are these strings:

```
(), ()(), (()), (()()(()))
```

Of course, there are an infinite number of strings of balanced parentheses, but every such string has finite length!

Finally, here are a few more convenient definitions: if w and v are two strings, then wv denotes the new string that is formed by concatenating w and v. Second, for a given string w, a *prefix* of w is any substring of zero or more consecutive symbols beginning at the front of w. So, if w is "spam" then the strings ϵ, "s", "sp", "spa", and "spam" are the prefixes of w. Notice that, as defined, a string w is a prefix of itself. We say that a string is a *proper prefix* of w if it is a prefix of w but is not w itself.

OK, now for the gratuitous back story! You've been hired as a summer intern at Rocket Labs, developers of the Rocket functional programming language which makes heavy use of balanced parentheses. Two different groups at Rocket Labs have come up with two different ways to describe the set of strings of balanced parentheses. Those two definitions are:

Definition 1.

1. *The empty string is balanced.*
2. *If w is a balanced string, then the string (w) is balanced.*
3. *If w and v are balanced strings, then the string wv is balanced.*

Definition 2. *A string w is balanced if and only if:*

1. *w has an equal number of open and closed parenthesis symbols.*
2. *Every prefix of w has at least as many open parenthesis symbols as closed parenthesis symbols.*

After weeks of feuding between the two groups about which definition is correct, you diplomatically point out that the two definitions are actually equivalent. Everyone is excited about the claim, but they aren't yet convinced. So, your task is to to prove that the two definitions are equivalent. Equivalent means that any string that is in the set of strings defined by Definition 1 is also in the set of strings defined by Definition 2 and vice versa.

Here's how you should proceed. Assume the alphabet is $\{(,)\}$, limited to open and closed parentheses. Let B_1 denote the set of strings that satisfy Definition 1. Let B_2 denote the set of strings that satisfy Definition 2. We'd like to show that $B_1 = B_2$. We'll break that up into two proofs, one that shows that $B_1 \subseteq B_2$ (meaning that every string in set B_1 is also in set B_2) and one that shows that $B_2 \subseteq B_1$.

Each of those two proofs should be by induction (or strong induction, you choose which one is the best choice for this problem). You'll need to decide what to induct on and make that explicit in your induction proofs. (*Note:* Our sample solution is about 1.5 pages long simply because there are two induction proofs.)

Note: Try to do this problem on your own (and/or in consultation with your classmates). But, I recognize that there will be a spectrum of prior experience with inductive proofs, so chatting with Prof. George and/or grutors can be a good way to identify what more you need to solve a problem and identify any potential gaps in experience.

Answers:

1. We will prove this by contrapositive. Let us assume that if x is an even integer and show that x^2 divisible by 4. If we know that x is even, then we can see clearly that we can write x as $x = 2d$ where d is some integer. However, if this is true, then consider that we can see clearly that $x^2 = 4k^2$ by virtue of multiplication, and thus, it follows from the definition of division that 4 divides x^2. Thus, we can see that if x is an even integer, then $4|x^2$. Thus by proof by contrapositive, we have proven that if x is an integer and x^2 is not divisible by 4, then x is odd.

2. (a) By way of contradiction let us assume that if a and b are positive real numbers, then $\frac{a+b}{2} < \sqrt{ab}$. Now, noting that as a and b are both positive real numbers, the action of squaring each side preserves our inequality. Therefore, squaring each side, we obtian that,

$$(\frac{a+b}{2})^2 = \frac{a^2+b^2+2ab}{4}$$

and similarly that,

$$(\sqrt{ab})^2 = ab$$

Thus, we now have that $\frac{a^2+b^2+2ab}{4} < ab \implies a^2+b^2+2ab < 4ab$. However, rearranging this expression, we can see that we obtain that, $a^2 - 2ab + b^2 < 0$. Furthermore, we can factor this expression as follows to obtain that $(a-b)^2 < 0$. However, consider that this is a contradiction, as the difference of two positive real numbers is another real number, and that the square of any real number is positive and thus greater than or equal to zero. Therefore, we have arrived at a contradiction as $(a-b) \geq 0$ must be true and furhter, that $\frac{a+b}{2} \geq \sqrt{ab}$.

   (b) By way of contradiction, let us assume that $\log_2 3$ is rational. By definition, a rational number is one that can be expressed as the quotient of two integers. Thus, it follows that $\log_2 3 = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$. Further more, it follows that we rearrange this expression as $b \log_2 3 = a$, which can be rewritten as, $a = \log_2(3^b)$, which we can see gives us that, $2^a = 3^b$. However, we can note that this is a contradiction as this expression will only be satisfied when $a = b = 0$ as 3^b will always be an odd number (since the prime factorization will simply be 3^α and thus never includes a 2) and 2^a will always be an even number for $a, b \neq 0$, and thus, the equality will never be true for non-zero values of a and b, which we know is not a solution since $\frac{0}{0}$ is undefined. Therefore, by contradiction, $\log_2 3$ must be irrational as desired.

3. (a) *Proof*

(1) $a \times 0$ from our premise

(2) $(a + -a) = 0$ from (A5)

(3) $a \times 0 = a \times (a + -a)$ using line 2

(4) $a \times 0 = (a \times a) + (a \times -a)$ by (A3)

(5) $a \times -a = -a^2$ by (A3) and multiplication

(6) $a \times a = a^2$ definition of multiplication

(7) $a \times 0 = a^2 + (-a^2)$ lines (7) and (6)

(8) $a^2 + (-a^2) = 0$ (A5)

(9) $a \times 0 = 0$ line 8

(b) *Proof*

(1) $a + (-1 \times a) = (1 \times a) + (-1 \times a)$ from (A4)
(2) $a + (-1 \times a) = (-1 \times a) + (1 \times a)$ from line 1 and (A1)
(3) $a + (-1 \times a) = a(-1 + 1)$ from line 2 and (A3)
(4) $a + (-1 \times a) = a \times 0$ from line 3 and (A5)
(5) $a + (-1 \times a) = 0$ from Challenge 3: Proof 1
(6) $(-1 \times a) = -a$ from line 5 and (A5)

4. First, let B_1 denote the set of all strings which satisfy Definition 1, and similarly, let B_2 be the set of all strings that satisfy Definition 2. Let us first prove that $B_1 \subseteq B_2$.

   First, consider our base case, the string ϵ. We can see that by definition 1, $\epsilon \in B_1$. Similarly, since ϵ has zero open and closed parentheses symbols, it follows that $\epsilon \in B_2$ as desired.

   Now, let us assume that our inductive hypothesis holds for up to n length strings in B_1. We will now prove that it holds for strings of length $n + 1$. Let $w \in B_1$ be a string of length n+1. Now, we can note that w is either of the form (w_1) for $w_1 \in B_1$, or $w = v_1 v_2$ for $v_1, v_2 \in B_1$.
   Considering the first instance, we can note that if we know that if $w = (w_1)$, then it is clear that the length of $w_1 < n + 1$, and thus, it falls under our inductive hypothesis that $w_1 \in B_2$. However, we can clearly count that w is simply w_1 wrapped

in an opening and closing parenthesis, and thus since we know that w_1 has an equal number of open and closed parenthesis symbols, then it follows that w also has an equal number of open and closed parenthesis symbols and thus is in B_2.
Now, considering the second instance, we can see that if $w = v_1v_2$ such that $v_1, v_2 \in B_2$, then it follows that we know that w is the concatenation of the two strings, we can assume that both v_1, v_2 have length less than $n+1$, and thus, are both in B_2 as desired. However, if we consider the concatenation of the two strings, then we can see that the full concatenation of the two strings would have equal numbers of opening and closing parenthesis since we can count the number of opening parenthesis as the number in v_1 + the number of opening parenthesis in v_2, which we know must equal the sum of closing parenthesis in v_1 and v_2. However, consider the prefixes of w. Consider the prefixes of w. We can see that any prefix that includes a prefix of v_2 would have the full number of opening and closing parenthesis from v_1 and could be written as the concatenation of v_1 and some prefix of v_2, which we know has at least as many open parenthesis symbols as closed parenthesis symbols as $v_2 \in B_2$, and therefore, w would have at least as many open parenthesis symbols as closed parenthesis symbols. Similarly, if we have a prefix of w that does not inclue v_2 would simply also be a prefix of v_1 and therefore, since $v_1 \in B_2$, it follows that the prefix meets the second condition as desired.

Therefore, as both conditions are met for definition 2, it follows that $w \in B_2$ for $|w| = n+1$, and therefore, by induction, it follows that $B_1 \subseteq B_2$ as desired.

Now, consider the proof that $B_2 \subseteq B_1$.

Considering the base case with ϵ, we can see clearly from Definition 1 that $\epsilon \in B_1$ by definition.

Now, let us assume that our inductive hypothesis holds up for up to n length strings in B_2. We will now prove that that this assumption holds for strings of length $n+1$. Let $w \in B_2$ be a string of length $n+1$.
Now, let every prefix of w have string more open parenthesis symbols as closed parenthesis symbols, we can see that it follows that the first prefix of w must be the first prefix that is balanced. This also has the consequence that w must then start with an open parenthesis, as we know that every prefix w has at least as many open parenthesis as closed. However, if w is to be balanced, then it follows that the last parenthesis in w must be a closing one since we know that the prefix of w of all but the last parenthesis has at least as many open parenthesis as closed parenthesis. Therefore, consider then that we can express $w = (v)$ where v is a string. Furthermore, we can see that v has the same number of open and closed parenthesis symbols, as we know that w has the same number of open and closed parenthesis. Therefore, we can see

that $v \in B_2$, and more formally, that $|v| < n+1$, and thus, is in B_1 and is a balanced string by Definition 1. Therefore, as $v \in B_1$, it follows that $(v) \in B_1$ or that $w \in B_1$ as desired.

Now, consider w has a proper prefix equal number of open and closed parenthesis symbols. Let this prefix be denoted w_1, and the remaining substring be denoted w_2. By our Definition 2, it follows that w_1 is a balanced string that has length strictly less than $n+1$, which means by oir inductive hypothesis, that $w_1 \in B_1$. Now, consider that it must follow from w_1 having equal numbers of opening and closing parenthesis, then w_2 must also have equal number of opening and closing parenthesis. We can see this is clearly true as if w_2 did not have equal numbers of opening and closing parenthesis, then it would follow that $w = w_1 w_2$ would have an unequal number of opening and closing parenthesis which we know is not true since $w \in B_2$. Therefore, it follows that w_2 has equal numbers of opening and closing parenthesis, meaning that $w_2 \in B_2$. Finally, since we know that $w_2 \in B_2$ and we know from our supposition that w_2 is the complement to w_1, it follows that w_2 has length less than $n+1$. Therefore, by our inductive hypothesis, we know that $w_2 \in B_1$. In conclusion, since $w_1, w_2 \in B_1$ and we can express $w = w_1 w_2$, it follows that $w \in B_1$ as desired.

Therefore, by induction, we can conclude that $B_2 \subseteq B_1$. Finally, as we have proven that $B_1 \subseteq B_2$ and $B_2 \subseteq B_1$, it follows that $B_1 = B_2$ as desired.