Luke Jaffe
Worked with: Emily Moxie
Theory of Computation
Due 1/27/16

Problem Set 1

Problem 1. Prove by induction on the number of elements in S: If S is any nonempty set the number of different nonempty subsets of S is $2^{|S|} - 1$.

Base case: The smallest nonempty set is one which contains a single element. If a set contains one element, it has two subsets: the empty set, and the set containing that element. Thus it contains just one nonempty subset. Now, applying the hypothesis: $2^1 – 1 = 1$. These values are equal, proving the hypothesis for the base case.

Induction step: Let us first determine how many new subsets are introduced when an element is added to a set. Take the set {a}, which has one nonempty subset, {a}. When element 'b' is added, there are now three nonempty subsets: {a}, {b}, {a,b}. We can see a pattern emerging when adding element 'c'. We have seven nonempty subsets, the three old ones {a}, {b}, {a,b}, plus four new ones: {c}, {a,c}, {b,c}, {a,b,c}. When we add a new element to a set, we get all the subsets of the previous set, with the new element added, plus the new element in its own set. To quantify this rule, let us define N(x) as the number of nonempty subsets of a set with x elements. Then: $N(|S| + 1) = 2*N(|S|) + 1$. Substituting in the induction hypothesis, we can create the following equality: $2*(2^{|S|} – 1) + 1 = 2^{|S| + 1} – 1$. On each side is a different representation of the set with |S|+1 elements. Reducing this equality:
$\rightarrow 2^{|S|+1} – 2 + 1 = 2^{|S| + 1} – 1$
$\rightarrow 2^{|S| + 1} – 1 = 2^{|S| + 1} – 1$

Conclusion: By the principle of induction, the hypothesis is therefore true for all nonempty sets.

Problem 2. Use the contrapositive to prove: If $x,y \in \mathbb{Z}$ and both xy and x+y are even, then both x and y are even.

To restate the definitions of even and off for reference:
x is even iff $x=2a$ for some $a \in \mathbb{Z}$
x is odd iff $x=2a+1$ for some $a \in \mathbb{Z}$

The contrapositive can be stated as follows: If x and y are not both even, then xy and x+y are not both even.

For $x,y \in \mathbb{Z}$, there are four possible combinations of even and odd. We need to observe the three cases in which x and y are not both even.

Case 1: x and y both odd
Therefore, $x = 2a+1$ for some $a \in \mathbb{Z}$, and $y = 2b+1$ for some $b \in \mathbb{Z}$.
To show that xy and x+y are not both even, it is sufficient to show that just one is not even. We will use xy in this case:
$xy = (2a + 1)(2b + 1) =$
$4ab + 2a + 2b + 1 =$
$2(2ab + a + b) + 1$

Let $c = 2ab + a + b$, where c is an integer because the integers are closed under addition and multiplication.
Then $xy = 2c+1$, so is odd. Thus xy and $x+y$ are not both even, because xy is odd.

Case 2: x even, y odd
Therefore, $x = 2a$ for some $a \in \mathbb{Z}$, and $y = 2b+1$ for some $b \in \mathbb{Z}$.
To show that xy and $x+y$ are not both even, it is sufficient to show that just one is not even. We will use $x+y$ in this case:
$x+y = 2a + 2b + 1 =$
$2(a+b) + 1$
Let $c = a+b$, where c is an integer because the integers are closed under addition.
Then $x+y = 2c + 1$, so is odd. Thus xy and $x+y$ are not both even, because $x+y$ is odd.

Case 3: x odd, y even
Symmetric to case 2, proved without loss of generality.

Conclusion: By proving that xy and $x+y$ are not both even for the three relevant combinations (even, odd) of $x,y \in \mathbb{Z}$, we have proved the contrapositive of the original statement, and therefore also the original statement.

Problem 3. Suppose $R_<$ is the usual "less than" relation on the reals, so $R_< = \{(a,b): a,b \in \mathbb{R} \text{ and } a < b\}$.

a) Does $R_<$ have property of being transitive?

Yes, $R_<$ has the property of being transitive. If $a < b$, and $b < c$, then $a < c$.

b) Describe the reflexive closure of $R_<$. Identify a particular operator that describes this relation.

$a < a$ is false, so we must add elements to the relation. The smallest relation true for just the reflexive property is $=$. So the smallest we can keep the relation while maintaining the $<$ operator is $\leq$.

c) Describe the symmetric closure of $R_<$. Again, identify a particular operator, if you can.

If $a < b$, then $b < a$ is always false, so we must add to the relation. The only comparators true for just symmetry (between a and b) are $=$ and $\neq$. Adding $=$ doesn't work, since $a \leq b$ does not necessarily mean $b \leq a$. This is only true when a and b are equal. If we combine $<$ and $\neq$, the relation seems to work. If a $<$ or $\neq$ b then b $<$ or $\neq$ a. In fact, since $<$ is a subset of $\neq$, we can simplify the operator to just $\neq$.

Problem 4. Let $\Sigma = \{a, b, c\}$. Describe the following languages over Σ^* as succinctly as possible.

a) $\{a^n b^n : n \geq 0\} \cap \{b^{2n} : n \geq 0\}$

Any string that contains an a will have an empty intersection set. So the only relevant value of n is 0, which produces the empty string on both sides.
Answer: $\{\varepsilon\}$

b) $\Sigma^* - \Sigma^*$

Answer: $\varnothing$

c) The complement of this union: $\{x : x = by, y \in \Sigma^*\} \cup \{x : x = cy, y \in \Sigma^*\} \cup \varepsilon$

In words: {All strings starting with b} U {All strings starting with c} U ε
Since $\Sigma = \{a, b, c\}$, the complement leaves only strings which start with a.
Answer: $\{x: x = ay, y \in \Sigma^*\}$

d) $\{x : x = yaz, y, z \in \Sigma^*\} \cup \{x : x = ybz, y, z \in \Sigma^*\} \cup \{x : x = ycz, y, z \in \Sigma^*\}$

In words: Any string containing a, b, or c. ε is the only valid string which contains none of these.
Answer: $\Sigma^* - \varepsilon$

Problem 5. Let x^R be the string x reversed, defined inductively as $\varepsilon^R = \varepsilon$ and $(xa)^R = ax^R$.
Let $Q = \{x : x \in \{a,b\}^* \text{ and } x = x^R\}$ — that is, the set of "palindromes" of a's and b's that read the same forwards and backwards. aa, bab, and ε are examples of members of Q.

a) Prove by contradiction that Q is infinite.

Suppose Q is finite. We know Σ^* is countably infinite. Let us create a set of palindromes
$P = \{x: yy^R, y \in \Sigma^*\}$
We know this is a set of palindromes because yy^R must read the same forwards as backwards.

If Σ^* is infinite, P must also be infinite, since it contains the same number of elements as Σ^*. Thus, we have arrived at a contradiction: P is a valid set of palindromes, and Q is the set of all palindromes. Thus, $P \subseteq Q$ must be true. Since P is infinite, and Q is finite, P cannot be a subset of Q. For this to be true, Q would also have to be infinite. Thus, we have proved by contradiction that Q is infinite.

b) Describe a reasonable way to list all the elements of Q in some order that lists every element exactly once. Explain in your own words (including the words "bijection," "one-to-one," and "onto") why this demonstrates that the set is countably infinite.

A palindrome can have either an even or an odd number of characters. Since our alphabet is {a,b}, the middle character in palindromes of odd length must be either a or b. In even palindromes, there is no middle character (or treat middle character as ε). Thus, we can construct the set of all palindromes by combining these three types of palindromes for all elements in Σ^*.

$Q = \{x: yy^R, y \in \Sigma^*\} \cup \{x: yay^R, y \in \Sigma^*\} \cup \{x: yby^R, y \in \Sigma^*\}$

Individually, we know these three sets contain no common elements, because one contains only even strings, and the two which contain only odd strings always have a different character at the center. We know we have listed every possible palindrome, because every palindrome must start and end with a string and its reverse, and each set of our union covers all strings in Σ^*, and because we have covered all possible center characters {a, b, ε} in the union. Thus, this union lists every palindrome (of the alphabet) exactly once.

To show that this set Q is countably infinite, we will start with the basis that Σ^* is countably infinite. This is true, because Σ^* can be listed in lexicographic order, showing a bijection to the natural numbers. For each of the sets of the union, we know that there is a bijection to the set Σ^*, because every palindrome in that set is composed of a unique string (one-to-one mapping), and because all strings are listed and a palindrome is made from each one (onto mapping). Finally, because the union of a countably infinite number of countably infinite sets is countably infinite, the union of three countably infinite sets is also countably infinite. Thus Q is countably infinite.

c) Consider the set of all possible languages of palindromes over {a,b} — in other words, the power set of Q. Prove by contradiction (using diagonalization) that this set is uncountably infinite.

We have already determined that the set of palindromes on the alphabet {a,b}, Q, is countably infinite. We can therefore set up our diagonalization argument in a similar way to the argument presented for the natural numbers and their power set.

Suppose that P(Q) (power set of Q) is countable. Then there is a bijection between Q and P(Q), and we can create a table like the one below, with palindromes as column headers, and subsets of Q as row headers. This table contains a column for every palindrome, and a row for every subset of Q. If the palindrome in the column is present in the subset of Q, then we put Y in that entry, otherwise we put N. Suppose we take the string of diagonal elements (starting from the top left of the table). If we take the complement of this string (NYNY → YNYN) in the example below, we have created a valid set of palindromes, which must be a subset of Q. However, it is impossible for this entry to be in the table by design. There must be at least one differing element in the complement (in the diagonal entry) for every single subset of Q listed in the table. This means there is no bijection between Q and P(Q). Thus we have created a contradiction, showing that P(Q) must be uncountably infinite.

Example table:

	ε	**a**	**b**	**aa**
S0	N	N	N	N
S1	Y	Y	N	N
S2	N	Y	N	N
S3	N	N	Y	Y

Example subsets of Q could include... {ε, a, b}, {a}, {aa, bab}, {ababa, ε, bb, b}.