CSE 390Z: Mathematics of Computing

Week 9 Workshop Solutions

Conceptual Review

Relations definitions: Let R be a relation on A. In other words, $R \subseteq A \times A$. Then:

- R is reflexive iff for all $a \in A$, $(a, a) \in R$.
- R is symmetric iff for all a, b, if $(a, b) \in R$, then $(b, a) \in R$.
- R is antisymmetric iff for all a, b, if $(a, b) \in R$ and $a \neq b$, then $(b, a) \notin R$.
- R is transitive iff for all a, b, if $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

Let R, S be relations on A. Then:

- $R \circ S = \{(a, c) : \exists b$ such that $(a, b) \in R$ and $(b, c) \in S\}$

1. Relations Examples

(a) Suppose that R, S are relations on the integers, where $R = \{(1, 2), (4, 3), (5, 5)\}$ and $S = \{(2, 5), (2, 7), (3, 3)\}$. What is $R \circ S$? What is $S \circ R$?

Solution:

$R \circ S = \{(1, 5), (1, 7), (4, 3)\}$
$S \circ R = \{(2, 5)\}$

(b) Consider the relation $R \subseteq \mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \in R$ iff $a \leq b + 1$. List 3 pairs of integers that are in R, and 3 pairs of integers that are not.

Solution:

In R: $(0, 0), (1, 0), (-1, 0)$
Not in R: $(2, 0), (3, 0), (17, 5)$

(c) Consider the relation $R \subseteq \mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \in R$ iff $a \leq b+1$. Determine if R is reflexive, symmetric, antisymmetric, and/or transitive. If a relation has a property, explain why. If not, state a counterexample.

Solution:

- Reflexive: Yes. For any integer a, it is true that $a \leq a + 1$. So $(a, a) \in R$.
- Symmetric: No. For example, $(0, 20) \in R$ but $(20, 0) \notin R$.
- Antisymmetric: No. For example $(0, 1) \in R$ and $(1, 0) \in R$.
- Transitive: No. For example $(2, 1) \in R$ and $(1, 0) \in R$, but $(2, 0) \notin R$.

2. Relations Proofs

Suppose that $R, S \subseteq \mathbb{Z} \times \mathbb{Z}$ are relations.

(a) Prove or disprove: If R and S are transitive, $R \cup S$ is transitive.

Solution:

False. Let $R = \{(1,2)\}$, $S = \{(2,1)\}$. By definition, R and S are transitive. By definition of intersect, $R \cup S = \{(1,2),(2,1)\}$. However, if $R \cup S$ was transitive, we would require $(1,1)$ to be in $R \cup S$, because (1,2) and (2,1) is in $R \cup S$. However, this is not the case. Therefore the claim is false.

(b) Prove or disprove: If R and S are reflexive, then $R \circ S$ is reflexive.

Solution:

True. Let $a \in \mathbb{Z}$ be arbitrary. Then $(a,a) \in R$ and $(a,a) \in S$ by definition of reflexive. Then $(a,a) \in R \circ S$. So $R \circ S$ is reflexive.

(c) Prove or disprove: If $R \circ S$ is reflexive, then R and S are reflexive.

Solution:

False. Let $R = \{(a, a+1) : a \in \mathbb{Z}\}$. In other words, $R = \{...(-2,-1),(-1,0),(0,1),(1,2)...\}$. Let $S = \{(a, a-1) : a \in \mathbb{Z}\}$. In other words, $S = \{...(-1,-2),(0,-1),(1,0),(2,1)...\}$. Then for any arbitrary $a \in \mathbb{Z}$, we have $(a, a+1) \in R$ and $(a+1, a) \in S$. So $(a,a) \in R \circ S$. So $R \circ S$ is reflexive. Thus we have found an example where $R \circ S$ is reflexive, but R and S are not.

(d) Prove or disprove: If R is symmetric, $\overline{R}$ (the complement of R) is symmetric.

Solution:

True. Since R is symmetric, we know the following.

$$\forall a \forall b\ [(a,b) \in R \to (b,a) \in R]$$

Taking the contrapositive, this is equivalent to:

$$\forall a \forall b\ [(b,a) \notin R \to (a,b) \notin R]$$

By the definition of complement, this is equivalent to:

$$\forall a \forall b\ [(b,a) \in \overline{R} \to (a,b) \in \overline{R}]$$

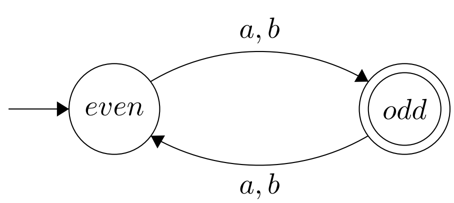
This is the definition of $\overline{R}$ being symmetric.

3. Constructing DFAs

For each of the following, construct a DFA for the specified language.

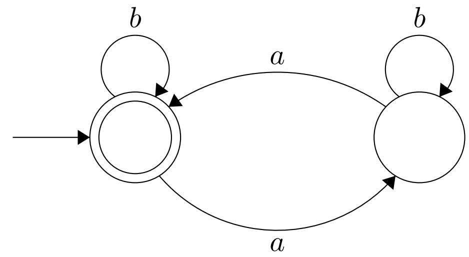
(a) Strings of a's and b's with odd length ($\Sigma = \{a,b\}$).

Solution:



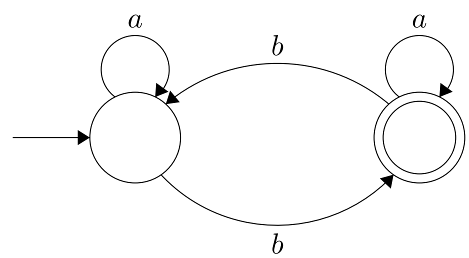
(b) Strings with an even number of a's ($\Sigma = \{a,b\}$).

Solution:



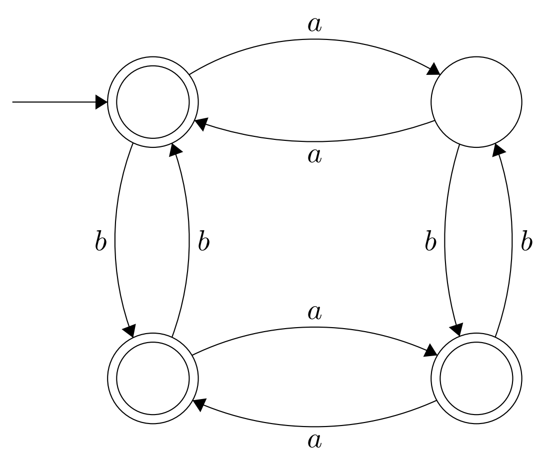
(c) Strings with an odd number of b's ($\Sigma = \{a, b\}$).

Solution:



(d) Strings with an even number of a's or an odd number of b's ($\Sigma = \{a, b\}$).

Solution:



4. Structural Induction: Dictionaries

Recursive definition of a Dictionary (i.e. a Map):

- Basis Case: [] is the empty dictionary
- Recursive Case: If D is a dictionary, and a and b are elements of the universe, then $(a \to b)$ :: D is a dictionary that maps a to b (in addition to the content of D).

Recursive functions on Dictionaries:

$$\begin{aligned} \text{AllKeys}([\,]) &= [\,] \\ \text{AllKeys}((a \to b) :: \text{D}) &= a :: \text{AllKeys}(\text{D}) \\ \text{len}([\,]) &= 0 \\ \text{len}((a \to b) :: \text{D}) &= 1 + \text{len}(\text{D}) \end{aligned}$$

Recursive functions on Sets:

$$\begin{aligned} \text{len}([\,]) &= 0 \\ \text{len}(a :: \text{C}) &= 1 + \text{len}(\text{C}) \end{aligned}$$

Statement to prove:
Prove that len(D) = len(AllKeys(D)).

Solution:

Define P(D) to be len(D) = len(AllKeys(D)) for a Dictionary D. We will use structural induction to show P(D) for all dictionaries D.

Base Case: D = []:
len(D) = len([]) $= 0$ by definition of dictionary len.
Since AllKeys([]) = [] by definition of AllKeys, len(AllKeys(D)) = len([]) = 0 by definition of set len.
Since $0 = 0$, P([]) is true.

Inductive Hypothesis: Suppose P(B) holds for an arbitrary dictionary B. That is, len(B) = len(AllKeys(B)).
Inductive Step: Let a, b be arbitrary.

Goal: Show P($(a \to b) :: B$) i.e. len($(a \to b) :: B$) = len(AllKeys($(a \to b) :: B$))

$$\begin{aligned} \text{len}((a \to b) :: \text{B}) &= 1 + \text{len}(\text{B}) && \text{[Definition of Len]} \\ &= 1 + \text{len}(\text{AllKeys}(\text{B})) && \text{[IH]} \\ &= \text{len}(a :: \text{AllKeys}(\text{B})) && \text{[Definition of Len]} \\ &= \text{len}(\text{AllKeys}((a \to b) :: \text{B})) && \text{[Definition of AllKeys]} \end{aligned}$$

So P($(a \to b) :: B$) holds.
Conclusion: Thus, the claim holds for all dictionaries D by structural induction.

5. Structural Induction on Palindromes

Consider the following *recursive* defintion of the set B of palindrome binary strings:

- **Base case:** $\varepsilon \in B$, $0 \in B$, $1 \in B$.
- **Recursive steps**:
  - If $s \in B$, then $0s0 \in E$, $1s1 \in B$, and $ss \in B$.

  Now define the functions numOnes(x) and numZeros(x) to be the number of 1s and 0s respectively in the string x.

Use structural induction to prove that for any string $s \in B$, numOnes(s) · numZeros(s) is even.

Solution:

Define P(n) to be "$2 \mid$ numOnes(s) · numZeros(s)". We will show P(n) for all $n \in B$ by structural induction.
Base Cases:

- $s = \varepsilon$: numOnes(ε) · numZeros(ε) $= 0 \cdot 0 = 0 = 2 \cdot 0$, thus P($\varepsilon$) holds.
- $s = 0$: numOnes(0) · numZeros(0) $= 0 \cdot 1 = 0 = 2 \cdot 0$, thus P(0) holds.
- $s = 1$: numOnes(1) · numZeros(1) $= 1 \cdot 0 = 0 = 2 \cdot 0$, thus P(1) holds.

Inductive Hypothesis: Suppose P(s) holds for an arbitrary string $s \in B$.
Inductive Step:

- **Case 1:** $0s0$

  $$\begin{aligned} \text{numOnes}(0s0) \cdot \text{numZeros}(0s0) &= (2 + \text{numZeros}(s)) \cdot \text{numOnes}(s) && \text{(Def. of numZeros, numOnes)} \\ &= 2 \cdot \text{numOnes}(s) + \text{numZeros}(s) \cdot \text{numOnes}(s) \end{aligned}$$

  By the I.H., $2 \mid$ numZeros(s)·numOnes(s), thus there is an integer k s.t. numZeros(s)·numOnes(s) $= 2 \cdot k$. We can substitute this to get $2 \cdot$ numOnes(s) $+ 2 \cdot k$, which we can rearrange to get $2 \cdot$ (numOnes(s) $+ k$), thus $2 \mid$ numOnes($0s0$) · numZeros($0s0$) and P($0s0$) holds.

- **Case 2:** $1s1$

  $$\begin{aligned} \text{numOnes}(1s1) \cdot \text{numZeros}(1s1) &= \text{numZeros}(s) \cdot (2 + \text{numOnes}(s)) && \text{(Def. of numZeros, numOnes)} \\ &= 2 \cdot \text{numZeros}(s) + \text{numZeros}(s) \cdot \text{numOnes}(s) \end{aligned}$$

  By the I.H., $2 \mid$ numZeros(s)·numOnes(s), thus there is an integer k s.t. numZeros(s)·numOnes(s) $= 2 \cdot k$. We can substitute this to get $2 \cdot$ numZeros(s) $+ 2 \cdot k$, which we can rearrange to get $2 \cdot$ (numZeros(s) $+ k$), thus $2 \mid$ numOnes($1s1$) · numZeros($1s1$) and P($1s1$) holds.

- **Case 3:** ss

  $$\begin{aligned} \text{numOnes}(ss) \cdot \text{numZeros}(ss) &= (2 \cdot \text{numOnes}(s)) \cdot (2 \cdot \text{numZeros}(s)) && \text{(Def. of numZeros, numOnes)} \\ &= 4 \cdot \text{numOnes}(s) \cdot \text{numZeros}(s) \end{aligned}$$

  By the I.H., $2 \mid$ numZeros(s)·numOnes(s), thus there is an integer k s.t. numZeros(s)·numOnes(s) $= 2 \cdot k$. We can substitute this to get $4 \cdot 2 \cdot k = 2 \cdot (4 \cdot k)$, thus $2 \mid$ numOnes(ss) · numZeros(ss) and P(ss) holds.

Thus, P(s) holds for all $s \in B$ by structural induction.