COMP 330 Autumn 2021
Assignment 1
Solutions

Prakash Panangaden

Question 1[20 points] We fix a finite alphabet Σ for this question. As usual, Σ^* refers to the set of all finite strings (words) over Σ.

(a) Given $x, y \in \Sigma^*$ we say that x is a **prefix** of y if $\exists z \in \Sigma^*\ y = xz$. If x is a prefix of y and y is a prefix of x what can you *deduce* about the relationship between x and y? [5 points]

(b) For this part we assume that $\Sigma = \{a, b\}$. We write $\#_a(x)$ for the number of occurrences of the letter a in the word x and similarly for $\#_b$. We claim that

$$\forall x \in \Sigma^*, \exists y, z \in \Sigma^* \text{ such that } x = yz \wedge [\#_a(y) = \#_b(z)].$$

Is this true? If so prove it, if not disprove it. You will have to understand what the symbolic expression is saying. [15 points]

Solution (a) If x is a prefix of y it means that y is longer than (or the same length as) x and it starts with an exact copy of x. Thus if each string is a prefix of the other they must be exactly the same as each other.

(b) This is indeed true. It says that it is always possible to divide a string into two parts such that the number of a's in the first part is the same as the number of b's in the second part. Let p denote a position in the string. If $p = 0$ we are just to the left of the string, so the value of p gives the number of characters to the left of the position. Now let M be the number of a's to the left of p *minus* the number of b's to the right of p. Initially $M = -\#_b(x)$ since there are no a's to the left of p and all the b's in x are to the right of p. Now consider what happens when p is shifted to the right by one place. The letter that was just crossed over may be an a: in this case M increases by 1. The letter that was just crossed over may be a b: in this case also M increases by 1. Thus at every step M increases by exactly 1. When p is at the right end of the string we have $M = \#_a(x)$, which is a positive number. So M starts as a negative number and increases by steps of 1 and becomes a positive number: somewhere it must have hit zero. At this point we have divided the string in the desired fashion.

Question 2[20 points] Fix a finite alphabet Σ and let $\emptyset \neq L \subseteq \Sigma^*$. We define the following relation R on words from Σ^*:

$$\forall x, y \in \Sigma^*, xRy \text{ if } \forall z \in \Sigma^*, xz \in L \text{ iff } yz \in L.$$

Prove that this is an equivalence relation.

Solution. We must check the three properties:

reflexivity: We want to show $\forall x \in \Sigma^*, xRx$. This means that $\forall z \in \Sigma^*, xz \in L$ iff $xz \in L$; this is clearly true since the two sides of the "iff" are exactly the same.

symmetry: Here we want to show that $\forall x, y \in \Sigma^*, xRy$ implies yRx.

$$\forall z \in \Sigma^*, xz \in L \text{ iff } yz \in L$$

implies that

$$\forall z \in \Sigma^*, yz \in L \text{ iff } xz \in L.$$

But "iff" is reversible so clearly this holds.

transitivity: Here we must show that $\forall x, y, z \in \Sigma^*$ if we have (first assumption)

$$\forall w \in \Sigma^*, xw \in L \text{ iff } yw \in L$$

and (second assumption)

$$\forall w \in \Sigma^*, yw \in L \text{ iff } zw \in L$$

then (conclusion)

$$\forall w \in \Sigma^*, xw \in L \text{ iff } zw \in L.$$

Suppose w is some word in Σ^* and suppose that $xw \in L$, then the first assumption tells us that $yw \in L$. Using this fact with the second assumption tells us that $zw \in L$. Thus $xw \in L$ implies that zw is in L. Proceeding in the same way, if $zw \in L$ we must have $yw \in L$ and thence $xw \in L$. Thus we have established the conclusion.

This is a very pedantically written proof, far too detailed for most tastes. I just want you to have the sense of what goes into such a proof. In future you can state obvious things as "obvious" but don't try and pass off things that are not at all obvious as obvious.

Old Question 3[20 points] Consider, pairs of natural numbers $\langle m, n\rangle$ where $m, n \in \mathbf{N}$. We order them by the relation $\langle m, n\rangle \sqsubseteq \langle m', n'\rangle$ if $m < m'$ or $(m = m') \wedge n \leq n'$, where $\leq$ is the usual numerical order.

1. Prove that the relation $\sqsubseteq$ is a partial order. [10 points]
2. Prove that $\sqsubseteq$ is a well-founded order. [10 points]

Solution

1. From the definition of a partial order we have to verify that $\sqsubseteq$ is (i) reflexive, (ii) antisymmetric and (iii) transitive. We tackle each property in turn. (i) If we compare $\langle m, n\rangle$ with itself we see that $m = m$ so we are in the second case, and here we have $n \leq n$ so we have $\langle m, n\rangle \sqsubseteq \langle m, n\rangle$ [You may be tempted to just say this is obvious; yes it is and I would accept that, in this case.] (ii) Suppose that $\langle m_1, n_1\rangle \sqsubseteq \langle m_2, n_2\rangle$ and $\langle m_2, n_2\rangle \sqsubseteq \langle m_1, n_1\rangle$. Now suppose that

$m_1 < m_2$ then it is impossible for $\langle m_2, n_2\rangle \sqsubseteq \langle m_1, n_1\rangle$ to hold. So if both hold we must have $m_1 = m_2$. Then we know that $n_1 \leq n_2$ and $n_2 \leq n_1$. But the ordinary $\leq$ relation is known to be antisymmetric so $n_1 = n_2$. Thus the two pairs are equal as pairs. (iii) Since there are two possible cases for each instance of the $\sqsubseteq$ relation we have 4 combinations to consider. Suppose $\langle m_1, n_1\rangle \sqsubseteq \langle m_2, n_2\rangle$ and $\langle m_2, n_2\rangle \sqsubseteq \langle m_3, n_3\rangle$. We must show that $\langle m_1, n_1\rangle \sqsubseteq \langle m_3, n_3\rangle$.

(a) Suppose that $m_1 = m_2$, $n_1 \leq n_2$, $m_2 = m_3$ and $n_2 \leq n_3$. Then clearly we have $m_1 = m_3$ (equality is transitive) and $n_1 \leq n_3$ (the $\leq$ relation is transitive) so we have $\langle m_1, n_1\rangle \sqsubseteq \langle m_3, n_3\rangle$.

(b) Suppose $m_1 < m_2$ and $m_2 = m_3$ then $m_1 < m_3$ and we have $\langle m_1, n_1\rangle \sqsubseteq \langle m_3, n_3\rangle$.

(c) Suppose that $m_1 = m_2$ and $m_2 < m_3$, again we have $m_1 < m_3$ so $\langle m_1, n_1\rangle \sqsubseteq \langle m_3, n_3\rangle$.

(d) Suppose $m_1 < m_2$ and $m_2 < m_3$ then $m_1 < m_3$ and we have $\langle m_1, n_1\rangle \sqsubseteq \langle m_3, n_3\rangle$.

We have checked all possible cases so we conclude that $\sqsubseteq$ is transitive and have thus completed the proof that it is a partial order.

2. Suppose that we have an arbitrary non-empty set X of pairs. If we ignore the second member of each pair and only look at the first we have a set of natural numbers so there must be a least natural number l that occurs as the first part of a pair in X. Now we consider all those pairs in X that have l as the first component; this gives a non-empty subset $Y \subset X$. All the members of Y are strictly less than any member of $X \setminus Y$ in the $\sqsubseteq$ ordering. Now, consider the second components of the pairs in Y. This gives another set of natural numbers and there must be a smallest element of such a set, call this smallest number that occurs as the second component of a pair in Y, k. The pair $\langle l, k\rangle$ is the least element of the original set X.

New Question 3[20 points] Consider the set of positive integers : $\mathbf{Z}^+ = \{1, 2, 3, \ldots\}$. We define the following binary relation div on $\mathbf{Z}^+$: n div m if n divides m with no remainder. For example 5; div 35, 12 div 36. On the negative side **not** 14 div 21. In formal logic terms n div m means $\exists k \in \mathbf{Z}^+, m = k * n$. Prove that div is a partial order relation.

Solution We need to show that div satisfies the properties of a partial order: (i) reflexivity, (ii) antisymmetry and (iii) transitivity.

1. It is obvious that $\forall n$, n div n since $n = 1 * n$.

2. If n div m and m div n then there must be positive integers, call them p, q, such that $m = p * n$ and $n = q * m$. Substituting the second equation in the first we get $m = p * (q * m)$ or $m = (p * q) * m$. Thus $p * q = 1$ but this is only possible if both p and q are 1. Thus $m = 1 * n = n$.

3. Suppose n div m and m div p; we must show n div p. From the given assumptions we know that there are positive integers, call them k and l, such that $m = k * n$ and $p = l * m$. Thus, $p = l * (k * n)$ or $p = (l * k) * n$. But this last statement is exactly what it means to say n div p.

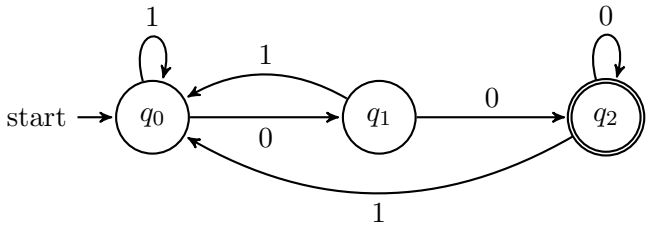
Question 4[20 points] Give deterministic finite automata accepting the following languages over the alphabet $\{0, 1\}$.

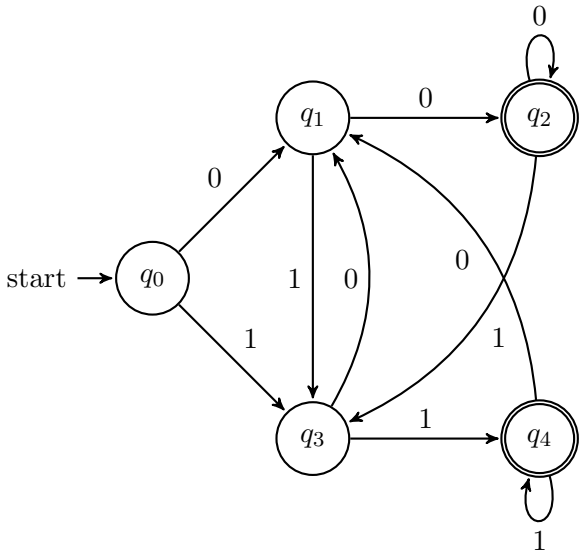
1. The set of all words ending in 00.

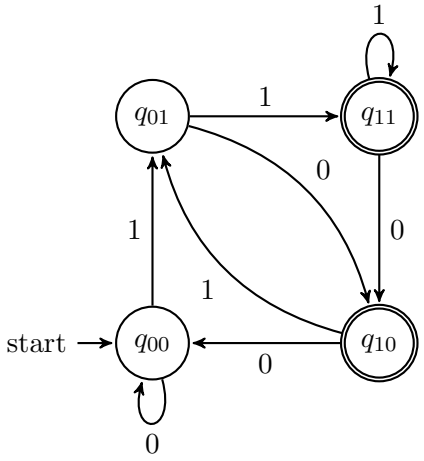
2. The set of all words ending in 00 *or* 11.

3. The set of all words such that the *second* last element is a 1. By "second last" I mean the second element counting backwards from the end. Thus, 0001101 is not accepted and 11101010 is accepted.

Solutions: The automata are shown in the following pictures:



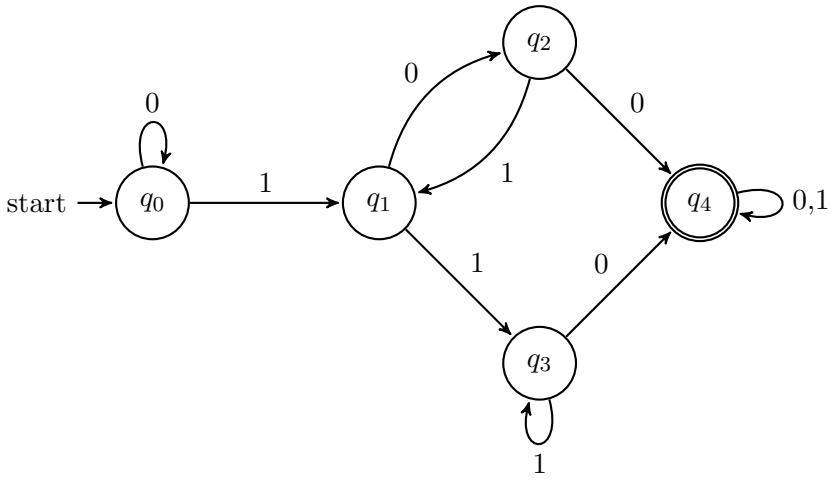




Question 5[20 points]

1. Give a deterministic finite automaton accepting the following language over the alphabet $\{0, 1\}$: The set of all words containing 100 or 110. [5 points]
2. Show that *any* dfa for recognizing this language must have at least 5 states. [15 points]

Solution We need to remember the last two characters seen so far and we need to know that we have never seen a 1, so intuitively one expects to have 5 states. Of course, this is not a proof that you really *need* 5 states. Here is the automaton:



To prove that 5 states are really necessary we should find 5 strings and show that they all must end up in different states. If you look at the automaton you can see 5 strings that take you to each one of the states. These are $w_0 = \varepsilon$, $w_1 = 1$, $w_2 = 10$, $w_3 = 11$ and $w_4 = 100$. We have numbered them so that w_i takes you to state q_i. Now let us consider any putative recognizer for the language. Let the states that are reached from the start state by string w_0 be called A, the state reached by w_1 be called B and so on to give states A, B, C, D, E. In this machine we do not know that these are all distinct states; we have to prove that. We will analyze all the possible cases.

- We can see right away that all the states A, B, C, D are different from E since w_4 is accepted and all the others are rejected.
- Suppose $A = B$ so w_0 and w_1 end up in the same state. Now consider the strings $w_0 \cdot 00 = \varepsilon \cdot 00 = 00$ and $w_1 \cdot 00 = 1 \cdot 00 = 100$. The first string should be rejected and the second one should be accepted so A and B cannot be the same state.
- Suppose $A = C$. This is not possible since $w_0 \cdot 0 = 0$ should be rejected and $w_2 \cdot 0 = 100$ should be accepted.
- Suppose $A = D$. This time we choose to extend the strings by 0 and we get a contradiction.
- Suppose $B = C$. We choose to extend the strings w_1 and w_3 by 0 and get a contradiction.
- Suppose $B = D$. We choose to extend the strings w_2 and w_3 by 0 and get a contradiction.
- Suppose $C = D$. We choose to extend the strings w_2 and w_3 by 10 and get a contradiction.