ICCS310: Assignment 1

Possawat Sanorkam
possawat2017@hotmail.com
January 14, 2021

1: Review: Something About Sets

---

(1) Let A_1, A_2, A_3 be any sets from a universe $\mathcal{U}$. *Prove that* $\overline{A_1 \cup A_2 \cup A_3} = \overline{A_1} \cap \overline{A_2} \cap \overline{A_3}$.

Proof: We want to show that $\overline{A_1 \cup A_2 \cup A_3} \subseteq \overline{A_1} \cap \overline{A_2} \cap \overline{A_3}$ and $\overline{A_1} \cap \overline{A_2} \cap \overline{A_3} \subseteq \overline{A_1 \cup A_2 \cup A_3}$

Let A_1, A_2, A_3 be any three given sets. We'll first prove that $\overline{A_1 \cup A_2 \cup A_3} \subseteq \overline{A_1} \cap \overline{A_2} \cap \overline{A_3}$. Let $x \in \overline{A_1 \cup A_2 \cup A_3}$. Then, $x \notin A_1 \cup A_2 \cup A_3$ by the definition of complement, so then $x \notin A_1$, $x \notin A_2$ and $x \notin A_3$, by the definition of union. This means that $x \in \overline{A_1}$, $x \in \overline{A_2}$, and $x \in \overline{A_3}$, by the definition of complement. Hence, $x \in \overline{A_1} \cap \overline{A_2} \cap \overline{A_3}$ since x is in $\overline{A_1}$, $\overline{A_2}$, and $\overline{A_3}$.

Also, we will show that $\overline{A_1} \cap \overline{A_2} \cap \overline{A_3} \subseteq \overline{A_1 \cup A_2 \cup A_3}$. Let $y \in \overline{A_1} \cap \overline{A_2} \cap \overline{A_3}$, so y is in $\overline{A_1}$, $\overline{A_2}$, and $\overline{A_3}$, by the definition of intersection. This means $y \notin A_1$, $y \notin A_2$, and $y \notin A_3$, by the definition of complement. It follows that $y \notin A_1 \cup A_2 \cup A_3$, and so $y \in \overline{A_1 \cup A_2 \cup A_3}$.

In conclusion, $\overline{A_1 \cup A_2 \cup A_3} = \overline{A_1} \cap \overline{A_2} \cap \overline{A_3}$. $\square$

(2) Let A and B be any sets from a universe $\mathcal{U}$. *Prove that* $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Proof: We want to show that $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$ and $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$

Let A and B be any two given sets. We'll first prove that $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$. Let $x \in \overline{A \cup B}$. Then, $x \notin A \cup B$ by the definition of complement, so then $x \notin A$, and $x \notin B$, by the definition of union. This means that $x \in \overline{A}$, and $x \in \overline{B}$, by the definition of complement. Hence, $x \in \overline{A} \cap \overline{B}$ since x is in $\overline{A}$ and $\overline{B}$.

Also, we will show that $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$. Let $y \in \overline{A} \cap \overline{B}$, so y is in $\overline{A}$ and $\overline{B}$, by the definition of intersection. This means $y \notin A$ and $y \notin B$, by the definition of complement. It follows that $y \notin A \cup B$, and so $y \in \overline{A \cup B}$.

In conclusion, $\overline{A \cup B} = \overline{A} \cap \overline{B}$. $\square$

2: Prime and Irrational

---

(1) Let $p \geq 2$ be a prime and a be a positive integer. Prove that if p divides a^2, then p divides a.

Proof: Using contraposition, we can prove that if p does not divides a, then p does not divides a^2 instead.

Let a be any number that cannot be divided by p, so $a = (p * q) + r$ where $r < p$ and $r, q \in \mathbb{I}^+$. So, we have $a^2 = ((p * q) + r)^2 = (p * q)^2 + 2 * (p * q * r) + r^2$. We can see that r^2 cannot be divided by p. Hence, p does not divides a^2.

Therefore, if p divides a^2, then p divides a. $\square$

(2) Prove that if p is any positive prime number, then $\sqrt{p}$ is irrational.

Proof: Assume for the sake of contradiction, let $\sqrt{p}$ be a rational number and p is any positive prime number. Then, $\sqrt{p} = a/b$ where a and b are integers and $b \neq 0$.

$$\begin{aligned} \sqrt{p} &= a/b && (1) \\ p &= a^2/b^2 && (2) \\ p * b^2 &= a^2 && (3) \end{aligned}$$

From observation, p divides a^2 and that means p divide a (Lemma 2.1). Let $a = bq$ for some $q \in \mathbb{I}^+$ and plug it back into equation 3.

$$\begin{aligned} p * b^2 &= p^2 q^2 && (4) \\ b^2 &= pq^2 && (5) \end{aligned}$$

From observation, p divides b^2 and that means p divide b (Lemma 2.1). Since we showed that $p = a^2/b^2$ but p is a common factor of a and b. We can conclude that the equation is false and our assumption is contradicting. Hence, $\sqrt{p}$ is irrational. Therefore, if p is any positive prime number, then $\sqrt{p}$ is irrational. □

3: Spacing

Prove that in any set of $n + 1$ numbers from $\{1, ..., 2n\}$, there are always two numbers that are consecutive.

Proof: Assume for the sake of contradiction that there is no two numbers that are consecutive given any set of $n + 1$ numbers from $\{1, ..., 2n\}$. Let A be the set of $n + 1$ numbers from $\{1, ..., 2n\}$. Using pigeonhole principle, the required size of A is too large to prevent consecutive numbers because the when the size of A is n we could use the set of odd natural number or even natural number where all elements in A is less than n. However, the last number to be added will contradict to our assumption that no two numbers are consecutive since there would be no other number to pick, except the consecutive number from $\{1, ..., 2n\}$. Hence, A is contradicting to our assumption.

Therefore, any set of $n + 1$ numbers from $\{1, ..., 2n\}$, there are always two numbers that are consecutive.□

4: Curious Fact about Graphs

Let $G = (V, E)$ be an undirected graph. Show that G contains two nodes that have equal degrees.

Proof: Without loss of generality, assume for the sake of contradiction that G is an undirected graph with no loops which has n vertices and every vertices have different degrees. Let D be the set of degrees for each vertex, $D = \{d_1, d_2, d_3, \ldots, d_n\}$. Then, $D = \{0, 2, ..., n - 1\}$, since the number of degree is between 0 to $n - 1$. From observation, we have that there is a vertex with degree $n - 1$ and a vertex with degree 0 which is not possible for any undirected graph. Hence, D contradicted to what we assumed.

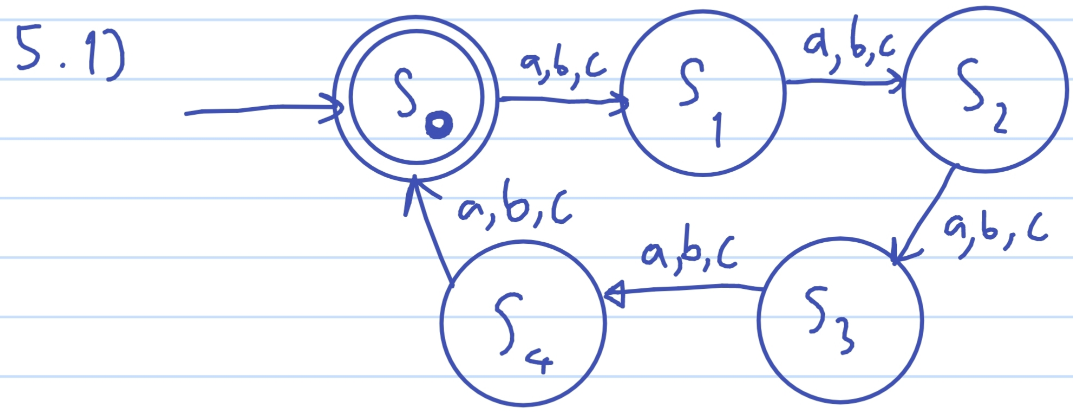
Therefore, if $G = (V, E)$ is an undirected graph, then G contains two nodes that have equal degrees.□

5: Basic DFAs

Let $\sum = \{a, b, c\}$.

(1) The language of strings on $\sum$ whose length is divisible by 5.

Solution:



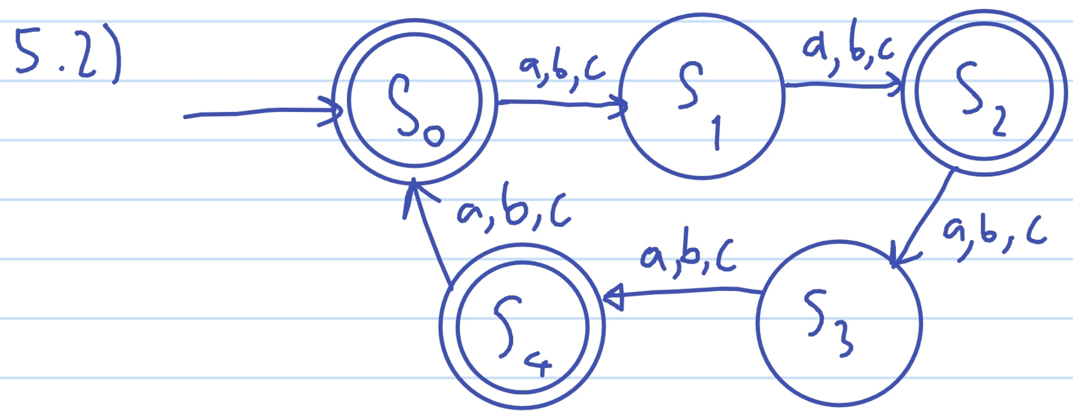
Let n be the length of the input string.

S_0 represents the state where $0 \pmod 5 \equiv n$.
S_1 represents the state where $1 \pmod 5 \equiv n$.
S_2 represents the state where $2 \pmod 5 \equiv n$.
S_3 represents the state where $3 \pmod 5 \equiv n$.
S_4 represents the state where $4 \pmod 5 \equiv n$.

So, the accepting state is S_0 since this state means the length is divisible by 5.

(2) The language of strings on $\sum$ whose length is either even or divisible by 5 (or both).

Solution:



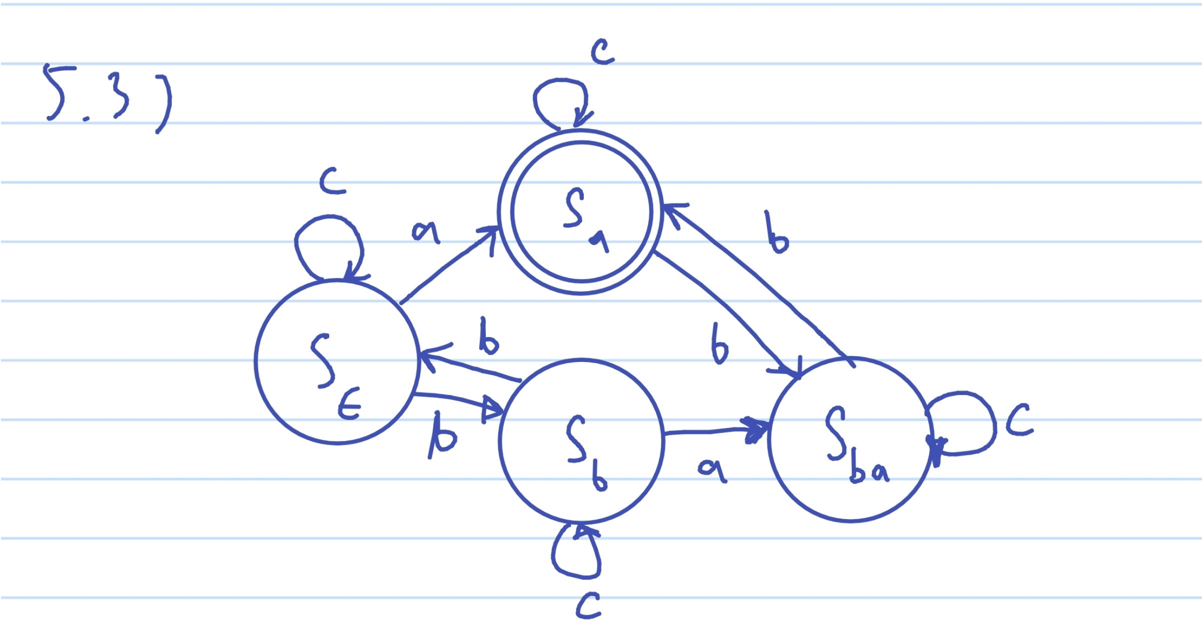
Let n be the length of the input string.

S_0 represents the state where $0 \pmod 5) \equiv n$.
S_1 represents the state where $1 \pmod 5) \equiv n$.
S_2 represents the state where $2 \pmod 5) \equiv n$.
S_3 represents the state where $3 \pmod 5) \equiv n$.
S_4 represents the state where $4 \pmod 5) \equiv n$.

So, the accepting state is S_0, S_2, S_4 since this state means the length is either even or divisible by 5

(3) The language of strings on $\sum$ that has at least one a and contains an even number of bs.

Solution:



Let K be any input string from language set $\sum$.

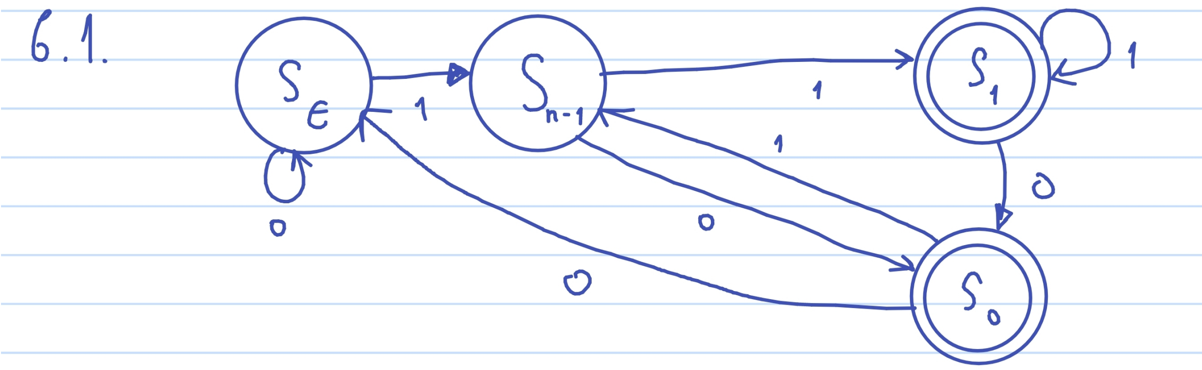
S_ϵ represents the state where there is not a match with the pattern.
S_a represents the state where K has at least one a and contains an even number of bs.
S_{ba} represents the state where K has at least one a and contains an odd number of bs.
S_b represents the state where K has no a and contains an odd number of bs.

So, the accepting state is S_a since this state means the input string has at least one a and contains an even number of bs.

6: Penultimate

(1) Let $L_2 = \{x \in \sum^* :$ the 2nd-to-last symbol of x is $1\}$. Draw a DFA with 4 states that accepts L_2.

Solution:



S_ϵ represents the state where there is not a match with the pattern.
S_{n-1} represents the state where 1 is found but at the last position.
S_1 represents the state where 1 is found at the second-to-last position, and the last alphabet is 1.
S_0 represents the state where 1 is found at the second-to-last position, and the last alphabet is 0.

So, the accepting state is S_1 and S_0 since these states mean the second-to-last symbol of input string is 1.

(2) Show that any DFA that correctly recognizes L_2 must have at least 4 states.

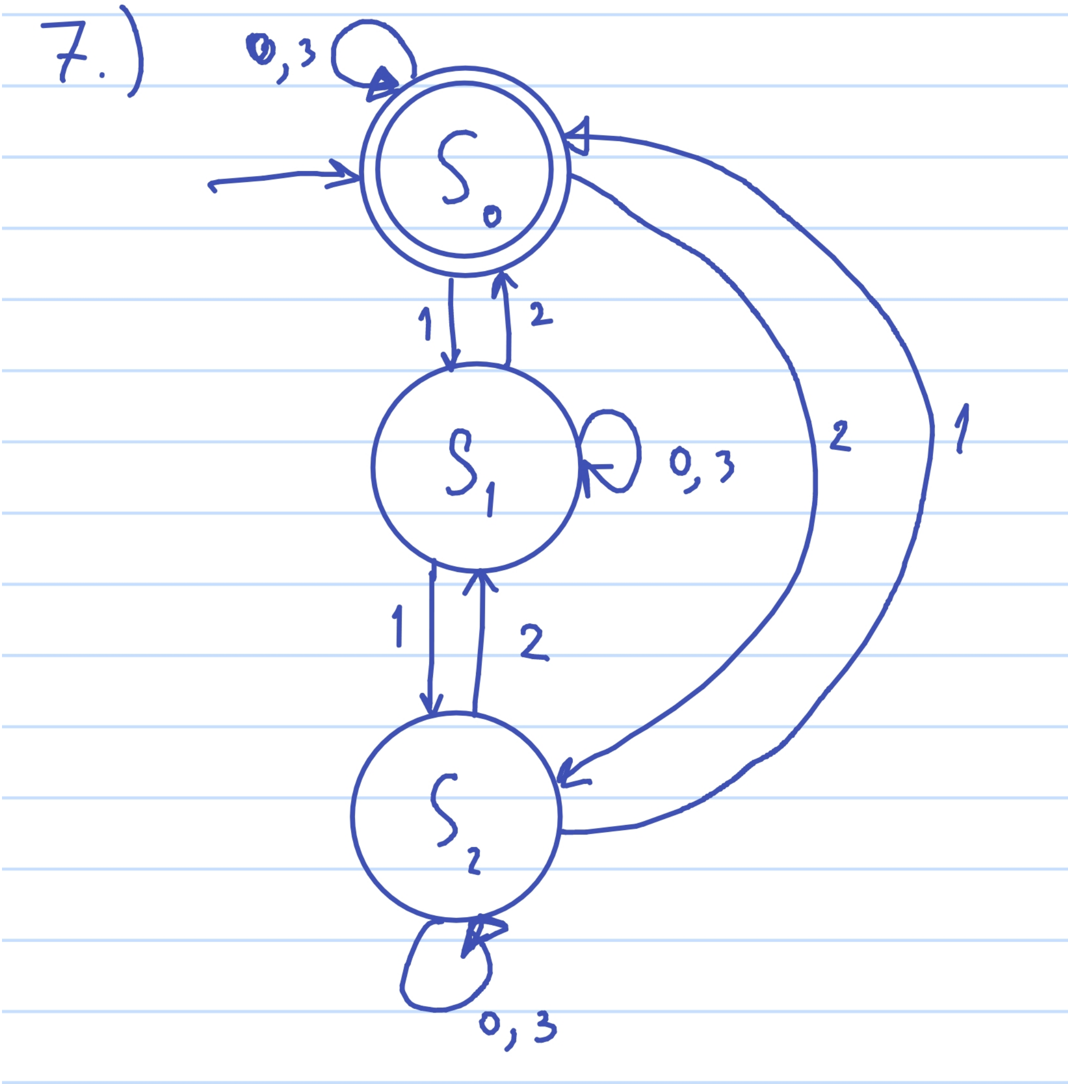
Proof: Without loss of generality, let us assume for the sake of contradiction that there exist D, a DFA that correctly recognizes L_2 using less than 4 states. Let D be a DFA that has 3 states. By the Pigeonhole Principle, if we choose 4 strings over $\sum$, then at least two of those strings must end at the same state q. Let t_i and t_j be these 2 strings that satisfies the above. Let $t_0 = \epsilon, t_1 = 1, t_2 = 10, t_3 = 100$. For one of the pairs of strings, the supposed 3-state DFA is forced into the same state for both strings, and w_{ix} and w_{jx} must be both accepted or both rejected, for any string x. We want to show, for each possible pair, that this is not true.

Therefore, any DFA that correctly recognizes L_2 must have at least 4 states. □

7: Digit Sum

(1) $L = \{x \in \sum^* :$ `DIGITSUM(x)`is divisible by $3\}$. Draw a DFA that recognizes L. Explain what each of your states represents.

Solution:



Let n_i be the accumulating sum of input string at position i.

S_0 represents the state where $0 \pmod 3 \equiv n_i$.
S_1 represents the state where $1 \pmod 3 \equiv n_i$.
S_2 represents the state where $2 \pmod 3 \equiv n_i$.

So, the accepting state is S_0 since this state means `DIGITSUM(x)`is divisible by 3 where $x \in \sum^*$.