Exercise 1 - Computational Models - Spring 2022

Question 1

Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$ and a boolean circuit C of size $|C| = s$ that computes f, Lets proof that there existences of a boolean circuit C' that's stand with the question property.

claim 0.1. *Any simple logic statement that uses $\vee$ or $\wedge$ before $\neg$ can be re-form to $\neg$ before $\vee$ or $\wedge$ using one additional gate*

Proof. using De-Morgan law for $x, y \in \{0,1\}$: $\neg(x \vee y)= \neg x \wedge \neg y$ and on the same way for $\neg(x \wedge y)= \neg x \vee \neg y$, we apply the same statement using extra one gate in total. $\square$

using the claim above we can intuitive say that we need to "roll down the tree" all the NOT gates, and from quick indication I can claim the following.

claim 0.2. *if P have some cycle C size K that compute it $\Rightarrow$ three is some cycle $|C'| = |2K-1|$ that can computes P where all the $\neg$ gate's before any $\wedge$ or $\vee$ gates*

Proof. the indication base case is given from claim0.1, so for some Atomic P where $P_i \in \{0,1\} \Rightarrow$ in total $|K|$ simple gates we get:

$$\neg(P_1 \vee P_2 \vee \dots P_n) \Rightarrow \neg P_1 \wedge \neg P_2 \wedge \dots \neg P_n$$

we can notice that now we need $|K|$ NOT gates and$|K-1|$ of $\wedge$ gates, and in total $|K+K-1|$ gates. and all the $\neg$ gate's before any $\wedge$ gate's.
Now lets P_k be any boolean function that stand with the induction property,for some $x, y \in \{0,1\}$ lets look at:

$$X = \neg(P_k \vee x) = \neg P_K \wedge \neg x, Y = \neg(P_k \wedge y) = \neg P_K \vee \neg y$$

so in any case X, Y can be written in $|2k-1|$ gates of P_k, additional NOT gate and one $\wedge$ or $\vee$ gate, in total $|2k-1+3| = |2k+2|$ under the induction assumption we know that P have some $|C| = K$ that compute it ,so C including the following $\neg, \vee$ witch is size $|K+3|$ and can compute X $\square$

on the same way we proof claim 0.2 we can get the same property for the $\wedge$ gate, so in total for some f we can find for any appearance of $\neg$ gate $\in C$, and each time apply De-Morgan law. based on claim 2 this new $|C'|$ hold the property (a)(b)(c).

Question 2

For f that has a circuit C of size m over B_ℓ, C can be written as a binary tree with m internal nodes. Each internal node is labelled by a gate, and each leaf is labelled by a variable, for each $v \in C$ lets $L_v : \{0,1\}^k \to \{0,1\}$be the circut that accept language , according to Lupanov '58 theorem its can be expressed as language over DeMorgan basis ,using the result of exercise 2 at Recitation 1 ,we know that for such L_v language there is some C that can accept it when $|C| = O(2^k)$ hence for $\forall v \in C \Rightarrow M|L_v|$ can be decided with some C_m size $O(m2^\ell)$.

Question 3

$\Longrightarrow$ Lets M be an DFA such as $M = (Q, \sum, \delta, q_0, F)$ and assume that M accept some $w \in \sum^*$ i.e $\hat{\delta}_m(q_0, w) \in F$. using $\hat{\delta}_m$ definition ,lets k_i be the state such as

$$\hat{\delta}_m(q_0, w) = k_n$$

$$\hat{\delta}_m(q_0, w) = \delta(\hat{\delta}_m(q_0, w_1, w_2 \dots w_n - 1), w_n) \Rightarrow k_{n-1} = \hat{\delta}_m(q_0, w_1, w_2 \dots w_n - 1)$$

follow same proses for $n-2, n-3, \dots$ so for general k_i on the "back-word" path

$$\hat{\delta}_m(q_0, w_j) = \delta(\hat{\delta}_m(q_0, w_1, w_2 \dots w_{j-1}), w_j) \Rightarrow k_{j-1} = \hat{\delta}_m(q_0, w_1, w_2 \dots w_{j-1})$$

hence $\forall k_i \in Q$, $k_n \in F$, $k_0 = q_0$ and $\delta_m(k_{i-1}, w_i) = k_i$ for $1 \leq i \leq n$
so we can claim that the sequence $k_1, k_2, \dots k_n$ stand with the property of the second equivalent DFA definition.

$\Longleftarrow$ Lets M be an DFA such as $M = (Q, \sum, \delta, q_0, F)$ and we assume that
$\forall q_i \in Q$, $q_n \in F$,$w_0 = q_0$ and $\delta_m(q_{i-1}, w_i) = q_i$ for some $w = w_1, w_2, \dots w_n$ and $q_1, q_2, \dots q_n$ with the same way decribed above

$$\delta(q_0, w_1) = q_1, \hat{\delta_m}(q_0, w_1, w_2) = \delta(\delta(q_0, w_1), w_2) = \delta(q_1, w_2) = q_2,$$

in general

$$\hat{\delta_m}(q_0, w_1, \dots, w_j) = \delta(\hat{\delta_m}(q_0, w_1, \dots, w_{j-1}), w_j) = q_j$$

$$\hat{\delta_m}(q_0, w_1, \dots, w_n) = \delta(\hat{\delta_m}(q_0, w_1, \dots, w_{n-1}), w_n) = q_n \in F$$

and we proof that both definition are equivalent

Question 4

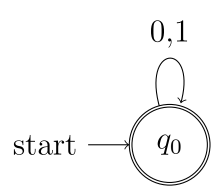

Figure 1: DFA (a) Σ^*

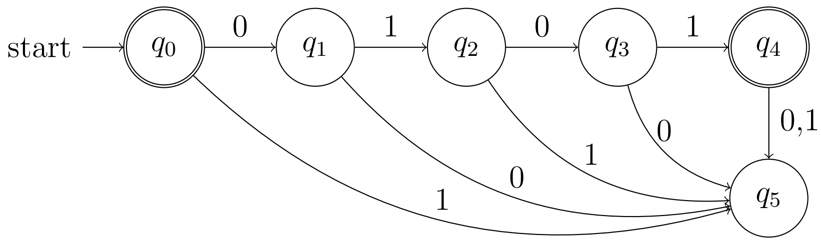

Figure 2: DFA (b) $\{\epsilon, 0101\}$

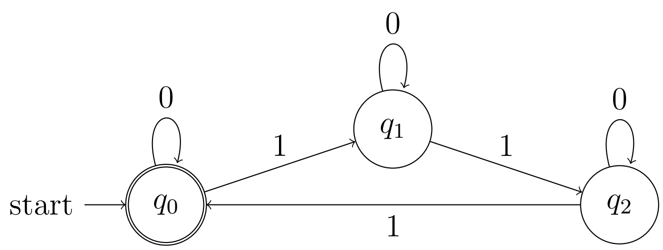

Figure 3: DFA (c) $\{w|\#_1 w \bmod 3 \ \equiv 0\}$

Question 5

Given n, Lets formalize the language

$$L_n = \{w0w_n | w \in \{0,1\}^* \wedge w_n \in \{0,1\}^{n-1}\}$$

lets present NFA $N = (Q, \Sigma, \delta, S, F)$ that accept L_n , we know that any NFA can be transform to DFA .

$$Q = \{q_0, q_1 \ldots, q_n\}, \Sigma = \{0,1\}, S = \{q_0\}, F = \{q_n\}$$

$$\delta(q_i, \sigma) = \begin{cases} \{q_0, q_1\} & \text{if } q_i = q_0 \wedge \sigma = 0 \\ \{q_0\} & \text{if } q_i = q_0 \wedge \sigma = 1 \\ \{q_{i+1}\} & \text{if } 0 < q_i < q_n \forall \sigma \in \Sigma \\ \phi & \text{if } q_i = q_n \forall \sigma \in \Sigma \end{cases}$$

claim 0.3. *N accept L_n*

Proof. $w \in L_n \Leftrightarrow$

$$w \in \{w0w_n | w \in \{0,1\}^* \wedge w_n \in \{0,1\}^{n-1}\} \Leftrightarrow \exists \hat{w} \in \Sigma^*. \exists \sigma \in \{0\}. w_n \in \{0,1\}^{n-1}$$

$$\Leftrightarrow \exists \hat{w} \in \Sigma^*. \exists \sigma \in \{0\}. \hat{\delta}_w(q_1, w_n) \in Q \Leftrightarrow \exists \hat{w} \in \Sigma^*. \exists \exists \delta(q_0, q_1), \hat{\delta}_w(q_1, w_n)) \in Q$$

$$\Leftrightarrow \exists \hat{w} \in \Sigma^*. \exists \hat{\delta}(q_0, q_n) \in Q \Leftrightarrow \exists \exists \ldots q_i, q_j \in Q. \exists \hat{\delta}(q_0, q_n) \in F$$

$$\Leftrightarrow \delta(\hat{\delta}_w(q', q_n), \sigma) \exists q' \in Q \forall \sigma \in \Sigma. \hat{\delta}(q_0, q_n) \in F \Leftrightarrow \phi.(q_0, q_n) \in F \Leftrightarrow (q_0, q_n) \in L(N)$$

to be honest i'm not relay sure about the last few equivalence :) ☐

Now lets show N as DFA

$$Q_m = \{[R] | R \in Q\}, \Sigma = \{0,1\}, \delta_0 = q_0, F_m = \{[R] | R \cap Q \neq \phi\}, \delta_m([R], \sigma) = \cup_{q \in R} \delta(q, \sigma)$$

Question 5 (b)

claim 0.4. *All regular languages is closed under \ with a any regular language.*

Proof. Lets L_1 and L_2 be regular, using the regular opertor we know already, we can immediately claim that following holds

$$L_1 \cap \overline{L_2} \Rightarrow L_1 \backslash L_2 \text{ is regular language}$$

□

Question 6

Let $A = (Q, \sum, \delta, q_0, F)$ be a DFA, and let $w_1, w_2 \in \Sigma^*$ be words such that $\hat{\delta}(q_0, w_1) = \hat{\delta}(q_0, w_2)$. Lets proof that for every word $w \in \Sigma^*$ it holds that $w_1 w \in L(A) \Leftrightarrow w_2 w \in L(A)$ now we set some q_k such as
$\hat{\delta}(q_0, w_1) = \hat{\delta}(q_0, w_2) = q_k \in Q$. now we construct new A_1 and A_2 in the following way:

$$A_1 = (Q, \Sigma, \delta, q_0, q_k = F_1), A_2 = (Q, \Sigma, \delta, q_k, F_2 = F)$$

we can notice that $\hat{\delta}(q_0, w_1) = \hat{\delta}(q_0, w_2) \in L(A_1)$,and for some w such as $w \in L(A_2)$ we get

$$w \in L(A_2) \Leftrightarrow \hat{\delta}(q_k, w) \in F_2 \Leftrightarrow \hat{\delta}(q_k, w) \in F$$

$$\Leftrightarrow q_k \in F_1, \hat{\delta}(q_k, w) \in F$$

$$\Leftrightarrow \forall w' \in L(A_1).\hat{\delta}(\hat{\delta}(q_0, w')), w) \in F$$

$$\hat{\delta}(\hat{\delta}(q_0, w_1)), w) \in F \Leftrightarrow \hat{\delta}(\hat{\delta}(q_0, w_2)), w) \in F$$

$$w_1 w \in L(A) \Leftrightarrow w_2 w \in L(A)$$

Question 6 (b)

Let n be a number and let A be a DFA such that $L(A) = \{0^i 1^i : 0 \leq i \leq n\}$. now follow the hint

claim 0.5. $\hat{\delta}(q_0, 0^i) \neq \hat{\delta}(q_0, 0^i)$ *for any* $i \neq j$

Proof. lets assume that $\hat{q} = \hat{\delta}(q_0, 0^i) = \hat{\delta}(q_0, 0^j)$ and without any loss of generality $i < j$ .from A definition we know that $w_i := 0^i 1^i, w_i := 0^j 1^j \in L(A)$ i.e for $\hat{\delta}(\hat{\delta}(q_0, 0^j), 1^i)$ we can get to for some $q \in F$. now lets look at

$$\hat{\delta}(q_0, w) \in F \Rightarrow \ \hat{\delta}(\hat{\delta}(q_0, 0^i), 1^j) = \hat{\delta}(\hat{q}, 1^i)$$

under the assuming we lets look at

$$\hat{\delta}(\hat{q}, 1^i) = \hat{\delta}(\hat{\delta}(q_0, 0^j), 1^i) = \hat{\delta}(q_0, 0^j 1^i) \in F$$

and we got an contradiction.

□

Hence the claim above hold for any $i \neq j$ and in total we find that A has at least n accepting state.