Student name: _____ **Student Number:** _____

CSE 311: Foundations of Computing I - Spring 2023

Final Exam - Practice Solutions

Do not open until instructed to start.

Read the instructions on this page carefully.

Instructions. This exam is meant to be solved in 1 hour and 50 minutes. **The start time is given on the syllabus and you are required to stop writing at** after 1 hour and 50 minutes, unless otherwise instructed. When done, wait for a proctor to collect your solution, or follow any other instructions by the proctors.

- This exam consists of **eight tasks**, overall with **120 points**.
- **Write your name and student number on the top of this page**
- This is a **closed-book exam.** No written document is allowed. In particular, you are not allowed to use any textbooks, nor additional personal notes, homework assignments or solutions, etc.
- Four pages of detachable cheat sheet are provided on the front and back of the last two pages of this exam. Please be gentle when removing them! You must keep the rest of your exam together. (We will also collect the cheat sheets at the end of the exam.)
- **No electronics are allowed** during the exam (no smart phones, no laptops, no smart watches, no pocket calculators, etc). Keep them stored in your bag.
- Write your solutions in the appropriate spaces. The backs of pages are also available for solutions. if you use them to extend an answer to a question, please put a pointer from that question to the place on the back that you use.

Good luck!

Task 1 – Regularly Irregular [15 pts]

Let $\Sigma = \{0, 1\}$. Prove that the language $L = \{x \in \Sigma^* \ : \ \#_0(x) < \#_1(x)\}$ is irregular.

Suppose for contradiction that M is an arbitrary DFA that recognizes L.

Let $S = \{0^n \ : \ n \geqslant 0\}$. Since S is infinite and M has finitely many states, there exist two different elements of S that end in the same state. Since these two strings are different, and since every element of S consists only of 0s, it follows that the two strings have different length. Let i be the length of the shorter of the two strings and j be the length of the longer string. Then $i < j$ and the two elements of S can be written as 0^i and 0^j.

Now consider appending 1^j to both strings. Then we get

$a = 0^i 1^j$	Note that $a \in L$ because $i < j$
$b = 0^j 1^j$	Note that $b \notin L$ because $j \not< j$

Since a and b both end in the same state, and that state cannot both be an accept and reject state, M must give the wrong answer for one of the strings a or b. Therefore, D does not recognize L. Since D was arbitrary, no DFA recognizes L, so, L is irregular.

Task 2 – Recurrences, Recurrences [15 pts]

Define

$$T(n) = \begin{cases} n & \text{if } n = 0 \text{ or } n = 1 \\ 4T\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + n & \text{otherwise.} \end{cases}$$

Prove that $T(n) \leqslant n^3$ for all integers $n \geqslant 3$.

We will proceed by strong induction on n.

Let $P(n)$ be "$T(n) \leqslant n^3$" for $n \in \mathbb{N}$. We will prove $P(n)$ holds for all integers $n \geqslant 3$.

Base Cases. First, note that $T(1) = 1$ and $T(2) = 4T(1) + 2 = 6$.

When $n = 3$, we have $T(3) = 4T\left(\left\lfloor \frac{3}{2} \right\rfloor\right) + 3 = 4T(1) + 3 = 7 \leqslant 27 = 3^3$.

When $n = 4$, we have $T(4) = 4T\left(\left\lfloor \frac{4}{2} \right\rfloor\right) + 4 = 4T(2) + 4 = 4 \cdot 6 + 4 = 28 \leqslant 64 = 4^3$.

When $n = 5$, we have $T(5) = 4T\left(\left\lfloor \frac{5}{2} \right\rfloor\right) + 5 = 4T(2) + 5 = 4 \cdot 6 + 5 = 29 \leqslant 125 = 5^3$.

Therefore $P(3)$, $P(4)$, and $P(5)$ are all true.

Induction Hypothesis. Suppose that $P(j)$ is true for every integer j with $3 \leqslant j \leqslant k$ for $k \geqslant 5$; that is, supposed that $T(j) \leqslant j^3$ for every integer j with $3 \leqslant j \leqslant k$.

Inductive Step. Goal: We want to prove $P(k+1)$; that is, $T(k+1) \leqslant (k+1)^3$.

Since $k \geqslant 5$, we have $k + 1 \geqslant 6$ and so $3 \leqslant \lfloor \frac{k+1}{2} \rfloor \leqslant k$. Therefore,

$$\begin{aligned}
T(k+1) &= 4T\left(\left\lfloor \frac{k+1}{2} \right\rfloor\right) + (k+1) && \text{by definition of } T \text{ since } k+1 \geqslant 2 \\
&\leqslant 4\left(\left\lfloor \frac{k+1}{2} \right\rfloor\right)^3 + (k+1) && \text{by I.H. for } j = \left\lfloor \frac{k+1}{2} \right\rfloor \text{ since } 3 \leqslant j \leqslant k \\
&\leqslant 4\left(\frac{k+1}{2}\right)^3 + (k+1) && \text{by definition of } \lfloor \cdot \rfloor \\
&= 4\frac{(k+1)^3}{8} + (k+1) && \text{[Algebra]} \\
&= \frac{(k+1)^3}{2} + (k+1) && \text{[Algebra]} \\
&= (k+1) \cdot \left(\frac{(k+1)^2}{2} + 1\right) && \text{[Algebra]} \\
&\leqslant (k+1) \cdot \left(\frac{(k+1)^2}{2} + \frac{(k+1)^2}{2}\right) && \text{since } k+1 \geqslant 2 \text{ so } (k+1)^2 \geqslant 2 \\
&= (k+1)^3 && \text{[Algebra]}
\end{aligned}$$

which is what we wanted to show. Therefore $P(k+1)$ is true.

Conclusion. Therefore $T(n) \leqslant n^3$ for all $n \geqslant 3$.

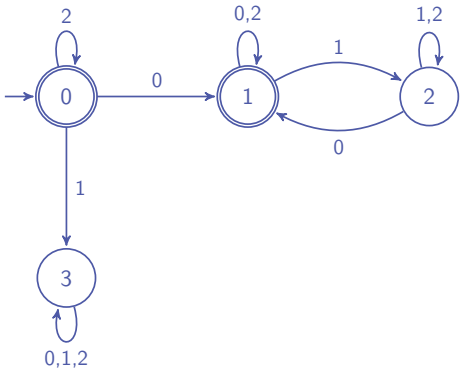
Task 3 – All the Machines! [15 pts]

Let $\Sigma = \{0, 1, 2\}$. Consider $A = \{w \in \Sigma^* \text{ : Every 1 in the string has at least one 0 before and after it}\}$.

a) Give a regular expression that represents A.

$(0 \cup 2)^* \cup (0 \cup 2)^*0(0 \cup 1 \cup 2)^*0(0 \cup 2)^*$

b) Give a DFA that recognizes A.



c) Give a CFG that generates A.

One solution:

$$\begin{aligned}
&\mathbf{S} \to \mathbf{U} \mid \mathbf{UTU} \\
&\mathbf{T} \to 0\mathbf{V}0 \\
&\mathbf{U} \to \varepsilon \mid 0\mathbf{U} \mid 2\mathbf{U} \\
&\mathbf{V} \to \varepsilon \mid 0\mathbf{V} \mid 1\mathbf{V} \mid 2\mathbf{V}
\end{aligned}$$

S generates all strings in A.
T generates all strings in Σ^* that begin and end in 0.
U generates all in Σ^* that that don't contain a 1.
V generates all strings in Σ^*.

Another solution:

$$\begin{aligned}
&\mathbf{S} \to \varepsilon \mid 0\mathbf{S} \mid 2\mathbf{S} \mid 0\mathbf{ST} \\
&\mathbf{T} \to 1\mathbf{R}0\mathbf{S} \\
&\mathbf{R} \to \varepsilon \mid 0\mathbf{R} \mid 1\mathbf{R} \mid 2\mathbf{R}
\end{aligned}$$

S generates all strings in A (which can't begin with 1).
R generates all strings in Σ^*
T generates the ends of strings in Σ^* that begin with a 1, have a later 0 followed by a string in A.

Task 4 – Structural CFGs [15 pts]

Consider the following CFG: $\mathbf{S} \to \varepsilon \mid \mathbf{SS} \mid \mathbf{S}1 \mid \mathbf{S}01$. Another way of writing the recursive definition of this set, Q, is as follows:

- $\varepsilon \in Q$.
- If $s \in Q$, then $s1 \in Q$ and $s01 \in Q$
- If $s, t \in Q$, then $st \in Q$.

Prove by structural induction that if $w \in Q$, then w has at least as many 1's as 0's.

We go by structural induction over the set Q. Let $P(w)$ be "$\#_1(w) \geqslant \#_0(w)$" for $w \in Q$. We prove that $P(w)$ is true for all $w \in Q$.

Base Case. When $w = \varepsilon$, note that $\#_0(w) = 0 = \#_1(w)$. So, $P(\varepsilon)$ is true.

Induction Hypothesis. Suppose that $P(s)$ and $P(t)$ are true for some s and t in Q.

Inductive Step. Goal: We need to show that $P(s1)$, $P(s01)$, and $P(st)$ are all true.

$$\begin{aligned} \#_1(s1) &= \#_1(s) + 1 && \text{by definition} \\ &\geqslant \#_0(s) + 1 && \text{by I.H. for } s \\ &= \#_0(s1) + 1 && \text{by definition} \\ &> \#_0(s1) \end{aligned}$$

so $P(s1)$ is true.

$$\begin{aligned} \#_1(s01) &= \#_1(s) + 1 && \text{by definition} \\ &\geqslant \#_0(s) + 1 && \text{by I.H. for } s \\ &= \#_0(s01) && \text{by definition} \end{aligned}$$

so $P(s01)$ is true.

$$\begin{aligned} \#_1(st) &= \#_1(s) + \#_1(t) && \text{by definition} \\ &\geqslant \#_0(s) + \#_0(t) && \text{by I.H. for } s \text{ and for } t \\ &= \#_0(st) && \text{by definition} \end{aligned}$$

so $P(st)$ is true.

Conclusion: Therefore $P(w)$ is true for every element in Q and hence everything generated by the grammar has at least as many 1's as 0's.

Task 5 – Tralse! [15 pts]

For each of the following answer True or False and give a short explanation of your answer.

a) True or False: Any subset of a regular language is also regular.

Solution: False. Consider $\{0,1\}^*$ and $\{0^n1^n \ : \ n \geqslant 0\}$. Note that the first is regular and the second is irregular, but the second is a subset of the first.

b) True or False: The set of programs that loop forever on at least one input is decidable.

False. If we could solve this problem, we could solve HaltNoInput. Intuitively, a program that solves this problem would have to try all inputs, but, since the program might infinite loop on some of them, it won't be able to.

c) True or False: If $\mathbb{R} \subseteq A$ for some set A, then A is uncountable.

True. Diagonalization would still work; alternatively, if A were countable, then we could find an onto function between $\mathbb{N}$ and $\mathbb{R}$ by skipping all the elements in A that aren't in $\mathbb{R}$.

d) True or False: If the domain of discourse is people, the logical statement

$$\exists x \left(P(x) \rightarrow \forall y \left((x \neq y) \rightarrow \neg P(y)\right)\right)$$

can be correctly translated as "There exists a unique person who has property P".

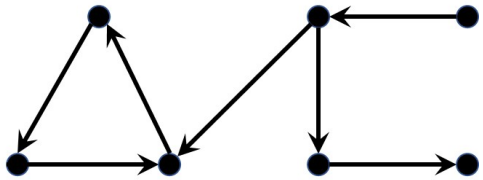
False. Any x for which $P(x)$ is false makes the entire statement true. This is not the same as there existing a unique person with property P.

e) True or False: $(\exists x \ \forall y P(x,y)) \rightarrow (\forall y \exists x \, P(x,y))$ is true regardless of what predicate P is.

True. The left part of the implication is saying that there is a single x that works for all y; the right one is saying that for every y, we can find an x that may depends on it, but the single x that works for all y will still work.

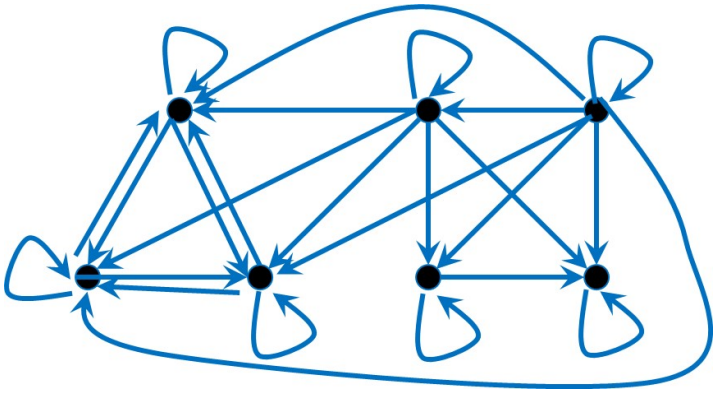
Task 6 – Relationships! [15 pts]

The following is a graph of a binary relation R.



a) Draw the transitive-reflexive closure of R.

Solution:

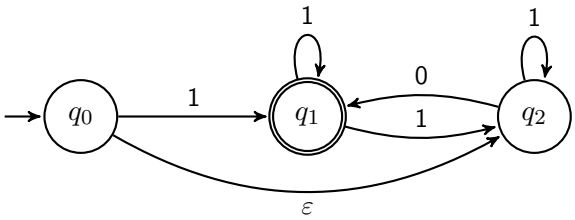


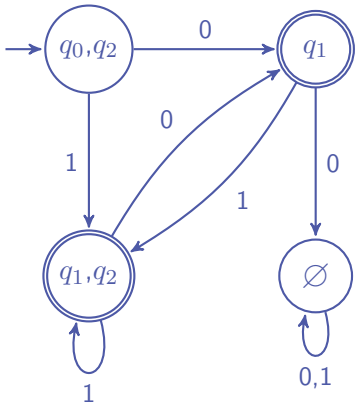
b) Let $S = \{(X, Y) \ : \ X, Y \in \mathcal{P}(\mathbb{N}) \ \wedge \ X \subseteq Y\}$.
Recall that R is antisymmetric iff $((a, b) \in R \ \wedge a \neq b) \rightarrow (b, a) \notin R$.
Prove that S is antisymmetric.

Suppose that $(a, b) \in S$ and $a \neq b$. Then, by definition of S, $a \subseteq b$ and there is some $x \in b$ where $x \notin a$ (since they aren't equal). Then, $(b, a) \notin S$, because $b \nsubseteq a$, because $x \in b$ and $x \notin a$. So, S is antisymmetric.

Task 7 – Construction Paper [15 pts]

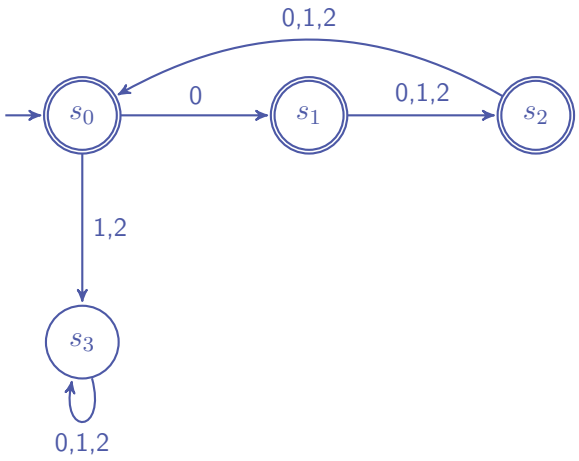
Convert the following NFA into a DFA using the algorithm from lecture.





Task 8 – Modern DFAs [15 pts]

Let $\Sigma = \{0, 1, 2\}$. Construct a DFA that recognizes exactly strings with a 0 in all positions i (counting from the left end of the string where the first character is $i = 0$) where $i \bmod 3 = 0$.



CSE 311: Foundations of Computing I

Logical Equivalences Reference Sheet

Identity

$$p \wedge \mathsf{T} \equiv p$$
$$p \vee \mathsf{F} \equiv p$$

Domination

$$p \vee \mathsf{T} \equiv \mathsf{T}$$
$$p \wedge \mathsf{F} \equiv \mathsf{F}$$

Idempotency

$$p \vee p \equiv p$$
$$p \wedge p \equiv p$$

Commutativity

$$p \vee q \equiv q \vee p$$
$$p \wedge q \equiv q \wedge p$$

Associativity

$$(p \vee q) \vee r \equiv p \vee (q \vee r)$$
$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$$

Distributivity

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$
$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

Absorption

$$p \vee (p \wedge q) \equiv p$$
$$p \wedge (p \vee q) \equiv p$$

Negation

$$p \vee \neg p \equiv \mathsf{T}$$
$$p \wedge \neg p \equiv \mathsf{F}$$

DeMorgan's Laws

$$\neg(p \vee q) \equiv \neg p \wedge \neg q$$
$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

Double Negation

$$\neg\neg p \equiv p$$

Law of Implication

$$p \rightarrow q \equiv \neg p \vee q$$

Contrapositive

$$p \rightarrow q \equiv \neg q \rightarrow \neg p$$

CSE 311: Foundations of Computing I

Axioms & Inference Rules

Excluded Middle

$$\therefore \quad A \vee \neg A$$

Direct Proof

$$\frac{A \Rightarrow B}{\therefore \quad A \to B}$$

Modus Ponens

$$\frac{A \qquad A \to B}{\therefore \qquad B}$$

Intro $\wedge$

$$\frac{A \qquad B}{\therefore \quad A \wedge B}$$

Elim $\wedge$

$$\frac{A \wedge B}{\therefore \; A \qquad B}$$

Intro $\vee$

$$\frac{A}{\therefore \; A \vee B \quad B \vee A}$$

Elim $\vee$

$$\frac{A \vee B \qquad \neg A}{\therefore \qquad B}$$

Intro $\exists$

$$\frac{P(c) \text{ for some } c}{\therefore \qquad \exists x \; P(x)}$$

Elim $\forall$

$$\frac{\forall x \; P(x)}{\therefore \; P(a) \text{ for any } a}$$

Intro $\forall$

$$\frac{\text{Let } a \text{ be arbitrary} \ldots P(a)}{\therefore \; \forall x \; P(x) \qquad (\text{If no other name in } P \text{ depends on } a)}$$

Elim $\exists$

$$\frac{\exists x \; P(x)}{\therefore \; P(c) \text{ for some } \textit{special } c \qquad \text{list dependencies for } c}$$

CSE 311: Foundations of Computing I

Modular Arithmetic: Definitions and Properties

Definition: "a divides b"

For $a \in \mathbb{Z}, b \in \mathbb{Z}$ with $a \neq 0$:

$\boxed{a \mid b \leftrightarrow \exists k \in \mathbb{Z}\ (b = ka)}$

Division Theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}$ with $d > 0$, there exist *unique integers* q, r with $0 \leq r < d$, such that $a = dq + r$.

To put it another way, if we divide d into a, we get a unique quotient ($q = a$ div d) and non-negative remainder smaller than d ($r = a$ mod d).

Definition: "a is congruent to b modulo m"

For $a, b, m \in \mathbb{Z}$ with $m > 0$:

$\boxed{a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)}$

Properties of mod

- Let a, b, m be integers with $m > 0$. Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.
- Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.
- Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
- Let a, b, m be integers with $m > 0$. Then, $(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$.
  - You can derive this using the Multiplication Property of Congruences; note that $a \equiv (a \bmod m) \pmod{m}$ and $b \equiv (b \bmod m) \pmod{m}$.

GCD and Euclid's algorithm

- $\gcd(a, b)$ is the largest integer d such that $d \mid a$ and $d \mid b$.
- **Euclid's algorithm:** To efficiently compute $\gcd(a, b)$, you can repeatedly apply these facts:
  - $\gcd(a, b) = \gcd(b, a \bmod b)$
  - $\gcd(a, 0) = a$

Bézout's Theorem and Multiplicative Inverses

- **Bézout's Theorem:** If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.
  - To find s and t, you can use the Extended Euclidean Algorithm. See slides for a full walkthrough.
- The **multiplicative inverse mod** m of $a \bmod m$ is $b \bmod m$ iff $ab \equiv 1 \pmod{m}$.
- Suppose $\gcd(a, m) = 1$. By Bézout's Theorem, there exist integers s and t such that $sa + tm = 1$. Taking the mod of both sides, we get $(sa + tm) \bmod m = 1 \bmod m = 1$, so $sa \equiv 1 \pmod{m}$. Thus, $s \bmod m$ is the multiplicative inverse of a.

CSE 311: Foundations of Computing I

Set Definitions

Common Sets

- $\mathbb{N} = \{0, 1, 2, \dots\}$ is the set of *Natural Numbers*.
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is the set of *Integers*.
- $\mathbb{Q} = \left\{ \frac{p}{q} \ : \ p, q \in \mathbb{Z} \wedge q \neq 0 \right\}$ is the set of *Rational Numbers*.
- $\mathbb{R}$ is the set of *Real Numbers*.

Containment, Equality, and Subsets

Let A, B be sets. Then:

- $x \in A$ ("x is an *element* of A") means that x is an element of A.
- $x \notin A$ ("x is *not* an *element* of A") means that x is *not* an element of A.
- $A \subseteq B$ ("A is a *subset* of B") means that all the elements of A are also in B.
- $A \supseteq B$ ("A is a *superset* of B") means that all the elements of B are also in A.
- $(A = B) \equiv (A \subseteq B) \wedge (B \subseteq A) \equiv \forall x \ (x \in A \leftrightarrow x \in B)$

Set Operations

Let A, B be sets. Then:

- $A \cup B$ is the *union* of A and B. $A \cup B = \{x \ : \ x \in A \vee x \in B\}$.
- $A \cap B$ is the *intersection* of A and B. $A \cap B = \{x \ : \ x \in A \wedge x \in B\}$.
- $A \setminus B$ is the *difference* of A and B. $A \setminus B = \{x \ : \ x \in A \wedge x \notin B\}$.
- $A \oplus B$ is the *symmetric difference* of A and B. $A \oplus B = \{x \ : \ x \in A \oplus x \in B\}$.
- $\overline{A}$ is the *complement* of A. If we restrict ourselves to a "universal set", $\mathcal{U}$, (a set of all possible things we're discussing), then $\overline{A} = \{x \in \mathcal{U} \ : \ x \notin A\} = \{x \in \mathcal{U} \ : \ \neg(x \in A)\}$.

Set Constructions

Let A, B, C, D be sets and P be a predicate. Then:

- $S = \{x \ : \ \mathrm{P}(x)\}$ is notation which means that S is a set that contains all objects x (in the domain of P) with property P.
- $A \times B$ is the *cartesian product* of A and B. $A \times B = \{(a, b) \ : \ a \in A, \ b \in B\}$.
- $[n]$ ("*brackets* n") is the set of natural numbers from 1 to n. $[n] = \{x \in \mathbb{N} \ : \ 1 \leq x \leq n\}$.
- $\mathcal{P}(A)$ is the *power set* of A. $\mathcal{P}(A) = \{S \ : \ S \subseteq A\}$.