**Student name:** ______________ **Student Number:** ______________

CSE 311: Foundations of Computing I - Spring 2023

# Final Exam - Practice

**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.

## 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 $n \geqslant 3$.

## 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 $A$.

**b)** Give a DFA that recognizes $A$.

**c)** Give a CFG that generates $A$.

## Task 4 – Structural CFGs [15 pts]

Consider the following CFG: **S** $\to \varepsilon$ | **SS** | **S**$1$ | **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.

## 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.

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

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

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

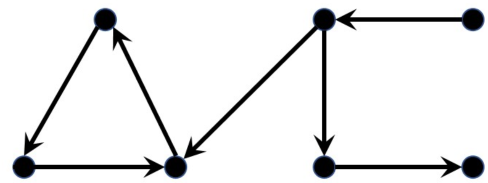
$$\exists x \, (P(x) \to \forall y \, ((x \neq y) \to \neg P(y))$$

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

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

## Task 6 – Relationships! [15 pts]

The following is a graph of a binary relation $R$.

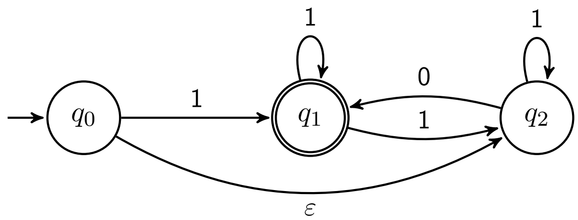


**a)** Draw the transitive-reflexive closure of $R$.

**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.

## 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

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

## Axioms & Inference Rules

**Excluded Middle**

$$\begin{array}{l} \\ \hline \therefore\ A \lor \neg A \end{array}$$

**Direct Proof**

$$\begin{array}{l} \quad A \Rightarrow B \\ \hline \therefore\ A \rightarrow B \end{array}$$

**Modus Ponens**

$$\begin{array}{lcc} & A & A \rightarrow B \\ \hline \therefore & & B \end{array}$$

**Intro $\land$**

$$\begin{array}{lcc} & A & B \\ \hline \therefore & \multicolumn{2}{c}{A \land B} \end{array}$$

**Elim $\land$**

$$\begin{array}{lcc} & \multicolumn{2}{c}{A \land B} \\ \hline \therefore & A & B \end{array}$$

**Intro $\lor$**

$$\begin{array}{lcc} & \multicolumn{2}{c}{A} \\ \hline \therefore & A \lor B & B \lor A \end{array}$$

**Elim $\lor$**

$$\begin{array}{lcc} & A \lor B & \neg A \\ \hline \therefore & & B \end{array}$$

**Intro $\exists$**

$$\begin{array}{ll} & P(c) \text{ for some } c \\ \hline \therefore & \exists x\ P(x) \end{array}$$

**Elim $\forall$**

$$\begin{array}{ll} & \forall x\ P(x) \\ \hline \therefore & P(a) \text{ for any } a \end{array}$$

**Intro $\forall$**

$$\begin{array}{ll} \multicolumn{2}{c}{\text{Let } a \text{ be arbitrary} \ldots P(a)} \\ \hline \therefore\ \forall x\ P(x) & \text{(If no other name in } P \text{ depends on } a\text{)} \end{array}$$

**Elim $\exists$**

$$\begin{array}{ll} \multicolumn{2}{c}{\exists x\ P(x)} \\ \hline \therefore\ P(c) \text{ for some } \textit{special } c & \text{list dependencies for } c \end{array}$$

# 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 $a$ mod $m = b$ mod $m$.
- 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

- $\mathbb{N} = \{0, 1, 2, \ldots\}$ is the set of *Natural Numbers*.
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is the set of *Integers*.
- $\mathbb{Q} = \left\{\frac{p}{q} \;:\; p, q \in \mathbb{Z} \land q \neq 0\right\}$ 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 $A$.
- $(A = B) \equiv (A \subseteq B) \land (B \subseteq A) \equiv \forall x\, (x \in A \leftrightarrow x \in B)$

## Set Operations

Let $A, B$ be sets. Then:

- $A \cup B$ is the *union* of $A$ and $B$. $A \cup B = \{x \;:\; x \in A \lor x \in B\}$.
- $A \cap B$ is the *intersection* of $A$ and $B$. $A \cap B = \{x \;:\; x \in A \land x \in B\}$.
- $A \setminus B$ is the *difference* of $A$ and $B$. $A \setminus B = \{x \;:\; x \in A \land x \notin B\}$.
- $A \oplus B$ 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:

- $S = \{x \;:\; \mathsf{P}(x)\}$ 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 $A$. $\mathcal{P}(A) = \{S \;:\; S \subseteq A\}$.