CIS 570 — Introduction to Formal Language Theory — Fall 2008

Exercise Set 1

Model Answers

Exercise 1

Suppose A, B and C are sets.

(1) $(A \cup (B \cap C) = (A \cup B) \cap (A \cup C))$ It will suffice to show that

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C).$$

- $(A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C))$ Suppose that $x \in A \cup (B \cap C)$. We must show that $x \in (A \cup B) \cap (A \cup C)$. Since $x \in A \cup (B \cap C)$, there are two cases to consider.
  - Suppose $x \in A$. Thus $x \in A \cup B$ and $x \in A \cup C$, so that $x \in (A \cup B) \cap (A \cup C)$.
  - Suppose $x \in B \cap C$. Hence $x \in B$ and $x \in C$. Since $x \in B$, we have that $x \in A \cup B$. And, since $x \in C$, we have that $x \in A \cup C$. Thus $x \in (A \cup B) \cap (A \cup C)$.
- $((A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C))$ Suppose $x \in (A \cup B) \cap (A \cup C)$. We must show that $x \in A \cup (B \cap C)$. Since $x \in (A \cup B) \cap (A \cup C)$, we have that $x \in A \cup B$ and $x \in A \cup C$. Since $x \in A \cup B$, there are two cases to consider.
  - Suppose $x \in A$. Thus $x \in A \cup (B \cap C)$.
  - Suppose $x \in B$. Since $x \in A \cup C$, there are two sub-cases to consider.
    - Suppose $x \in A$. Thus $x \in A \cup (B \cap C)$.
    - Suppose $x \in C$. Since $x \in B$ and $x \in C$, we have that $x \in B \cap C$. Thus $x \in A \cup (B \cap C)$.

(2) $((A \cap B) \cup C = (A \cup C) \cap (B \cup C))$ It will suffice to show that

$$(A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C.$$

- $((A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C))$ Suppose that $x \in (A \cap B) \cup C$. We must show that $x \in (A \cup C) \cap (B \cup C)$. Since $x \in (A \cap B) \cup C$, there are two cases to consider.
  - Suppose $x \in A \cap B$. Hence $x \in A$ and $x \in B$. Since $x \in A$, we have that $x \in A \cup C$. And, since $x \in B$, we have that $x \in B \cup C$. Thus $x \in (A \cup C) \cap (B \cup C)$.
  - Suppose $x \in C$. Thus $x \in A \cup C$ and $x \in B \cup C$, so that $x \in (A \cup C) \cap (B \cup C)$.
- $((A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C)$ Suppose $x \in (A \cup C) \cap (B \cup C)$. We must show that $x \in (A \cap B) \cup C$. Since $x \in (A \cup C) \cap (B \cup C)$, we have that $x \in A \cup C$ and $x \in B \cup C$. Since $x \in A \cup C$, there are two cases to consider.
  - Suppose $x \in A$. Since $x \in B \cup C$, there are two sub-cases to consider.
    - Suppose $x \in B$. Since $x \in A$ and $x \in B$, we have that $x \in A \cap B$. Thus $x \in (A \cap B) \cup C$.
    - Suppose $x \in C$. Thus $x \in (A \cap B) \cup C$.
  - Suppose $x \in C$. Thus $x \in (A \cap B) \cup C$.

Exercise 2

The problems are:

- Because f is supposed to be a function from $\mathbb{N}$ to $\mathbb{N}$, and $0 \in \mathbb{N}$, $f\,0$ must be defined. But when $n = 0$, neither clause's condition holds, and so $f\,0$ could any element of $\mathbb{N}$. Hence f isn't uniquely specified.
- Because $1 \geq 1$ and $1 \leq 10$, the first clause requires that $f\,1 = 1 - 2 = -1$. But $-1 \notin \mathbb{N}$, and thus $f \notin \mathbb{N} \to \mathbb{N}$.
- When $n = 10$, we have that both
  - $n \geq 1$ and $n \leq 10$, and
  - $n \geq 10$,

  i.e., both clauses' conditions hold. Hence $f\,10$ must be equal to both $10-2 = 8$ and $10+2 = 12$, which is impossible.

Exercise 3

We proceed by mathematical induction.

- (Basis Step) We have that $0(0^2 + 5) = 0 = 6 \cdot 0$ and $0 \in \mathbb{N}$. Thus $0(0^2 + 5)$ is divisible by 6.
- (Inductive Step) Suppose $n \in \mathbb{N}$, and assume the inductive hypothesis: $n(n^2 + 5)$ is divisible by 6. Since $n(n^2 + 5) = n^3 + 5n$, it follows that $n^3 + 5n = 6l$, for some $l \in \mathbb{N}$. By Proposition 1.2.2, we have that $3n^2 + 3n + 6$ is divisible by 6. Hence $3n^2 + 3n + 6 = 6m$, for some $m \in \mathbb{N}$. Thus, we have that

$$\begin{aligned}(n+1)((n+1)^2+5) &= (n+1)((n^2+2n+1)+5) = (n+1)(n^2+2n+6) \\ &= n^3+2n^2+6n+n^2+2n+6 = n^3+3n^2+8n+6 \\ &= (n^3+5n)+(3n^2+3n+6) = 6l+6m = 6(l+m),\end{aligned}$$

  and $l + m \in \mathbb{N}$, showing that $(n + 1)((n + 1)^2 + 5)$ is divisible by 6.

Exercise 4

We proceed by strong induction. Suppose $n \in \mathbb{N}$, and assume the inductive hypothesis: for all $m \in \mathbb{N}$, if $m < n$, then

$$\text{if } m \geq 1, \text{ then there are } i, j \in \mathbb{N} \text{ such that } m = 2^i(2j + 1).$$

We must show that

$$\text{if } n \geq 1, \text{ then there are } i, j \in \mathbb{N} \text{ such that } n = 2^i(2j + 1).$$

Suppose $n \geq 1$. We must show that there are $i, j \in \mathbb{N}$ such that $n = 2^i(2j + 1)$. There are two cases to consider.

- Suppose n is odd. Then $n = 2j + 1$ for some $j \in \mathbb{N}$. Hence $n = 1(2j + 1) = 2^0(2j + 1)$ and $0, j \in \mathbb{N}$.
- Suppose n is even. Hence $n/2 \in \mathbb{N}$. And $n \geq 2$, so that $1 \leq n/2 < n$. By the inductive hypothesis, we have that

  $$\text{if } n/2 \geq 1, \text{ then there are } i, j \in \mathbb{N} \text{ such that } n/2 = 2^i(2j + 1).$$

  But $n/2 \geq 1$, and thus there are $i, j \in \mathbb{N}$ such that $n/2 = 2^i(2j + 1)$. Hence $n = 2(n/2) = 2(2^i(2j + 1)) = 2^{i+1}(2j + 1)$ and $i + 1, j \in \mathbb{N}$.

Exercise 5

(a) We use induction on X to show that, for all $w \in X$, $w \in Y$. There are four steps to show.

(1) We must show that $\% \in Y$. Since the only prefix of $\%$ is itself, and $\mathbf{diff}\,\% = 0 \geq 0$, it follows that $\% \in Y$.

(2) We must show that $\mathsf{1} \in Y$. Since $\%$ and $\mathsf{1}$ are the only prefixes of $\mathsf{1}$, $\mathbf{diff}\,\% = 0 \geq 0$ and $\mathbf{diff}\,\mathsf{1} = 1 \geq 0$, we have that $\mathsf{1} \in Y$.

(3) Suppose $x, y \in X$, and assume the inductive hypothesis: $x, y \in Y$. We must show that $\mathsf{1}x\mathsf{1}y\mathsf{0} \in Y$. Suppose that v is a prefix of $\mathsf{1}x\mathsf{1}y\mathsf{0}$. We must show that $\mathbf{diff}\,v \geq 0$. There are four cases to consider.

- Suppose $v = \%$. Then $\mathbf{diff}\,v = \mathbf{diff}\,\% = 0 \geq 0$.
- Suppose $v = \mathsf{1}u$, for some prefix u of x. Because $x \in Y$ and u is a prefix of x, we have that $\mathbf{diff}\,u \geq 0$. Thus

  $$\mathbf{diff}\,v = \mathbf{diff}(\mathsf{1}u) = \mathbf{diff}\,\mathsf{1} + \mathbf{diff}\,u = 1 + \mathbf{diff}\,u \geq 1 + 0 \geq 0.$$

- Suppose $v = \mathsf{1}x\mathsf{1}u$, for some prefix u of y. Because $x \in Y$ and x is a prefix of itself, we have that $\mathbf{diff}\,x \geq 0$. Because $y \in Y$ and u is a prefix of y, we have that $\mathbf{diff}\,u \geq 0$. Thus

  $$\begin{aligned}\mathbf{diff}\,v = \mathbf{diff}(\mathsf{1}x\mathsf{1}u) &= \mathbf{diff}\,\mathsf{1} + \mathbf{diff}\,x + \mathbf{diff}\,\mathsf{1} + \mathbf{diff}\,u \\ &= 1 + \mathbf{diff}\,x + 1 + \mathbf{diff}\,u = 2 + \mathbf{diff}\,x + \mathbf{diff}\,u \\ &\geq 2 + 0 + 0 = 2 \geq 0.\end{aligned}$$

- Suppose $v = \mathsf{1}x\mathsf{1}y\mathsf{0}$. Because $x \in Y$ and x is a prefix of itself, we have that $\mathbf{diff}\,x \geq 0$. Because $y \in Y$ and y is a prefix of itself, we have that $\mathbf{diff}\,y \geq 0$. Thus

  $$\begin{aligned}\mathbf{diff}\,v = \mathbf{diff}(\mathsf{1}x\mathsf{1}y\mathsf{0}) &= \mathbf{diff}\,\mathsf{1} + \mathbf{diff}\,x + \mathbf{diff}\,\mathsf{1} + \mathbf{diff}\,y + \mathbf{diff}\,\mathsf{0} \\ &= 1 + \mathbf{diff}\,x + 1 + \mathbf{diff}\,y + -2 = \mathbf{diff}\,x + \mathbf{diff}\,y \geq 0 + 0 = 0.\end{aligned}$$

(4) Suppose $x, y \in X$, and assume the inductive hypothesis: $x, y \in Y$. We must show that $xy \in Y$. Suppose that v is a prefix of xy. We must show that $\mathbf{diff}\,v \geq 0$. There are two cases to consider.

- Suppose v is a prefix of x. Since $x \in Y$, it follows that $\mathbf{diff}\, v \geq 0$.
- Suppose $v = xu$, for some prefix u of y. Since $x \in Y$ and x is a prefix of itself, we have that $\mathbf{diff}\, x \geq 0$. And, since $y \in Y$ and u is a prefix of y, we have that $\mathbf{diff}\, u \geq 0$. Thus $\mathbf{diff}\, v = \mathbf{diff}(xu) = \mathbf{diff}\, x + \mathbf{diff}\, u \geq 0 + 0 = 0$.

(b) We begin by proving a useful lemma.

Lemma ES1.5.1
For all $w \in \{\mathsf{0}, \mathsf{1}\}^*$, if $\mathbf{diff}\, w \geq 1$ and $w \in Y$, then there are $x, y \in Y$ such that $w = x\mathsf{1}y$.

Proof. Suppose $w \in \{\mathsf{0}, \mathsf{1}\}^*$, $\mathbf{diff}\, w \geq 1$ and $w \in Y$. Let z be the shortest suffix of w such that $\mathbf{diff}\, z \geq 1$ (z is well-defined, because w is a suffix of itself and $\mathbf{diff}\, w \geq 1$.) Let $x \in \{\mathsf{0}, \mathsf{1}\}^*$ be such that $w = xz$. Because $\mathbf{diff}\, z \geq 1$, we have that $z \neq \%$, so that $z = by$ for some $b \in \{\mathsf{0}, \mathsf{1}\}$ and $y \in \{\mathsf{0}, \mathsf{1}\}^*$. Thus $w = xz = xby$. Because y is a shorter suffix of w than z, it follows that $\mathbf{diff}\, y \leq 0$.

Suppose, toward a contradiction, that $b = \mathsf{0}$. Since $-2 + \mathbf{diff}\, y = \mathbf{diff}\, b + \mathbf{diff}\, y = \mathbf{diff}(by) = \mathbf{diff}\, z \geq 1$, we have $\mathbf{diff}\, y \geq 3$, contradicting the fact that $\mathbf{diff}\, y \leq 0$. Thus $b = \mathsf{1}$, so that $z = \mathsf{1}y$ and $w = xby = x\mathsf{1}y$.

Since $1 + \mathbf{diff}\, y = \mathbf{diff}(\mathsf{1}y) = \mathbf{diff}\, z \geq 1$, we have that $\mathbf{diff}\, y \geq 0$. But $\mathbf{diff}\, y \leq 0$, so that $\mathbf{diff}\, y = 0$.

To see that $x \in Y$, suppose v is a prefix of x. We must show that $\mathbf{diff}\, v \geq 0$. Because v is a prefix of x, and x is a prefix of $x\mathsf{1}y = w$, it follows that v is a prefix of w. But $w \in Y$, and thus $\mathbf{diff}\, v \geq 0$.

To see that $y \in Y$, suppose v is a prefix of y. We must show that $\mathbf{diff}\, v \geq 0$. Suppose, toward a contradiction, that $\mathbf{diff}\, v \leq -1$. Let $u \in \{\mathsf{0}, \mathsf{1}\}^*$ be such that $y = vu$. Hence $z = \mathsf{1}y = \mathsf{1}vu$ and $w = x\mathsf{1}y = x\mathsf{1}vu$. Because $\mathbf{diff}\, v + \mathbf{diff}\, u = \mathbf{diff}(vu) = \mathbf{diff}\, y = 0$ and $\mathbf{diff}\, v \leq -1$, we have that $\mathbf{diff}\, u \geq 1$. But u is a shorter suffix of w than z, and thus $\mathbf{diff}\, u \leq 0$, by the definition of z—contradiction. Thus $\mathbf{diff}\, v \geq 0$, as required. □

Now, we show that $Y \subseteq X$. Since $Y \subseteq \{\mathsf{0}, \mathsf{1}\}^*$, it will suffice to show that, for all $w \in \{\mathsf{0}, \mathsf{1}\}^*$,

$$\text{if } w \in Y, \text{ then } w \in X.$$

We proceed by strong string induction. Suppose $w \in \{\mathsf{0}, \mathsf{1}\}^*$, and assume the inductive hypothesis: for all $x \in \{\mathsf{0}, \mathsf{1}\}^*$, if x is a proper substring of w, then

$$\text{if } x \in Y, \text{ then } x \in X.$$

We must show that

$$\text{if } w \in Y, \text{ then } w \in X.$$

Suppose $w \in Y$. We must show that $w \in X$. There are three cases to consider.

- Suppose $w = \%$. Then $w = \% \in X$, by Part (1) of the definition of X.
- Suppose $w = \mathsf{0}s$, for some $s \in \{\mathsf{0}, \mathsf{1}\}^*$. Because $w \in Y$ and $\mathsf{0}$ is a prefix of w, we have that $-2 = \mathbf{diff}\, \mathsf{0} \geq 0$—contradiction. Thus $w \in X$.
- Suppose $w = \mathsf{1}s$, for some $s \in \{\mathsf{0}, \mathsf{1}\}^*$. There are two sub-cases to consider.

- Suppose $s \in Y$. By Part (2) of the definition of X, we have that $\mathsf{1} \in X$. And, because s is a proper substring of w, the inductive hypothesis tells us that $s \in X$. Thus, by Part (4) of the definition of X, we have that $w = \mathsf{1}s \in X$.
- Suppose $s \notin Y$. Because $s \in \{\mathsf{0},\mathsf{1}\}^*$, there is a prefix of s with a negative diff. Let z be the shortest prefix of s such that $\textbf{diff}\, z \leq -1$, and let $t \in \{\mathsf{0},\mathsf{1}\}^*$ be such that $s = zt$. Since $\textbf{diff}\, z \leq -1$, we have that $z \neq \%$, so that $z = ub$ for some $u \in \{\mathsf{0},\mathsf{1}\}^*$ and $b \in \{\mathsf{0},\mathsf{1}\}$. Thus $s = zt = ubt$ and $w = \mathsf{1}s = \mathsf{1}ubt$. Because u is a shorter prefix of s than z, it follows that $\textbf{diff}\, u \geq 0$.

  Suppose, toward a contradiction, that $b = \mathsf{1}$. Since $\textbf{diff}\, u + 1 = \textbf{diff}\, u + \textbf{diff}\, b = \textbf{diff}(ub) = \textbf{diff}\, z \leq -1$, we have $\textbf{diff}\, u \leq -2$, contradicting the fact that $\textbf{diff}\, u \geq 0$. Thus $b = \mathsf{0}$, so that $z = ub = u\mathsf{0}$, $s = zt = u\mathsf{0}t$ and $w = \mathsf{1}s = \mathsf{1}u\mathsf{0}t$.

  Since $\textbf{diff}\, u + -2 = \textbf{diff}(u\mathsf{0}) = \textbf{diff}\, z \leq -1$, we have that $\textbf{diff}\, u \leq 1$. But $\textbf{diff}\, u \geq 0$, so that $\textbf{diff}\, u \in \{0, 1\}$.

  Suppose, toward a contradiction, that $\textbf{diff}\, u = 0$. Since $w \in Y$ and $\mathsf{1}u\mathsf{0}$ is a prefix of w, it follows that $-1 = 1 + 0 + -2 = \textbf{diff}(\mathsf{1}u\mathsf{0}) \geq 0$—contradiction. Thus $\textbf{diff}\, u = 1$.

  To see that $u \in Y$, suppose v is a prefix of u. We must show that $\textbf{diff}\, v \geq 0$. Because u is a shorter prefix of s than z, it follows that v is a shorter prefix of s than z. Thus, by the definition of z, we have that $\textbf{diff}\, v \geq 0$. This completes the proof that $u \in Y$.

  To see that $t \in Y$, suppose v is a prefix of t. We must show that $\textbf{diff}\, v \geq 0$. Because $w = \mathsf{1}u\mathsf{0}t$, it follows that $\mathsf{1}u\mathsf{0}v$ is a prefix of w. But $w \in Y$, and thus $\textbf{diff}\, v = 1 + 1 + -2 + \textbf{diff}\, v = \textbf{diff}(\mathsf{1}u\mathsf{0}v) \geq 0$. This completes the proof that $t \in Y$.

  Summarizing, we have that $w = \mathsf{1}u\mathsf{0}t$, $u, t \in Y$ and $\textbf{diff}\, u = 1$. Since $\textbf{diff}\, u \geq 1$ and $u \in Y$, Lemma ES1.5.1 tells us that $u = x\mathsf{1}y$, for some $x, y \in Y$. Thus $w = \mathsf{1}x\mathsf{1}y\mathsf{0}t$. Since x, y and t are proper substrings of w, the inductive hypothesis tells us that $x, y, t \in X$. Since $x, y \in X$, we have that $\mathsf{1}x\mathsf{1}y\mathsf{0} \in X$, by Part (3) of the definition of X. Thus $w = (\mathsf{1}x\mathsf{1}y\mathsf{0})t \in X$, by Part (4) of the definition of X.