# CSE 311: Foundations of Computing I

## Section 4: English Proofs and Sets Solutions

## 1. Odds and Ends

Here is a formal proof that, for any even integer, there is an odd integer greater than it.

| | | |
|---|---|---|
| 1. | Let $x$ be an arbitrary integer | |
| 2.1. | Even($x$) | Assumption |
| 2.2. | $\exists n\,(x = 2n)$ | Defn of Even: 2.1 |
| 2.3. | $x = 2k$ | Elim $\exists$: 2.2 |
| 2.4. | Let $y = 2k + 1$ | |
| 2.5. | $\exists n\,(y = 2n + 1)$ | Intro $\exists$: 2.4 |
| 2.6. | Odd($y$) | Defn of Odd: 2.5 |
| 2.7. | $2k + 1 > 2k$ | Prop of "+" |
| 2.8. | $y > 2k$ | Prop of "=": 2.7, 2.4 |
| 2.9. | $y > x$ | Prop of "=": 2.8, 2.3 |
| 2.10. | Odd($y$) $\wedge$ $(y > x)$ | Intro $\wedge$: 2.6, 2.9 |
| 2.11. | $\exists z$ (Odd($z$) $\wedge$ $(z > x)$) | Intro $\exists$: 2.10 |
| 2. | Even($x$) $\rightarrow \exists z$ (Odd($z$) $\wedge$ $(z > x)$) | Direct Proof |
| 3. | $\forall x$ (Even($x$) $\rightarrow \exists z$ (Odd($z$) $\wedge$ $(z > x)$)) | Intro $\forall$: 1, 2 |

Translate this formal proof to an English proof.

### Solution:

Let $x$ be an arbitrary integer. Suppose that $x$ is even. By the definition of even, we know that $x = 2k$ for some integer $k$. Now, we define $y$ to be the integer $2k + 1$, which is odd by the definition of odd. We know that $2k + 1 > 2k$ regardless of the value of $k$, so we can see that $y$ is both odd and satisfies $y > x$. Since $x$ was arbitrary, we have shown that every even integer has an odd integer greater than it.

## 2. Primality Checking

When checking if a number $n$ is prime by brute force, it is only necessary to check possible factors up to $\sqrt{n}$.

Specifically, we can show the following. Let $n$, $a$, and $b$ be positive integers. Here is a proof that, if $n = ab$, then either $a$ or $b$ is at most $\sqrt{n}$.

| | | |
|---|---|---|
| 1.1. | $n = ab$ | Assumption |
| 1.2.1 | $\neg(a \leq \sqrt{n} \lor b \leq \sqrt{n})$ | Assumption |
| 1.2.2 | $(a > \sqrt{n}) \land (b > \sqrt{n})$ | De Morgan: 1.2.1 |
| 1.2.3 | $a > \sqrt{n}$ | Elim $\land$: 1.2.2 |
| 1.2.4 | $b > \sqrt{n}$ | Elim $\land$: 1.2.2 |
| 1.2.5 | $ab > \sqrt{n}\sqrt{n} = n$ | Prop of ">": 1.2.3, 1.2.4 Algebra |
| 1.2.6 | $(ab = n) \land (ab > n)$ | Intro $\land$: 1.1, 1.2.5 |
| 1.2.7 | F | Prop of ">", 1.2.6 |
| 1.2. | $\neg(a \leq \sqrt{n} \lor b \leq \sqrt{n}) \to \mathsf{F}$ | Direct Proof |
| 1.3. | $\neg\neg(a \leq \sqrt{n} \lor b \leq \sqrt{n}) \lor \mathsf{F}$ | Law of Implication: 1.2 |
| 1.4. | $\neg\neg(a \leq \sqrt{n} \lor b \leq \sqrt{n})$ | Identity: 1.3 |
| 1.5. | $a \leq \sqrt{n} \lor b \leq \sqrt{n}$ | Double Negation: 1.4 |
| 1. | $(n = ab) \to (a \leq \sqrt{n} \lor b \leq \sqrt{n})$ | Direct Proof |

Translate this formal proof to an English proof. (Hint: notice which of the proof strategies is being used in part of this proof. Our proof strategies each have special, often shorter, English translations.)

### Solution:

Suppose that $n = ab$. Suppose for contradiction that $a, b > \sqrt{n}$. It follows that $ab > \sqrt{n}\sqrt{n} = n$. We cannot have both $a = n$ and $ab > n$, so this is a contradiction. It follows that $a$ or $b$ is at most $\sqrt{n}$.

## 3. How Many Elements?

For each of these, how many elements are in the set? If the set has infinitely many elements, say so.

(a) $A = \{1, 2, 3, 2\}$

### Solution:

$3$

(b) $B = \{\{\},\ \{\{\}\},\ \{\{\},\{\}\},\ \{\{\},\{\},\{\}\},\ \ldots\}$

### Solution:

$$\begin{aligned} B &= \{\{\},\ \{\{\}\},\ \{\{\},\{\}\},\ \{\{\},\{\},\{\}\},\ \ldots\} \\ &= \{\{\},\ \{\{\}\},\ \{\{\}\},\ \{\{\}\},\ \ldots\} \\ &= \{\varnothing, \{\varnothing\}\} \end{aligned}$$

So, there are two elements in $B$.

(c) $C = A \times (B \cup \{7\})$

**Solution:**

$C = \{1, 2, 3\} \times \{\varnothing, \{\varnothing\}, 7\} = \{(a, b) \mid a \in \{1, 2, 3\}, b \in \{\varnothing, \{\varnothing\}, 7\}\}$. It follows that there are $3 \times 3 = 9$ elements in $C$.

(d) $D = \varnothing$

**Solution:**

0.

(e) $E = \{\varnothing\}$

**Solution:**

1.

(f) $F = \mathcal{P}(\{\varnothing\})$

**Solution:**

$2^1 = 2$. The elements are $F = \{\varnothing, \{\varnothing\}\}$.

## 4. Game, Set, Match

Let $A$, $B$, and $C$ be arbitrary sets. Consider the claim that $A \setminus B \subseteq A \cup C$.

(a) Write a formal proof of the claim.

**Solution:**

| | | |
|---|---|---|
| 1. | Let $x$ be an arbitrary object. | |
| 2.1. | $x \in A \setminus B$ | Assumption |
| 2.2. | $(x \in A) \land \neg(x \in B)$ | Defn of "$\setminus$": 2.1 |
| 2.3. | $x \in A$ | Elim $\land$: 2.2 |
| 2.4. | $(x \in A) \lor (x \in C)$ | Intro $\lor$: 2.3 |
| 2.5. | $x \in A \cup C$ | Defn of $\cup$: 2.4 |
| 2. | $(x \in A \setminus B) \to (x \in A \cup C)$ | Direct Proof |
| 3. | $\forall x\, ((x \in A \setminus B) \to (x \in A \cup C))$ | Intro $\forall$: 1, 2 |
| 4. | $A \setminus B \subseteq A \cup C$ | Defn of $\subseteq$: 3 |

(b) Translate your formal proof to an English proof.

**Solution:**

Let $x$ be an arbitrary object. Suppose that $x \in A \setminus B$. By definition, this means that $x \in A$ and $x \notin B$. Since $x \in A$, we have $x \in A \cup C$ by the definition of $\cup$. Since $x$ was arbitrary, this shows $A \setminus B \subseteq A \cup C$.

## 5. Bump, Set, Spike

Prove each of the following set identities. For each, give an English proof, but feel free to use a chain of equivalences as part of that proof (as in the "meta-theorem" from lecture), and let $\mathcal{U}$ denote the universe.

(a) For any sets $A, B$, we have $A \cap \overline{B} = A \setminus B$ .

**Solution:**

Let $A$ and $B$ be arbitrary sets. Let $x$ be an arbitrary object. Then, we can see that

$$\begin{aligned} x \in A \cap \overline{B} &\equiv x \in A \wedge x \in \overline{B} && \text{Defn of } \cap \\ &\equiv x \in A \wedge x \notin B && \text{Defn of } \bar{\cdot} \\ &\equiv x \in A \setminus B && \text{Defn of ``}\setminus\text{''} \end{aligned}$$

Thus, we have $x \in A \cap \overline{B} \leftrightarrow x \in A \setminus B$. Since $x$ was arbitrary, this shows that $A \cap \overline{B} = A \setminus B$. Since $A$ and $B$ were arbitrary, the claim follows.

(b) For any set $A$, we have $\overline{\overline{A}} = A$.

**Solution:**

Let $A$ be an arbitrary set. Let $x$ be an arbitrary object. Then, we can see that

$$\begin{aligned} x \in \overline{\overline{A}} &\equiv \neg(x \in \overline{A}) && \text{Defn of } \bar{\cdot} \\ &\equiv \neg(\neg(x \in A)) && \text{Defn of } \bar{\cdot} \\ &\equiv x \in A && \text{Double Negation} \end{aligned}$$

Thus, we have $x \in \overline{\overline{A}} \leftrightarrow x \in A$. Since $x$ was arbitrary, this shows that $\overline{\overline{A}} = A$. Since $A$ was arbitrary, the claim follows.

(c) For any sets $A$ and $B$, we have $(A \oplus B) \oplus B = A$.

**Solution:**

Let $A$ and $B$ be arbitrary sets. Let $x$ be an arbitrary object. Then, we can see that

$$\begin{aligned} &x \in (A \oplus B) \oplus B \\ &\quad\equiv (x \in A \oplus B) \oplus (x \in B) && \text{Defn of } \oplus \text{ (sets)} \\ &\quad\equiv ((x \in A) \oplus (x \in B)) \oplus (x \in B) && \text{Defn of } \oplus \text{ (sets)} \\ &\quad\equiv (x \in A) \oplus ((x \in B) \oplus (x \in B)) && \text{Associativity} \\ &\quad\equiv (x \in A) \oplus (((x \in B) \wedge \neg(x \in B)) \vee (\neg(x \in B) \wedge (x \in B))) && \text{Defn of } \oplus \text{ (logic)} \\ &\quad\equiv (x \in A) \oplus (\mathsf{F} \vee (\neg(x \in B) \wedge (x \in B))) && \text{Negation} \\ &\quad\equiv (x \in A) \oplus (\mathsf{F} \vee \mathsf{F}) && \text{Negation} \\ &\quad\equiv (x \in A) \oplus \mathsf{F} && \text{Idempotence} \\ &\quad\equiv ((x \in A) \wedge \neg\mathsf{F}) \vee (\neg(x \in A) \wedge \mathsf{F}) && \text{Defn of } \oplus \text{ (logic)} \\ &\quad\equiv ((x \in A) \wedge \neg\mathsf{F}) \vee \mathsf{F} && \text{Domination} \\ &\quad\equiv (x \in A) \wedge \neg\mathsf{F} && \text{Identity} \\ &\quad\equiv (x \in A) \wedge \mathsf{T} && \text{Defn of } \neg \\ &\quad\equiv x \in A && \text{Identity} \end{aligned}$$

Thus, we have $x \in (A \oplus B) \oplus B \leftrightarrow x \in A$. Since $x$ was arbitrary, this shows that $(A \oplus B) \oplus B = A$. Since $A$ and $B$ were arbitrary, the claim follows.