CSE 311: Foundations of Computing I

Section 4: English Proofs and Sets

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$(y) \land (y > x)$	Intro $\land$: 2.6, 2.9
2.11.	$\exists z\,(\text{Odd}(z) \land (z > x))$	Intro $\exists$: 2.10
2.	Even$(x) \to \exists z\,(\text{Odd}(z) \land (z > x))$	Direct Proof
3.	$\forall x\,(\text{Even}(x) \to \exists z\,(\text{Odd}(z) \land (z > x)))$	Intro $\forall$: 1, 2

Translate this formal proof to an English proof.

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	$\neg(a \le \sqrt{n} \lor b \le \sqrt{n})$	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.	$\neg(a \le \sqrt{n} \lor b \le \sqrt{n}) \to$ F	Direct Proof
1.3.	$\neg\neg(a \le \sqrt{n} \lor b \le \sqrt{n}) \lor$ F	Law of Implication: 1.2
1.4.	$\neg\neg(a \le \sqrt{n} \lor b \le \sqrt{n})$	Identity: 1.3
1.5.	$a \le \sqrt{n} \lor b \le \sqrt{n}$	Double Negation: 1.4
1.	$(n = ab) \to (a \le \sqrt{n} \lor b \le \sqrt{n})$	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.)

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

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

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

(d) $D = \varnothing$

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

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

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.

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

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 $A \cap \overline{B} = A \setminus B$.

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

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