Prose Proofs about Sets

Many observations about sets, their properties, and the relationships among them, can be stated and proven systematically. Some are obvious, and some are subtle. As a way of getting used to the style of mathematical proofs, we’ll state a few of them in English prose and give them prose proofs rather than deriving them as theorems in an axiomatic system.

Theorem 1: Any set \( S \) is a subset of its union with any set \( T \). (In other words: \( (S \subseteq (S \cup T)) \), regardless of what sets \( S \) and \( T \) are).

Proof: Recall that one set is a subset of another if each element of the former is also an element of the latter. Let \( x \) be any element of \( S \). From the premiss that \( x \in S \), we can infer that \( x \in S \) or \( x \in T \) (possibly both). Hence, by the definition of union, \( x \in (S \cup T) \).

Thus every element of \( S \) is an element of \( S \cup T \). Hence \( (S \subseteq S \cup T) \).

This proof demonstrates the use of the rule of universal quantifier introduction in a prose setting: The lemma is the part of the proof that begins with “Let \( x \ldots \)” and runs to the end of the paragraph. The second paragraph of the proof uses this lemma to justify the universally quantified statement.

You’ll also notice that the prose proof skips several steps that a formal proof would make explicit, because they are obvious from the context (universal quantifier eliminations to put the terms ‘\( S \)’ and ‘\( T \)’ into the body of the definition of union, for instance) or because they are built into the prose structure (the use of implication introduction in the transition from the first paragraph to the second, for instance). Similarly, the last paragraph uses the definition of subset without even mentioning it explicitly.

Writing out the formal proof in an axiom system is a useful check in case anyone suspects that a fallacy has been committed, which unfortunately is not uncommon. Another advantage is that the construction of formal proofs can be automated, at least in part, with tools called “proof assistants” (such as Coq, which is free software and is available on MathLAN, along with its own graphical user interface, as /usr/bin/coqide). Proof assistants check the formal derivations as they are constructed to ensure that every step is justified by one of the available axioms or rules of inference.

Theorem 2: For any sets \( S \) and \( T \), \( ((S \cup T) = (T \cup S)) \) (union is commutative).

Proof: Recall that we regard two sets as equal if they have the same elements. Let \( x \) be any element of \( (S \cup T) \). By the definition of union, \( (x \in S) \) or \( (x \in T) \). We consider the two cases separately:

Case 0: \( (x \in S) \). In this case, we can conclude by disjunction introduction that \( (x \in T) \) or \( (x \in S) \).

Case 1: \( (x \in T) \). We can again conclude by disjunction introduction that \( (x \in T) \) or \( (x \in S) \).

Thus in either case, \( (x \in T) \) or \( (x \in S) \). Hence, by the definition of union, \( (x \in (T \cup S)) \).

Thus every element of \( S \cup T \) is an element of \( (T \cup S) \). By precisely similar reasoning, every element of \( (T \cup S) \) is an element of \( (S \cup T) \). Hence \( ((S \cup T) = (T \cup S)) \).

In this proof, you’ll recognize the structure of the rule of disjunctive syllogism (sometimes called “case analysis”). The cases are the separate disjuncts of the disjunction obtained at the end
of the first paragraph. Since the case-lemmas reach the same conclusion, that conclusion is validly derived from the disjunction.

The other design pattern that is used here (introduced by the words “By precisely similar reasoning”) is the appeal to symmetry. Mathematicians use this pattern when it would be tedious and uninstructional to write out a part of the proof that has the same form as a part already presented. In this case, to prove that every element of \((T \cup S)\) is an element of \((S \cup T)\), one would go through the line of reasoning already presented, replacing each occurrence of ‘\(S\)’ with ‘\(T\)’ and each occurrence of ‘\(T\)’ with ‘\(S\)’. It’s obvious, though, that the way the sets are named does not affect the validity of the inference, so it’s not really necessary to write out the result of such a replacement.

One can use an appeal to symmetry whenever one is proving the equality of two sets that are constructed on the same pattern, differing only in the placement of corresponding identifiers. (In the list of laws of sets in the last section of this handout, the commutativity of intersection, the law \(((S - T) - U) = ((S - U) - T))\), and the symmetry of disjointness would all have proofs in which an appeal to symmetry would be appropriate.)

**Theorem 3:** For any sets \(S, T\), and \(U\), if \((S \subseteq T)\) and \((T \subseteq U)\), then \((S \subseteq U)\). (The subset relation is transitive.)

**Proof:** Suppose that \((S \subseteq T)\) and \((T \subseteq U)\), and let \(x\) be any element of \(S\). Since \(S\) is a subset of \(T\), every element of \(S\) is an element of \(T\), and so in particular \((x \in T)\). Since \(T\) is a subset of \(U\), every element of \(T\) is an element of \(U\), and so in particular \((x \in U)\).

Thus every element of \(S\) is an element of \(U\). By the definition of subset, this means that \(S \subseteq U\).

Therefore, if \((S \subseteq T)\) and \((T \subseteq U)\), then \((S \subseteq U)\). \(\blacksquare\)

**Theorem 4:** \(((\emptyset - S) = \emptyset)\). (The empty set is a left zero for the set-difference operation.)

**Proof:** Two sets are equal if they have the same elements. But, by definition, \(\emptyset\) has no elements. So we must show that \((\emptyset - S)\) has no elements either.

Suppose that \((\emptyset - S)\) could have an element, and let \(x\) be any element of \((\emptyset - S)\). By the definition of set difference, \((x \in (\emptyset - S))\) if, and only if, \(((x \in \emptyset) \land (x \notin S))\). Then by conjunction elimination, \((x \in \emptyset)\). But this is impossible, since \(\emptyset\) has no elements.

Hence, by *reductio ad absurdum*, \((\emptyset - S)\) has no elements. Thus \(((\emptyset - S) = \emptyset)\). \(\blacksquare\)

The use of the axiom of set equality is implicit in the structure of this proof: To show that two sets are equal, we prove that they have the same elements — in this case, no elements at all.

**Constructing the Notation and Axioms**

To work with sets formally, in an axiomatic system based on the predicate calculus and the theory of identity, we can adopt a technical vocabulary that includes the binary predicates *Element-of*, *Subset-of*, and *Strict-subset-of*, binary functions *union*, *intersection*, and *difference*, unary function \(\varphi\) (for “power set”), and a term \(\emptyset\). We’ll also subsume the theory of identity into our set theory, with its binary predicate \(\equiv\) and its axioms and rules of inference, including the axioms and rules of inference of the predicate calculus.

As is customary, and to bring our notation in line with the textbook, we’ll write \(\tau(\sigma \in \tau)\) for \(\tau{\text{-Element-of}}(\sigma, \tau)\) (for any terms \(\tau{\text{-Element-of}}\) and \(\tau\)), and similarly \(\tau(\sigma \subseteq \tau)\) for \(\tau{\text{-Subset-of}}(\sigma, \tau)\) and \(\tau(\sigma \subset \tau)\) for \(\tau{\text{-Strict-subset-of}}(\sigma, \tau)\). Likewise for the binary functions: \(\tau(\sigma \cup \tau)\) is a shorthand form for \(\tau{\text{-union}}(\sigma, \tau)\), \(\tau(\sigma \cap \tau)\) for \(\tau{\text{-intersection}}(\sigma, \tau)\), and \(\tau(\sigma - \tau)\) for \(\tau{\text{-difference}}(\sigma, \tau)\).

Next, we need axioms and inference rules that define all of these new symbols. All but one of these are really just formalizations of the informal definitions from section 4.1 of the textbook.
Naive Set Theory — page 3

- $\vdash ((\sigma \subseteq \tau) \iff \forall \xi (\xi \in \sigma \to \xi \in \tau))$ (definition of subset).
- $\vdash ((\sigma \subset \tau) \iff ((\sigma \subseteq \tau) \land \neg(\sigma = \tau)))$ (definition of strict subset).
- $\vdash \forall \xi ((\xi \in (\sigma \cup \tau)) \iff ((\xi \in \sigma) \lor (\xi \in \tau)))$ (definition of union).
- $\vdash \forall \xi ((\xi \in (\sigma \cap \tau)) \iff ((\xi \in \sigma) \land (\xi \in \tau)))$ (definition of intersection).
- $\vdash \forall \xi ((\xi \in (\sigma - \tau)) \iff ((\xi \in \sigma) \land \neg(\xi \in \tau)))$ (definition of set difference).
- $\vdash \forall \xi ((\xi \in \varnothing(\sigma)) \iff (\xi \subseteq \sigma))$ (definition of power set).
- $\vdash \forall \xi \neg(\xi \in \varnothing)$ (definition of empty set).
- $\vdash ((\sigma = \tau) \iff \forall \xi ((\xi \in \sigma) \iff (\xi \in \tau)))$ (axiom of set equality).

The last of these axioms is an observation, intended to be obviously and incontestably true, about what constitutes the identity of a set, namely, its membership. If $\sigma$ and $\tau$ have exactly the same elements, then $\sigma$ is $\tau$.

The axiom of set equality in this form means that the theory will only be true when the universe of discourse consists entirely of sets. For if there were any non-set entities in the universe of discourse, they would presumably have no elements. Under the axiom of set equality, then, they would all be identical to $\varnothing$ and so would be sets after all.

There is a kind of workaround for this, suggested by the logician Willard van Orman Quine in his book Set Theory and Its Logic, where he calls non-set entities “individuals.” For any individual $x$, we can adopt the convention that $(x = \{x\})$: An individual is the set that has that very individual as its only element. It turns out that this convention is consistent with the other axioms so long as we don’t mistakenly try to apply it to ordinary sets such as $\varnothing$, which cannot be individuals in Quine’s sense. (The empty set, by definition, has no elements at all; it is a subset of itself, but not an element of itself.)

**Proofs in Axiomatic Set Theory**

Full formal proofs in this system are straightforward applications of the methods that we have developed for the propositional and predicate calculi. Here are a few examples, including two of the laws proven above and one for which a prose proof was given in the textbook.

**Theorem 1** (again): To prove: $\vdash \forall x \forall y (x \subseteq (x \cup y))$.

Lemma A: $(c \in a) \vdash (c \in (a \cup b))$.

1. $(c \in a) \lor (c \in b)$ (0), disjunction introduction
2. $\forall x ((x \in (a \cup b)) \iff ((x \in a) \lor (x \in b)))$ (1), (2), equivalence elimination (right-to-left)
3. $(c \in (a \cup b))$ (0), (1), equivalence elimination (right-to-left)

Lemma B: $\vdash ((c \in a) \to (c \in (a \cup b)))$.

1. $(c \in a) \to (c \in (a \cup b))$ lemma A, implication introduction

Lemma C: $\vdash (a \subseteq (a \cup b))$.

1. $\forall x ((x \in a) \to (x \in (a \cup b)))$ lemma B, universal quantifier introduction
2. $(a \subseteq (a \cup b))$ definition of subset

Lemma D: $\vdash \forall y (a \subseteq (a \cup y))$.

1. $\forall y (a \subseteq (a \cup y))$ lemma C, universal quantifier introduction
Main proof of proposition:

\[(0) \quad \forall x \forall y (x \subseteq (x \cup y)) \quad \text{lemma D, universal quantifier introduction}\]

**Theorem 4 (again).** To prove: \(\vdash \forall x ((\emptyset - x) = \emptyset)\).

**Lemma A:** \(b \in (\emptyset - a) \vdash b \in \emptyset\).

\[(0) \quad (b \in (\emptyset - a)) \quad \text{premiss}\]
\[(1) \quad (b \in (\emptyset - a)) \iff ((b \in \emptyset) \land \neg (b \in a)) \quad \text{definition of set difference}\]
\[(2) \quad ((b \in (\emptyset - a)) \iff ((b \in \emptyset) \land \neg b \in a)) \quad (1), \text{universal quantifier elimination}\]
\[(3) \quad ((b \in \emptyset) \land \neg b \in a) \quad (0), (2), \text{modus ponens}\]
\[(4) \quad (b \in \emptyset) \quad (3), \text{conjunction elimination, left}\]

**Lemma B:** \(b \in \emptyset, \neg(b \in (\emptyset - a)) \vdash F\).

\[(0) \quad (b \in \emptyset) \quad \text{premiss}\]
\[(1) \quad \neg (b \in (\emptyset - a)) \quad \text{premiss}\]
\[(2) \quad \forall x \neg (x \in \emptyset) \quad \text{definition of empty set}\]
\[(3) \quad \neg (b \in \emptyset) \quad (2), \text{universal quantifier elimination}\]
\[(4) \quad F \quad (0), (3), \text{catastrophe of contradiction}\]

**Lemma C:** \((b \in \emptyset) \vdash (b \in (\emptyset - a))\).

\[(0) \quad (b \in \emptyset) \quad \text{premiss}\]
\[(1) \quad \neg \neg (b \in (\emptyset - a)) \quad (0), \text{lemma B, reductio ad absurdum}\]
\[(2) \quad (b \in (\emptyset - a)) \quad (1), \text{negation elimination}\]

**Lemma D:** \(\vdash ((b \in (\emptyset - a)) \iff (b \in \emptyset))\).

\[(0) \quad ((b \in (\emptyset - a)) \iff (b \in \emptyset)) \quad \text{lemmas A and C, equivalence introduction}\]

**Lemma E:** \(\vdash ((\emptyset - a) = \emptyset)\).

\[(0) \quad ((\emptyset - a) = \emptyset) \quad \text{lemma D, universal quantifier introduction}\]
\[(1) \quad (((\emptyset - a) = \emptyset) \iff \forall x ((x \in (\emptyset - a) \iff (x \in \emptyset))) \quad \text{axiom of set equality}\]
\[(2) \quad ((\emptyset - a) = \emptyset) \quad (0), (1), \text{equivalence elimination (right-to-left)}\]

Main proof of the proposition:

\[(0) \quad \forall x ((\emptyset - x) = \emptyset) \quad \text{lemma E, universal quantifier introduction}\]

**Theorem 5:** To prove: \(\vdash \forall x \forall y \forall z ((x \cap (y \cup z)) = ((x \cap y) \cup (x \cap z)))\).

This is a distributive law for sets: Union distributes over intersection. In the textbook, it is proven as Theorem 4.1.2.

**Lemma A:** \((d \in a), (d \in b) \vdash ((d \in (a \cap b)) \vee (d \in (a \cap c)))\).

\[(0) \quad (d \in a) \quad \text{premiss}\]
\[(1) \quad (d \in b) \quad \text{premiss}\]
\[(2) \quad ((d \in a) \land (d \in b)) \quad (0), (1), \text{conjunction introduction}\]
\[(3) \quad \forall x ((x \in (a \cap b)) \iff ((x \in a) \land (x \in b))) \quad \text{definition of intersection}\]
\[(4) \quad ((d \in (a \cap b)) \iff ((d \in a) \land (d \in b))) \quad (3), \text{universal quantifier elimination}\]
\[(5) \quad (d \in (a \cap b)) \quad (2), (4), \text{equivalence elimination (right-to-left)}\]
\[(6) \quad ((d \in (a \cap b)) \vee (d \in (a \cap c))) \quad (5), \text{disjunction introduction, left}\]
Lemma B: \( (d \in a) \land (d \in c) \vdash ((d \in (a \cap b)) \lor (d \in (a \cap c))). \)

\begin{align*}
(0) & \quad (d \in a) \quad \text{premiss} \\
(1) & \quad (d \in c) \quad \text{premiss} \\
(2) & \quad ((d \in a) \land (d \in c)) \quad (0), (1), \text{conjunction introduction} \\
(3) & \quad \forall x ((x \in (a \cap c)) \leftrightarrow ((x \in a) \land (x \in c))) \quad \text{definition of intersection} \\
(4) & \quad ((d \in (a \cap c)) \leftrightarrow ((d \in a) \land (d \in c))) \quad (3), \text{universal quantifier elimination} \\
(5) & \quad (d \in (a \cap c)) \quad (2), (4), \text{equivalence elimination (right-to-left)} \\
(6) & \quad ((d \in (a \cap b)) \lor (d \in (a \cap c))) \quad (5), \text{disjunction introduction, right}
\end{align*}

Lemma C: \( (d \in (a \cap (b \cup c))) \vdash (d \in ((a \cap b) \cup (a \cap c))). \)

\begin{align*}
(0) & \quad (d \in (a \cap (b \cup c))) \quad \text{premiss} \\
(1) & \quad \forall x ((x \in (a \cap (b \cup c))) \leftrightarrow ((x \in a) \land (x \in (b \cup c)))) \quad \text{definition of intersection} \\
(2) & \quad ((d \in (a \cap (b \cup c))) \leftrightarrow ((d \in a) \land (d \in (b \cup c)))) \quad (1), \text{universal quantifier elimination} \\
(3) & \quad ((d \in a) \land (d \in (b \cup c))) \quad (0), (2), \text{equivalence elimination (left-to-right)} \\
(4) & \quad (d \in a) \quad (3), \text{conjunction elimination (left)} \\
(5) & \quad (d \in (b \cup c)) \quad (3) \text{ conjunction elimination (right)} \\
(6) & \quad \forall x ((x \in (b \cup c)) \leftrightarrow ((x \in b) \lor (x \in c))) \quad \text{definition of union} \\
(7) & \quad ((d \in (b \cup c)) \leftrightarrow ((d \in b) \lor (d \in c))) \quad (6), \text{universal quantifier elimination} \\
(8) & \quad ((d \in b) \lor (d \in c)) \quad (5), (7), \text{equivalence elimination (left-to-right)} \\
(9) & \quad (d \in (a \cap b)) \lor (d \in (a \cap c)) \quad (4), (8), \text{lemmas A and B, disjunctive syllogism} \\
(10) & \quad \forall x ((x \in ((a \cap b) \cup (a \cap c))) \leftrightarrow ((x \in (a \cap b)) \lor (x \in (a \cap c)))) \quad \text{definition of union} \\
(11) & \quad ((d \in ((a \cap b) \cup (a \cap c))) \leftrightarrow ((d \in (a \cap b)) \lor (d \in (a \cap c)))) \quad (10), \text{universal quantification elimination} \\
(12) & \quad ((d \in ((a \cap b) \cup (a \cap c)))) \quad (9), (11), \text{equivalence elimination (right-to-left)}
\end{align*}

Lemma D: \( (d \in (a \cap b)) \vdash ((d \in a) \land (d \in (b \cup c))). \)

\begin{align*}
(0) & \quad (d \in (a \cap b)) \quad \text{premiss} \\
(1) & \quad \forall x ((x \in (a \cap b)) \leftrightarrow ((x \in a) \land (x \in b))) \quad \text{definition of intersection} \\
(2) & \quad ((d \in (a \cap b)) \leftrightarrow ((d \in a) \land (d \in b))) \quad (1), \text{universal quantifier elimination} \\
(3) & \quad ((d \in a) \land (d \in b)) \quad (0), (2), \text{equivalence elimination (left-to-right)} \\
(4) & \quad (d \in a) \quad (3), \text{conjunction elimination (left)} \\
(5) & \quad (d \in b) \quad (3), \text{conjunction elimination (right)} \\
(6) & \quad ((d \in b) \lor (d \in c)) \quad (5), \text{disjunction introduction, left} \\
(7) & \quad \forall x ((x \in (b \cup c)) \leftrightarrow ((x \in b) \lor (x \in c))) \quad \text{definition of union} \\
(8) & \quad ((d \in (b \cup c)) \leftrightarrow ((d \in b) \lor (d \in c))) \quad (7), \text{universal quantifier elimination} \\
(9) & \quad (d \in (b \cup c)) \quad (6), (8), \text{equivalence elimination (right-to-left)}
\end{align*}
Lemma E: \((d \in (a \cap c)) \vdash ((d \in a) \land (d \in (b \cup c)))\).

(0) \((d \in (a \cap c))\) 
(1) \(\forall x \ ((x \in (a \cap c)) \leftrightarrow ((x \in a) \land (x \in c)))\) 
(2) \(((d \in (a \cap c)) \leftrightarrow ((d \in a) \land (d \in c)))\) 
(3) \(((d \in a) \land (d \in c))\) 
(4) \((d \in a)\) 
(5) \((d \in c)\) 
(6) \(((d \in b) \lor (d \in c))\) 
(7) \(\forall x \ ((x \in (b \cup c)) \leftrightarrow ((x \in b) \lor (x \in c)))\) 
(8) \(((d \in (b \cup c)) \leftrightarrow ((d \in b) \lor (d \in c)))\) 
(9) \((d \in (b \cup c))\) 

Lemma F: \((d \in ((a \cap b) \cup (a \cap c))) \vdash (d \in (a \cap (b \cup c)))\).

(0) \((d \in ((a \cap b) \cup (a \cap c)))\) 
(1) \(\forall x \ ((x \in ((a \cap b) \cup (a \cap c))) \leftrightarrow ((x \in (a \cap b)) \lor (x \in (a \cap c))))\) 
(2) \(((d \in ((a \cap b) \cup (a \cap c))) \leftrightarrow ((d \in (a \cap b)) \lor (d \in (a \cap c)))\) 
(3) \(((d \in (a \cap b)) \lor (d \in (a \cap c)))\) 
(4) \((d \in a) \land (d \in (b \cup c))\) 
(5) \(\forall x \ ((x \in (a \cap (b \cup c))) \leftrightarrow ((x \in a) \land (x \in (b \cup c))))\) 
(6) \(((d \in (a \cap (b \cup c))) \leftrightarrow ((d \in a) \land (d \in (b \cup c)))\) 
(7) \((d \in (a \cap (b \cup c)))\) 

Lemma G: \(\vdash ((d \in (a \cap (b \cup c))) \leftrightarrow (d \in ((a \cap b) \cup (a \cap c))))\).

(0) \(((d \in (a \cap (b \cup c))) \leftrightarrow (d \in ((a \cap b) \cup (a \cap c)))\) 

Lemma H: \(\vdash ((a \cap (b \cup c)) = ((a \cap b) \cup (a \cap c)))\).

(0) \(\forall x \ ((x \in (a \cap (b \cup c))) \leftrightarrow (x \in ((a \cap b) \cup (a \cap c))))\) 

Lemma I: \(\vdash \forall z \ ((a \cap (b \cup z)) = (a \cap (b \cup (a \cap z))))\).

(0) \(\forall z \ ((a \cap (b \cup z)) = (a \cap (b \cup (a \cap z))))\) 

Lemma J: \(\vdash \forall y \forall z \ ((a \cap (y \cup z)) = ((a \cap y) \cup (a \cap z)))\).

(0) \(\forall y \forall z \ ((a \cap (y \cup z)) = ((a \cap y) \cup (a \cap z)))\) 

Main proof of proposition:

(0) \(\forall x \forall y \forall z \ ((x \cap (y \cup z)) = ((x \cap y) \cup (x \cap z)))\)
Here are some other laws of sets that can be proven by similarly elementary forms of reasoning.

- \((S \cup (T \cup U)) = ((S \cup T) \cup U)\): associativity of union
- \((S \cup S) = S\): idempotence of union
- \((S \cup \emptyset) = S\): identity of union
- \((S \cap T) = (T \cap S)\): commutativity of intersection
- \(((S \cap T) \cap U) = ((S \cap U) \cap T)\): associativity of intersection
- \((S \cap S) = S\): idempotence of intersection
- \((S \cap \emptyset) = \emptyset\): zero of intersection
- \(((S \cap (T \cup U)) = ((S \cap T) \cup (S \cap U)))\): distributivity of intersection over union
- \(((S \cup (S \cap T)) = S)\): union absorption in intersection
- \(((S \cap (S \cap T)) = S)\): intersection absorption in union
- \(((S - S) = \emptyset)\)
- \(((S - T) \cup (S \cap T)) = S)\)
- \(((S - T) \cap (S \cap T)) = \emptyset)\)
- \(((S - \emptyset) = S)\): right identity of set difference
- \(((S - T) - U) = ((S - U) - T)\)
- \(((S \cap (T - S)) = \emptyset)\)
- \(((S \cup (T - S)) = (S \cup T))\)
- \(((S - (T \cup U)) = ((S - T) \cap (S - U))\)
- \(((S - (T \cap U)) = ((S - T) \cup (S - U))\)
- \((S \subseteq S)\): reflexivity of subset
- \(((S \subseteq T) \land (T \subseteq S)) \rightarrow (S = T))\): antisymmetry of subset
- \((\emptyset \subseteq S)\)
- \(((S \cap T) \subseteq S)\)
- \(((S - T) \subseteq S)\)

I am indebted to Nediyana Daskalova 2014 for calling my attention to a typographical error in an earlier version of this document.