Proof Outlines

LINE NUMBERS: Only lines that are referred to have labels (for example, L1) in this document. For a formal proof, all lines are numbered. Line numbers appear at the beginning of a line. You can indent line numbers together with the lines they are numbering or all line numbers can be unindented, provided you are consistent.

INDENTATION: Indent when you make an assumption or define a variable. Unindent when this assumption or variable is no longer being used.

1. **Implication**: Direct proof of A IMPLIES B.

   > L1. Assume A.
   >
   > ⋮
   >
   > L2. B

   A IMPLIES B; direct proof: L1, L2

2. **Implication**: Indirect proof of A IMPLIES B.

   > L1. Assume $NOT(B)$.
   >
   > ⋮
   >
   > L2. $NOT(A)$

   A IMPLIES B; indirect proof: L1, L2

3. **Equivalence**: Proof of A IFF B.

   > L1. Assume A.
   >
   > ⋮
   >
   > L2. B

   L3. A IMPLIES B; direct proof: L1, L2

   > L4. Assume B.
   >
   > ⋮
   >
   > L5. A

   L6. B IMPLIES A; direct proof: L4, L5

   A IFF B; equivalence: L3, L6

4. **Proof by contradiction** of A.

   > L1. To obtain a contradiction, assume $NOT(A)$.
   >
   > ⋮
   >
   > > L2. B
   >
   > ⋮
   >
   > > L3. $NOT(B)$
   >
   > L4. This is a contradiction: L2, L3

   Therefore A; proof by contradiction: L1, L4

5. **Modus Ponens**.

   ⋮
   L1. A
   ⋮
   L2. A IMPLIES B
   B; modus ponens: L1, L2

6. **Conjunction:** Proof of A AND B:

   ⋮
   L1. A
   ⋮
   L2. B
   A AND B; proof of conjunction; L1, 2

7. **Use of Conjunction**:

   ⋮
   L1. A AND B
   A; use of conjunction: L1
   B; use of conjunction: L1

8. **Implication with Conjunction**: Proof of (A_1 AND A_2) IMPLIES B.

   L1. Assume A_1 AND A_2.
   A_1; use of conjunction; L1
   A_2; use of conjunction; L1
   ⋮
   L2. B
   (A_1 AND A_2) IMPLIES B; direct proof, L1, L2

9. **Implication with Conjunction**: Proof of A IMPLIES (B_1 AND B_2).

   L1. Assume A.
   ⋮
   L2. B_1
   ⋮
   L3. B_2
   L4. B_1 AND B_2; proof of conjunction: L2, L3
   A IMPLIES (B_1 AND B_2); direct proof: L1, L4

10. **Disjunction**: Proof of A OR B and B OR A.

   ⋮
   L1. A
   A OR B; proof of disjunction: L1
   B OR A; proof of disjunction: L1

11. **Proof by cases**.

L1. C OR $NOT(C)$ tautology
L2. Case 1: Assume C.

$\vdots$

L3. A
L4. C IMPLIES A; direct proof: L2, L3
L5. Case 2: Assume $NOT(C)$.

$\vdots$

L6. A
L7. $NOT(C)$ IMPLIES A; direct proof: L5, L6
A proof by cases: L1, L4, L7

12. **Proof by cases** of A OR B.

L1. C OR $NOT(C)$ tautology
L2. Case 1: Assume C.

$\vdots$

L3. A
L4. A OR B; proof of disjunction, L3
L5. C IMPLIES (A OR B); direct proof, L2, L4
L6. Case 2: Assume $NOT(C)$.

$\vdots$

L7. B
L8. A OR B; proof of disjunction, L7
L9. $NOT(C)$ IMPLIES (A OR B); direct proof: L6, L8
A OR B; proof by cases: L1, L5, L9

13. **Implication with Disjunction**: Proof by cases of (A_1 OR A_2) IMPLIES B.

L1. Case 1: Assume A_1.

$\vdots$

L2. B
L3. A_1 IMPLIES B; direct proof: L1,L2
L4. Case 2: Assume A_2.

$\vdots$

L5. B
L6. A_2 IMPLIES B; direct proof: L4, L5
(A_1 OR A_2) IMPLIES B; proof by cases: L3, L6

14. **Implication with Disjunction**: Proof by cases of A IMPLIES (B_1 OR B_2).

   L1. Assume A.
   L2. C OR NOT(C) tautology
   L3. Case 1: Assume C.
      $\vdots$
      L4. B_1
      L5. B_1 OR B_2; disjunction: L4
   L6. C IMPLIES (B_1 OR B_2); direct proof: L3, L5
   L7. Case 2: AssumeNOT(C).
      $\vdots$
      L8. B_2
      L9. B_1 OR B_2; disjunction: L8
   L10. NOT(C) IMPLIES (B_1 OR B_2); direct proof: L7, L9
   L11. B_1 OR B_2; proof by cases: L2, L6, L10
   A IMPLIES (B_1 OR B_2): direct proof. L1, L11

15. **Substitution of a Variable in a Tautology**:
   Suppose P is a propositional variable, Q is a formula, and R' is obtained from R by replacing *every* occurrence of P by (Q).

   L1. R tautology
   R'; substitution of all P by Q: L1

16. **Substitution of a Formula by a Logically Equivalent Formula**:
   Suppose S is a subformula of R and R' is obtained from R by replacing *some* occurrence of S by S'.

   L1. R
   L2. S IFF S'
   L3. R'; substitution of an occurrence of S by S': L1, L2

17. **Specialization**:

   L1. $c \in D$
   L2. $\forall x \in D.P(x)$
   $P(c)$; specialization: L1, L2

18. **Generalization**: Proof of $\forall x \in D.P(x)$.

   L1. Let x be an arbitrary element of D.
   $\vdots$
   L2. $P(x)$
   Since x is an arbitrary element of D,
   $\forall x \in D.P(x)$; generalization: L1, L2

19. **Universal Quantification with Implication**: Proof of $\forall x \in D.(P(x) \text{ IMPLIES } Q(x))$.

    L1. Let x be an arbitrary element of D.
    L2. Assume $P(x)$
    $\vdots$
    L3. $Q(x)$
    L4. $P(x)$ IMPLIES $Q(x)$; direct proof: L2, L3
    Since x is an arbitrary element of D,
    $\forall x \in D.(P(x) \text{ IMPLIES } Q(x))$; generalization: L1, L4

20. **Implication with Universal Quantification**: Proof of $(\forall x \in D.P(x))$ IMPLIES A.

    L1. Assume $\forall x \in D.P(x)$.
    $\vdots$
    L2. $a \in D$
    $P(a)$; specialization: L1, L2
    $\vdots$
    L3. A
    Therefore $(\forall x \in D.P(x))$ IMPLIES A; direct proof: L1, L3

21. **Implication with Universal Quantification**: Proof of A IMPLIES $(\forall x \in D.P(x))$.

    L1. Assume A.
    L2. Let x be an arbitrary element of D.
    $\vdots$
    L3. $P(x)$

    Since x is an arbitrary element of D,
    L4. $\forall x \in D.P(x)$; generalization, L2, L3
    A IMPLIES $(\forall x \in D.P(x))$; direct proof: L1, L4

22. **Instantiation**:

    L1. $\exists x \in D.P(x)$
    Let $c \in D$ be such that $P(c)$; instantiation: L1
    $\vdots$

23. **Construction**: Proof of $\exists x \in D.P(x)$.

    L1. Let $a = \cdots$
    $\vdots$
    L2. $a \in D$
    $\vdots$
    L3. $P(a)$
    $\exists x \in D.P(x)$; construction: L1, L2, L3

24. **Existential Quantification with Implication**: Proof of $\exists x \in D.(P(x)$ IMPLIES $Q(x))$.

L1. Let $a = \cdots$
$\vdots$
L2. $a \in D$
  L3. Suppose $P(a)$.
  $\vdots$
  L4. $Q(a)$
L5. $P(a)$ IMPLIES $Q(a)$; direct proof: L3, L4
$\exists x \in D.(P(x)$ IMPLIES $Q(x))$; construction: L1, L2, L5

25. **Implication with Existential Quantification**: Proof of $(\exists x \in D.P(x))$ IMPLIES A.

L1. Assume $\exists x \in D.P(x)$.
  Let $a \in D$ be such that $P(a)$; instantiation: L1
  $\vdots$
  L2. A
$(\exists x \in D.P(x))$ IMPLIES A; direct proof: L1, L2

26. **Implication with Existential Quantification**: Proof of A IMPLIES $(\exists x \in D.P(x))$.

L1. Assume A.
  L2. Let $a = \cdots$
  $\vdots$
  L3. $a \in D$
  $\vdots$
  L4. $P(a)$
L5. $\exists x \in D.P(x)$; construction: L2, L3, L4
A IMPLIES $(\exists x \in D.P(x))$; direct proof: L1, L5

27. **Subset**: Proof of $A \subseteq B$.

L1. Let $x \in A$ be arbitrary.
$\vdots$
L2. $x \in B$
The following line is optional:
L3. $x \in A$ IMPLIES $x \in B$; direct proof: L1, L2
$A \subseteq B$; definition of subset: L3 (or L1, L2, if the optional line is missing)

28. **Weak Induction**: Proof of $\forall n \in N.P(n)$

Base Case:

$\vdots$

L1. $P(0)$

L2. Let $n \in N$ be arbitrary.

L3. Assume $P(n)$.

$\vdots$

L4. $P(n+1)$

The following two lines are optional:

L5. $P(n)$ IMPLIES $(P(n+1)$; direct proof of implication: L3, L4

L6. $\forall n \in N.(P(n)$ IMPLIES $P(n+1))$; generalization L2, L5

$\forall n \in N.P(n)$ induction; L1, L6 (or L1, L2, L3, L4, if the optional lines are missing)

29. **Strong Induction**: Proof of $\forall n \in N.P(n)$

L1. Let $n \in N$ be arbitrary.

L2. Assume $\forall j \in N.(j < n$ IMPLIES $P(j))$

$\vdots$

L3. $P(n)$

The following two lines are optional:

L4. $\forall j \in N.(j < n$ IMPLIES $P(j))$ IMPLIES $P(n)$; direct proof of implication: L2, L3

L5. $\forall n \in N.[\forall j \in N.(j < n$ IMPLIES $P(j))$ IMPLIES $P(n)]$; generalization: L1, L4

$\forall n \in N.P(n)$; strong induction: L5 (or L1, L2, L3, if the optional lines are missing)

30. **Structural Induction**: Proof of $\forall e \in S.P(e)$, where S is a recursively defined set

Base case(s):

L1. For each base case e in the definition of S

L2. $P(e)$.

Constructor case(s):

L3. For each constructor case e of the definition of S,

L4. assume $P(e')$ for all components e' of e.

$\vdots$

L5. $P(e)$

$\forall e \in S.P(e)$; structural induction: L1, L2, L3, L4, L5

31. **Well Ordering Principle**: Proof of $\forall e \in S.P(e)$, where S is a well ordered set, i.e. every nonempty subset of S has a smallest element.

L1. To obtain a contradiction, suppose that $\forall e \in S.P(e)$ is false.
L2. Let $C = \{e \in S \mid P(e) \text{ is false}\}$ be the set of counterexamples to P.
L3. $C \neq \phi$; definition: L1, L2
    L4. Let e be the smallest element of C; well ordering principle: L2, L3
        Let $e' = \cdots$
        $\vdots$
        L5. $e' \in C$
        $\vdots$
        L6. $e' < e$.
L7. This is a contradiction: L4, L5, L6

$\forall e \in S.P(e)$; proof by contradiction: L1, L7