Advanced Proof Patterns

Example 1 : Proof by Cases (Three - Way Split)

Prove: For all integers n, n $\langle 0(or)(n) = 0(or)(n) \rangle$ 0

$$\dfrac{}{n < 0 \vee n = 0 \vee n > 0}\ [\text{trichotomy of integers, axiom}]$$

This uses the trichotomy property as an axiom. To prove something about all integers, we can case-analyze on these three possibilities.

Example 2 : Multi - Level Case Analysis

Prove: $(p \vee q) \wedge (r \vee s) \Rightarrow (p \wedge r) \vee (p \wedge s) \vee (q \wedge r) \vee (q \wedge s)$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{p \wedge r}\ [\wedge\ \text{intro}]}{(p \wedge r) \vee (p \wedge s) \vee (q \wedge r) \vee (q \wedge s)}\ [\vee\ \text{intro}] \qquad \dfrac{\dfrac{}{p \wedge s}\ [\wedge\ \text{intro}]}{(p \wedge r) \vee (p \wedge s) \vee (q \wedge r) \vee (q \wedge s)}\ [\vee\ \text{intro}]}{(p \wedge r) \vee (p \wedge s) \vee (q \wedge r) \vee (q \wedge s)}\ [\vee\ \text{elim on r} \vee \text{s}] \qquad \dfrac{\dfrac{\dfrac{}{q \wedge r}\ [\wedge\ \text{intro}]}{(p \wedge r) \vee (p \wedge s) \vee (q \wedge r) \vee (q \wedge s)}\ [\vee\ \text{intro}] \qquad \dfrac{\dfrac{}{q \wedge s}\ [\wedge\ \text{intro}]}{(p \wedge r) \vee (p \wedge s) \vee (q \wedge r) \vee (q \wedge s)}\ [\vee\ \text{intro}]}{(p \wedge r) \vee (p \wedge s) \vee (q \wedge r) \vee (q \wedge s)}\ [\vee\ \text{elim on r} \vee \text{s}]}{\dfrac{(p \wedge r) \vee (p \wedge s) \vee (q \wedge r) \vee (q \wedge s)}{((p \vee q) \wedge (r \vee s)) \Rightarrow (p \wedge r) \vee (p \wedge s) \vee (q \wedge r) \vee (q \wedge s)}\ [\Rightarrow\text{-intro}^{[1]}]}\ [\vee\ \text{elim on p} \vee \text{q}]$$

Nested case analysis on two disjunctions, exploring all four combinations.

Example 3 : Proof by Mathematical Induction (Base land Step)

Prove: For all n $\in \mathbb{N}$, sum(1 to n) = n(n+1)/2

Base case ($n = 0$):

$$\dfrac{\dfrac{\dfrac{\dfrac{\ulcorner true \urcorner^{[1]}}{sum\_to(0) = 0}\ [\text{definition}]}{0 * ((0+1))(div)(2) = 0}\ [\text{arithmetic}]}{sum\_to(0) = 0 * ((0+1))(div)(2)}\ [\text{equality}]}{true \Rightarrow (sum\_to(0) = 0 * ((0+1))(div)(2))}\ [\Rightarrow\text{-intro}^{[1]}]$$

Inductive step (assume for n, prove for n+1):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\ulcorner sum\_to(n) = n * ((n+1))(div)(2)\urcorner^{[1]}}{sum\_to(n+1) = sum\_to(n) + (n+1)}\;[\text{definition}]}{sum\_to(n+1) = n * ((n+1))(div)(2) + (n+1)}\;[\text{substitution}]}{sum\_to(n+1) = ((n * (n+1) + 2 * (n+1)))(div)(2)}\;[\text{algebra}]}{sum\_to(n+1) = (n+1) * ((n+2))(div)(2)}\;[\text{factoring}]}{(sum\_to(n) = n * ((n+1))(div)(2)) \Rightarrow (sum\_to(n+1) = (n+1) * ((n+2))(div)(2))}\;[\Rightarrow\text{-intro}^{[1]}]$$

By induction, the formula holds for all natural numbers.

Example 4 : Structural Induction on Lists

Prove: For all sequences s, reverse(reverse(s)) = s

Base case (empty sequence):

$$\dfrac{\dfrac{\dfrac{\dfrac{\ulcorner true\urcorner^{[1]}}{reverse(emptyseq) = emptyseq}\;[\text{definition}]}{reverse(reverse(emptyseq)) = reverse(emptyseq)}\;[\text{substitution}]}{reverse(reverse(emptyseq)) = emptyseq}\;[\text{definition}]}{true \Rightarrow (reverse(reverse(emptyseq)) = emptyseq)}\;[\Rightarrow\text{-intro}^{[1]}]$$

Inductive step (assume for s, prove for cons(x, s)):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\ulcorner reverse(reverse(s)) = s\urcorner^{[1]}}{reverse(cons(x,s)) = append(reverse(s), x)}\;[\text{definition}]}{reverse(reverse(cons(x,s))) = reverse(append(reverse(s), x))}\;[\text{substitution}]}{reverse(append(reverse(s), x)) = cons(x, reverse(reverse(s)))}\;[\text{definition}]}{cons(x, reverse(reverse(s))) = cons(x, s)}\;[\text{inductive hypothesis}]}{(reverse(reverse(s)) = s) \Rightarrow (reverse(reverse(cons(x,s))) = cons(x,s))}\;[\Rightarrow\text{-intro}^{[1]}]$$

By structural induction, reverse(reverse(s)) = s for all sequences.

Example 5 : Constructive Existence Proof

Prove: There ∃ an even number greater than 10

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\ulcorner true\urcorner^{[1]}}{12 = 2 * 6}\;[\text{arithmetic}]}{even(12)}\;[\text{definition of even}, 12 = 2 * 6]}{12 > 10}\;[\text{arithmetic}]}{even(12) \wedge 12 > 10}\;[\wedge\text{ intro}]}{\exists\, n : \mathbb{N} \bullet even(n) \wedge n > 10}\;[\exists\text{ intro with n = 12}]}{true \Rightarrow (\exists\, n : \mathbb{N} \bullet even(n) \wedge n > 10)}\;[\Rightarrow\text{-intro}^{[1]}]$$

Constructive proof: we exhibit a specific witness (12).

Example 6 : Non - Constructive Existence Proof

Prove: There exist irrational numbers a and b such that aˆ{}b is rational

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{[$\wedge$ intro]}
\UnaryInfC{$irrational(sqrt(2)) \wedge irrational(sqrt(2)) \wedge rational(power(sqrt(2), sqrt(2)))$}
\RightLabel{[$\exists$ intro with a = b = sqrt(2)]}
\UnaryInfC{$\exists\, a, b \bullet irrational(a) \wedge irrational(b) \wedge rational(power(a, b))$}
\AxiomC{}
\RightLabel{[exponent law]}
\UnaryInfC{$power(power(sqrt(2), sqrt(2)), sqrt(2)) = power(sqrt(2), sqrt(2) * sqrt(2))$}
\RightLabel{[arithmetic]}
\UnaryInfC{$power(sqrt(2), sqrt(2) * sqrt(2)) = power(sqrt(2), 2)$}
\RightLabel{[simplification]}
\UnaryInfC{$power(sqrt(2), 2) = 2$}
\RightLabel{[known]}
\UnaryInfC{$rational(2)$}
\RightLabel{[$\wedge$ intro]}
\UnaryInfC{$irrational(power(sqrt(2), sqrt(2))) \wedge irrational(sqrt(2)) \wedge rational(power(power(sqrt(2), sqrt(2)), sqrt(2)))$}
\RightLabel{[$\exists$ intro]}
\UnaryInfC{$\exists\, a, b \bullet irrational(a) \wedge irrational(b) \wedge rational(power(a, b))$}
\RightLabel{[$\vee$ elim]}
\BinaryInfC{$\exists\, a, b \bullet irrational(a) \wedge irrational(b) \wedge rational(power(a, b))$}
\RightLabel{[$\Rightarrow$ -intro$^{[1]}$]}
\UnaryInfC{$irrational(sqrt(2)) \Rightarrow (\exists\, a, b \bullet irrational(a) \wedge irrational(b) \wedge rational(power(a, b)))$}
\end{prooftree}
$$

Non-constructive: we don't know which case is true, but both lead to the conclusion.

Example 7 : Proof by Strong Induction

Prove: Every natural number n $\geq$ 2 has a prime factorization

Base case ($n = 2$):

$$
\begin{prooftree}
\AxiomC{$\ulcorner true \urcorner^{[1]}$}
\RightLabel{[definition]}
\UnaryInfC{$prime(2)$}
\RightLabel{[trivial, singleton factorization]}
\UnaryInfC{$prime\_factorization(2)$}
\RightLabel{[$\Rightarrow$ -intro$^{[1]}$]}
\UnaryInfC{$true \Rightarrow prime\_factorization(2)$}
\end{prooftree}
$$

Inductive step (assume for all $k < n$, prove for n):

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{[trivial, singleton factorization]}
\UnaryInfC{$prime\_factorization(n)$}
\AxiomC{}
\RightLabel{[definition of composite]}
\UnaryInfC{$\exists\, a, b \bullet 2 \leq a \wedge a < n \wedge 2 \leq b \wedge b < n \wedge n = a * b$}
\RightLabel{[strong IH, a $<$ n]}
\UnaryInfC{$prime\_factorization(a)$}
\RightLabel{[strong IH, b $<$ n]}
\UnaryInfC{$prime\_factorization(b)$}
\RightLabel{[multiplication of factorizations]}
\UnaryInfC{$prime\_factorization(a * b)$}
\RightLabel{[n = a $*$ b]}
\UnaryInfC{$prime\_factorization(n)$}
\RightLabel{[$\vee$ elim]}
\BinaryInfC{$prime\_factorization(n)$}
\RightLabel{[$\Rightarrow$ -intro$^{[1]}$]}
\UnaryInfC{$(n \geq 2) \Rightarrow prime\_factorization(n)$}
\end{prooftree}
$$

Strong induction: we assume the property for all smaller values, not just n-1.

Example 8 : Proof Using Lemmas

Lemma 1: If n is even, then nˆ{}2 is even

$$
\begin{prooftree}
\AxiomC{$\ulcorner even(n) \urcorner^{[1]}$}
\RightLabel{[definition of even]}
\UnaryInfC{$\exists\, k \bullet n = 2 * k$}
\RightLabel{[substitution]}
\UnaryInfC{$power(n, 2) = power(2 * k, 2)$}
\RightLabel{[algebra]}
\UnaryInfC{$power(2 * k, 2) = 4 * power(k, 2)$}
\RightLabel{[factoring]}
\UnaryInfC{$4 * power(k, 2) = 2 * (2 * power(k, 2))$}
\RightLabel{[$\exists$ intro with m = 2 $*$ power(k, 2)]}
\UnaryInfC{$\exists\, m \bullet power(n, 2) = 2 * m$}
\RightLabel{[definition of even]}
\UnaryInfC{$even(power(n, 2))$}
\RightLabel{[$\Rightarrow$ -intro$^{[1]}$]}
\UnaryInfC{$even(n) \Rightarrow even(power(n, 2))$}
\end{prooftree}
$$

Main theorem: If n^{}2 is odd, then n is odd

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{[Lemma1]}
\UnaryInfC{$even(power(n,2))$}
\RightLabel{[contradiction]}
\UnaryInfC{$odd(power(n,2)) \land even(power(n,2))$}
\RightLabel{[contradiction]}
\UnaryInfC{$false$}
\RightLabel{[false elim]}
\UnaryInfC{$odd(n)$}
\AxiomC{}
\RightLabel{[identity]}
\UnaryInfC{$odd(n)$}
\RightLabel{[$\lor$ elim]}
\BinaryInfC{$odd(n)$}
\RightLabel{[$\Rightarrow$ -intro$^{[1]}$]}
\UnaryInfC{$odd(power(n,2)) \Rightarrow odd(n)$}
\end{prooftree}
$$

Proof by contrapositive using lemma.

Example 9 : Proof by Minimal Counterexample

Prove: All natural numbers n $\geq$ 1 satisfy P(n)

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{[base case proved separately]}
\UnaryInfC{$\mathbb{P}\,1$}
\RightLabel{[contradiction]}
\UnaryInfC{$\neg\ \mathbb{P}\,m \land \mathbb{P}\,1$}
\RightLabel{[contradiction]}
\UnaryInfC{$false$}
\AxiomC{}
\RightLabel{[minimality of m]}
\UnaryInfC{$\forall\, k \bullet k \geq 1 \land k < m \Rightarrow \mathbb{P}\,k$}
\RightLabel{[since m $-$ 1 >= 1 $\land$ m $-$ 1 < m]}
\UnaryInfC{$\mathbb{P}(m-1)$}
\RightLabel{[by inductive step from P(m $-$ 1)]}
\UnaryInfC{$\mathbb{P}\,m$}
\RightLabel{[contradiction]}
\UnaryInfC{$\neg\ \mathbb{P}\,m \land \mathbb{P}\,m$}
\RightLabel{[contradiction]}
\UnaryInfC{$false$}
\RightLabel{[$\lor$ elim]}
\BinaryInfC{$false$}
\RightLabel{[$\neg$ -intro$^{[2]}$]}
\UnaryInfC{$\forall\, n \bullet n \geq 1 \Rightarrow \mathbb{P}\,n$}
\RightLabel{[$\Rightarrow$ -intro$^{[1]}$]}
\UnaryInfC{$true \Rightarrow (\forall\, n \bullet n \geq 1 \Rightarrow \mathbb{P}\,n)$}
\end{prooftree}
$$

Minimal counterexample combines well-ordering with contradiction.

Example 10 : Proof by Invariant

Prove: A loop maintains invariant I

Initialization:

$$
\begin{prooftree}
\AxiomC{$\ulcorner initial\_state \urcorner^{[1]}$}
\RightLabel{[verification]}
\UnaryInfC{$invariant(initial\_state)$}
\RightLabel{[$\Rightarrow$ -intro$^{[1]}$]}
\UnaryInfC{$initial\_state \Rightarrow invariant(initial\_state)$}
\end{prooftree}
$$

Preservation:

$$
\begin{prooftree}
\AxiomC{$\ulcorner invariant(before\_state) \land executes\_loop\_body \urcorner^{[1]}$}
\RightLabel{[$\land$ -elim-1]}
\UnaryInfC{$invariant(before\_state)$}
\RightLabel{[$\land$ -elim-2]}
\UnaryInfC{$executes\_loop\_body$}
\RightLabel{[verification]}
\UnaryInfC{$invariant(after\_state)$}
\RightLabel{[$\Rightarrow$ -intro$^{[1]}$]}
\UnaryInfC{$(invariant(before\_state) \land executes\_loop\_body) \Rightarrow invariant(after\_state)$}
\end{prooftree}
$$

Termination:

$$\dfrac{\dfrac{\dfrac{\dfrac{\ulcorner loop\_terminates \urcorner^{[1]}}{invariant(termination\_state)}\ [\text{by preservation}]}{invariant(termination\_state) \land termination\_condition}\ [\land \text{ intro}]}{desired\_property}\ [\text{logic}]}{loop\_terminates \Rightarrow desired\_property}\ [\Rightarrow \text{-intro}^{[1]}]$$

Example 11 : Proof by Diagonalization

Prove: The set of real numbers is uncountable

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\ulcorner countable(reals) \urcorner^{[2]}}{\exists f \bullet enumeration(f, reals)}\ [\text{definition of countable}]}{diagonal\_construction(r)}\ [\text{diagonal method}]}{\forall n \bullet r \neq apply(f, n)}\ [\text{by construction, differs at nth digit}]}{not\_in\_range(r, f)}\ [\text{previous line}]}{not\_in\_range(r, f) \land enumeration(f, reals)}\ [\text{contradiction}]}{false}\ [\text{contradiction}]}{uncountable(reals)}\ [\neg \text{-intro}^{[2]}]}{true \Rightarrow uncountable(reals)}\ [\Rightarrow \text{-intro}^{[1]}]$$

Cantor's diagonal argument (outline).

Example 12 : Constructive Proof Pattern

To constructively prove: $\exists x \bullet \mathbb{P}\, x$

Strategy:

1. Explicitly construct a witness w

2. Verify P(w) holds

3. Conclude $\exists x \bullet \mathbb{P}\, x$with $x = w$

Example: Prove $\exists n : \mathbb{N} \bullet n > 100 \land$ n is even

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\ulcorner true \urcorner^{[1]}}{witness\_construction(102)}\ [\text{construction}]}{102 > 100}\ [\text{arithmetic}]}{102 = 2 * 51}\ [\text{arithmetic}]}{even(102)}\ [\text{definition}]}{102 > 100 \land even(102)}\ [\land \text{ intro}]}{\exists n \bullet n > 100 \land even(n)}\ [\exists \text{ intro with n} = 102]}{true \Rightarrow (\exists n \bullet n > 100 \land even(n))}\ [\Rightarrow \text{-intro}^{[1]}]$$

Example 13 : Proof Composition

Combine multiple proof techniques:

Theorem: Property P holds for all cases

Overall strategy: Case analysis + Induction + Contradiction

$$\dfrac{\dfrac{\dfrac{}{\mathbb{P}\ \mathit{base}}\ [\text{direct proof}] \qquad \dfrac{\dfrac{\dfrac{\dfrac{\ulcorner \neg\ \mathbb{P}\ n \urcorner^{[2]}}{\mathit{contradiction\_derived}}\ [\text{proof steps}]}{\mathit{false}}\ [\text{contradiction}]}{\mathbb{P}\ n}\ [\neg\text{ -intro}^{[2]}] \qquad \dfrac{\dfrac{\ulcorner \mathbb{P}(n-1) \urcorner^{[3]}}{\mathbb{P}\ n}\ [\text{inductive step}]}{\mathbb{P}\ n}\ [\Rightarrow\text{ -intro}^{[3]}]}{\mathbb{P}\ n}\ [\vee\text{ elim over subcases}]}{\forall\, n \bullet \mathbb{P}\ n}\ [\vee\text{ elim over cases}]}{\mathit{true} \Rightarrow (\forall\, n \bullet \mathbb{P}\ n)}\ [\Rightarrow\text{ -intro}^{[1]}]$$

Example 14 : Best Practices for Complex Proofs

Guidelines for writing advanced proofs:

1. State strategy at the beginning

2. Label cases clearly

3. Discharge assumptions promptly

4. Reference lemmas explicitly

5. Show key algebraic steps

6. Justify non-obvious steps

7. Use proof by cases when structure suggests it

8. Use induction for recursive definitions

9. Use contradiction for negative conclusions

10. Verify base cases thoroughly

Example 15 : Proof Documentation

Document complex proofs:

- **Goal**: State what you're proving

- **Strategy**: Explain the proof approach

- **Lemmas needed**: List dependencies

- **Key insights**: Highlight non-obvious steps

- **Pitfalls**: Note where proof could go wrong

- **Generalization**: Explain how proof extends

Well-documented proofs are maintainable and reusable.