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

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

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):

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

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):

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

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

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

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

Example 5 : Constructive Existence Proof

Prove: There ∃ an even number greater than 10

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

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

Example 6 : Non - Constructive Existence Proof

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

$$\dfrac{\dfrac{\dfrac{\dfrac{}{irrational(sqrt(2)) \land irrational(sqrt(2)) \land rational(power(sqrt(2), sqrt(2)))}\,[\land\text{ intro}]}{\exists\, a, b \bullet irrational(a) \land irrational(b) \land rational(power(a, b))}\,[\exists\text{intro with a} = \text{b} = \text{sqrt(2)}] \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{power(power(sqrt(2), sqrt(2)), sqrt(2)) = power(sqrt(2), sqrt(2) * sqrt(2))}\,[\text{exponent law}]}{power(sqrt(2), sqrt(2) * sqrt(2)) = power(sqrt(2), 2)}\,[\text{arithmetic}]}{power(sqrt(2), 2) = 2}\,[\text{simplification}]}{rational(2)}\,[\text{known}]}{irrational(power(sqrt(2), sqrt(2))) \land irrational(sqrt(2)) \land rational(power(power(sqrt(2), sqrt(2)), sqrt(2)))}\,[\land\text{ intro}]}{\exists\, a, b \bullet irrational(a) \land irrational(b) \land rational(power(a, b))}\,[\exists\text{intro}]}{\exists\, a, b \bullet irrational(a) \land irrational(b) \land rational(power(a, b))}\,[\lor\text{ elim}]}{irrational(sqrt(2)) \Rightarrow (\exists\, a, b \bullet irrational(a) \land irrational(b) \land rational(power(a, b)))}\,[\Rightarrow\text{-intro}^{[1]}]$$

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 ($n = 2$):

$$\dfrac{\dfrac{\dfrac{\ulcorner true \urcorner^{[1]}}{prime(2)}\,[\text{definition}]}{prime\_factorization(2)}\,[\text{trivial, singleton factorization}]}{true \Rightarrow prime\_factorization(2)}\,[\Rightarrow\text{-intro}^{[1]}]$$

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

$$\dfrac{\dfrac{\dfrac{}{prime\_factorization(n)}\,[\text{trivial, singleton factorization}] \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\exists\, a, b \bullet 2 \leq a \land a < n \land 2 \leq b \land b < n \land n = a * b}\,[\text{definition of composite}]}{prime\_factorization(a)}\,[\text{strong IH, a} < \text{n}]}{prime\_factorization(b)}\,[\text{strong IH, b} < \text{n}]}{prime\_factorization(a * b)}\,[\text{multiplication of factorizations}]}{prime\_factorization(n)}\,[\text{n} = \text{a} * \text{b}]}{prime\_factorization(n)}\,[\lor\text{ elim}]}{(n \geq 2) \Rightarrow prime\_factorization(n)}\,[\Rightarrow\text{-intro}^{[1]}]$$

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 n^{}2 is even

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

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

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{even(power(n,2))}\;\text{[Lemma1]}}{odd(power(n,2)) \land even(power(n,2))}\;\text{[contradiction]}}{false}\;\text{[contradiction]}}{odd(n)}\;\text{[false elim]} \qquad \dfrac{}{odd(n)}\;\text{[identity]}}{odd(n)}\;\text{[$\lor$ elim]}}{odd(power(n,2)) \Rightarrow odd(n)}\;\text{[$\Rightarrow$ -intro$^{[1]}$]}$$

Proof by contrapositive using lemma.

Example 9 : Proof by Minimal Counterexample

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

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\mathbb{P}\ 1}\;\text{[base case proved separately]}}{\neg\ \mathbb{P}\ m \land \mathbb{P}\ 1}\;\text{[contradiction]}}{false}\;\text{[contradiction]} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall\ k \bullet k \geq 1 \land k < m \Rightarrow \mathbb{P}\ k}\;\text{[minimality of m]}}{\mathbb{P}(m-1)}\;\text{[since m $-$ 1 >= 1 $\land$ m $-$ 1 < m]}}{\mathbb{P}\ m}\;\text{[by inductive step from P(m $-$ 1)]}}{\neg\ \mathbb{P}\ m \land \mathbb{P}\ m}\;\text{[contradiction]}}{false}\;\text{[contradiction]}}{false}\;\text{[$\lor$ elim]}}{\forall\ n \bullet n \geq 1 \Rightarrow \mathbb{P}\ n}\;\text{[$\neg$ -intro$^{[2]}$]}}{true \Rightarrow (\forall\ n \bullet n \geq 1 \Rightarrow \mathbb{P}\ n)}\;\text{[$\Rightarrow$ -intro$^{[1]}$]}$$

Minimal counterexample combines well-ordering with contradiction.

Example 10 : Proof by Invariant

Prove: A loop maintains invariant I

Initialization:

$$\dfrac{\dfrac{\ulcorner initial\_state \urcorner^{[1]}}{invariant(initial\_state)}\;\text{[verification]}}{initial\_state \Rightarrow invariant(initial\_state)}\;\text{[$\Rightarrow$ -intro$^{[1]}$]}$$

Preservation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\ulcorner invariant(before\_state) \land executes\_loop\_body \urcorner^{[1]}}{invariant(before\_state)}\;\text{[$\land$ -elim-1]}}{executes\_loop\_body}\;\text{[$\land$ -elim-2]}}{invariant(after\_state)}\;\text{[verification]}}{(invariant(before\_state) \land executes\_loop\_body) \Rightarrow invariant(after\_state)}\;\text{[$\Rightarrow$ -intro$^{[1]}$]}$$

Termination:

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

Example 11 : Proof by Diagonalization

Prove: The set of real numbers is uncountable

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

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 $\exists\, n : \mathbb{N} \bullet n > 100\wedge$ n is even

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

Example 13 : Proof Composition

Combine multiple proof techniques:

Theorem: Property P holds for all cases

Overall strategy: Case analysis + Induction + Contradiction

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

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.