Massachusetts Institute of Technology — Lecture 2
6.042J/18.062J: Mathematics for Computer Science — September 12, 2000
Professors Nancy Lynch and Shlomi Dolev

Predicate Reasoning; Proof by Induction

This handout contains some formatted versions of proofs that will look messier on the blackboard.

1 Predicate reasoning examples

1.1 Birthdate

Step	Justification
Prove: $\forall n \in N(n^2 + n \text{ is even})$.	
1. Fix $n \in N$.	
2. $n^2 + n$ is even.	
1. If n is odd then $n^2 + n$ is even.	???
2. If n is even then $n^2 + n$ is even.	???
3. QED ($n^2 + n$ is even.)	Cases
3. QED ($\forall n \in N(n^2 + n \text{ is even})$.)	

Step	Justification
Prove: $\forall n \in N(n^2 + n \text{ is even})$.	
1. Fix $n \in N$.	
2. $n^2 + n$ is even.	
1. If n is odd then $n^2 + n$ is even.	
1. Assume n is odd.	
2. $n^2 + n$ is even.	
1. $\exists x \in N(n = 2x + 1)$	Definition of "odd"
2. Choose $x \in N$, $n = 2x + 1$	EI
3. $n^2 + n = 4x^2 + 4x + 1 + 2x + 1 = 2(2x^2 + 3x + 1)$	Algebra
4. $\exists y \in N(n^2 + n = 2y)$	EG
5. QED ($n^2 + n$ is even)	Definition of "even"
3. QED (If n is odd then $n^2 + n$ is even.)	Implication
2. If n is even then $n^2 + n$ is even.	
1. Assume n is even.	
2. $n^2 + n$ is even.	
1. $\exists x \in N(n = 2x)$	Definition of "even"
2. Choose $x \in N$, $n = 2x$	Existential Instantiation (EI)
3. $n^2 + n = 4x^2 + 2x = 2(2x^2 + x)$	Algebra
4. $\exists y \in N(n^2 + n = 2y)$	Existential Generalization (EG)
5. QED ($n^2 + n$ is even)	Definition of "even"
3. QED (If n is even then $n^2 + n$ is even.)	Implication
3. QED ($n^2 + n$ is even.)	Cases
3. QED ($\forall n \in N(n^2 + n \text{ is even})$.)	UG

Prove: $\forall n \in N(n^2 + n \text{ is even})$.

1. Fix $n \in N$.
2. $n^2 + n$ is even.
    1. If n is odd then $n^2 + n$ is even.
        1. Assume n is odd.
        2. Choose $x \in N$, $n = 2x + 1$ — Definition of "odd", EI
        3. $n^2 + n = 4x^2 + 4x + 1 + 2x + 1 = 2(2x^2 + 3x + 1)$ — Algebra
        4. $n^2 + n$ is even — EG, Definition of "even"
        5. QED (If n is odd then $n^2 + n$ is even.) — Implication
    2. If n is even then $n^2 + n$ is even.
        1. Assume n is even.
        2. Choose $x \in N$, $n = 2x$ — Definition of "even", EI
        3. $n^2 + n = 4x^2 + 2x = 2(2x^2 + x)$ — Algebra
        4. $n^2 + n$ is even. — EG, definition of "even"
        5. QED (If n is even then $n^2 + n$ is even.) — Implication
    3. QED ($n^2 + n$ is even.) — Cases
3. QED ($\forall n \in N(n^2 + n \text{ is even})$.) — UG

1.2 $\sqrt{2}$ is irrational

Prove: $\sqrt{2}$ is irrational.

1. $\sqrt{2}$ rational $\Rightarrow$ *false*
    1. Assume $\sqrt{2}$ rational.
    2. *false*
        1. Choose $a, b \in N^+$, $\sqrt{2} = \frac{a}{b}$, lowest terms. — Basic properties of rationals, EI
        2. $2b^2 = a^2$ — Algebra
        3. a^2 is even. — EG, definition of "even"
        4. a is even. — ???
        5. Choose $c \in N$, $a = 2c$. — Definition of "even", EI
        6. $4c^2 = a^2 = 2b^2$ — Algebra
        7. $2c^2 = b^2$ — Algebra
        8. b^2 is even. — EG, definition of "even"
        9. b is even. — ???
        10. a and b aren't in lowest terms. — 1.2.4, 1.2.9
        11. QED — 1.2.1, 1.2.10, propositional logic
    3. QED — Implication
2. QED — Contradiction

4. a is even.
    1. a is odd $\Rightarrow$ *false*
        1. Assume a is odd.
        2. a^2 is odd. — Do a proof like the one in the birthdate example, using EI, algebra, and EG.
        3. *false* — 1.2.3, 1.2.4.1.2, Propositional logic
    2. QED — Contradiction

Lemma 1:

Prove: $\forall x \in N[x \text{ odd} \implies x^2 \text{ odd}]$.	
1. Fix $x_0 \in N$.	
2. x_0 odd $\implies x_0^2$ odd.	
1. Assume x_0 is odd.	
2. Choose $y \in N$, $x_0 = 2y + 1$.	Definition of "odd", EI
3. $x_0^2 = 4y^2 + 4y + 1 = 2(2y^2 + 2y) + 1$	Algebra
4. x_0^2 is odd.	EG, definition of "odd".
5. QED	Implication
3. QED	UG

Lemma 2:

Prove: $\forall x \in N[x^2 \text{ even} \implies x \text{ even}]$.	
1. Fix $x_0 \in N$.	
2. x_0^2 even $\implies x_0$ even.	
1. Assume x_0^2 even	
2. x_0 odd $\implies x_0^2$ odd.	Lemma 1, UI
3. x_0 even.	Propositional reasoning
4. QED	Implication
3. QED	UG

Proof. The proof is by contradiction. Assume for purpose of contradiction that $\sqrt{2}$ is rational. Then we can write $\sqrt{2} = a/b$ where a and b are integers and the fraction is in lowest terms. Squaring both sides gives $2 = a^2/b^2$ and so $2b^2 = a^2$. This implies that a is even; that is, a is a multiple of 2. As a result, a^2 is a multiple of 4. Because of the equality $2b^2 = a^2$, $2b^2$ must also be a multiple of 4. This implies that b^2 is even and so b must be even. But since a and b are both even, the fraction a/b is not in lowest terms. This is a contradiction, and so the assumption that $\sqrt{2}$ is rational must be false. ∎

1.3 De Morgan's Law

Prove: $\forall A, B(\overline{A} \cap \overline{B} = \overline{A \cup B})$	
1. Fix A, B.	
2. $\overline{A} \cap \overline{B} = \overline{A \cup B}$	???
3. QED	UG

Prove: $\forall A, B(\overline{A} \cap \overline{B} = \overline{A \cup B})$.	
1. Fix A, B.	
2. $\overline{A} \cap \overline{B} = \overline{A \cup B}$	
1. $\forall x(x \in \overline{A} \cap \overline{B} \Leftrightarrow x \in \overline{A \cup B})$	
1. Fix x.	
2. $x \in \overline{A} \cap \overline{B} \Leftrightarrow x \in \overline{A \cup B}$	???
3. QED	UG
2. QED	Definition of set equality.
3. QED	UG

2. $x \in \overline{A} \cap \overline{B} \Leftrightarrow x \in \overline{A \cup B}$
   1. $x \in \overline{A} \cap \overline{B} \Rightarrow x \in \overline{A \cup B}$???
   2. $x \in \overline{A \cup B} \Rightarrow x \in \overline{A} \cap \overline{B}$???
   3. QED Propositional logic

2. $x \in \overline{A \cup B} \Rightarrow x \in \overline{A} \cap \overline{B}$
   1. Assume $x \in \overline{A \cup B}$.
   2. $x \notin A \cup B$ Definition of complement
   3. $x \notin A$, $x \notin B$ Definition of union
   4. $x \in \overline{A}$, $x \in \overline{B}$ Definition of complement
   5. $x \in \overline{A} \cap \overline{B}$ Definition of intersection
   6. QED Implication

2 Inductive proof examples

2.1 Sum of Series

Prove: $\forall n \geq 0 (\sum_{i=1}^{n} i = \frac{n(n+1)}{2})$.

1. (Base) $\sum_{i=1}^{0} i = \frac{0(0+1)}{2}$. ???
2. (Inductive step) $\forall n \geq 0 (\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \Rightarrow \sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2})$???
3. QED Induction

1. (Base) $\sum_{i=1}^{0} i = \frac{0(0+1)}{2}$
   1. $\sum_{i=1}^{0} i = 0$ Definition of summation with no terms
   2. $\frac{0(0+1)}{2} = 0$ Arithmetic
   3. QED By 1.1 and 1.2.

2. (Inductive step) $\forall n \geq 0 (\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \Rightarrow \sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2})$
   1. Fix $n \geq 0$.
   2. $\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \Rightarrow \sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$
      1. Assume $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$
      2. $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$???
      3. QED Implication
   3. QED UG

2. $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$
   1. $\sum_{i=1}^{n+1} i = (\sum_{i=1}^{n} i) + (n+1)$ Summation has one extra term.
   2. $(\sum_{i=1}^{n} i) + (n+1) = \frac{n(n+1)}{2} + n + 1$ Inductive hypothesis $P(n)$ (2.2.1)
   3. $\frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}$ Algebra
   4. QED Combining the previous 3 equations.

2.2 Divisibility

Prove: $\forall n \in N, n \geq 0 (6 | n^3 - n)$

1. (Base) $6 | 0^3 - 0$
2. (Inductive step) $\forall n \geq 0 (6 | n^3 - n \Rightarrow 6 | (n+1)^3 - (n+1))$
    1. Fix $n \geq 0$.
    2. Assume $6 | n^3 - n$
    3. $6 | (n+1)^3 - (n+1)$

1. $(n+1)^3 - (n+1) = n^3 - n + 3(n^2 + n)$	Algebra
2. $n^2 + n$ is even	Proved this earlier today
3. $2 \| n^2 + n$	Definition of $\|$
4. $6 \| 3(n^2 + n)$	Multiplying both sides by 3 (basic properties of N)
5. $6 \| (n^3 - n) + 3(n^2 + n)$	Divides both terms (2.2, 2.3.4), so divides sum.
6. QED	2.3.1, 2.3.5

    4. QED
3. QED