CHAPTER 3: REFLECTIONS ON LOGIC AND PROOF

Number Systems and Bases (Non-textbook material)

Base 10: digits {0,1,2,3,4,5,6,7,8,9} (decimal)
Base 2: digits {0,1} (binary)

Counting in Decimal versus Binary:

Base 10	Base 2		Base 10	Base 2		Base 10	Base 2
0	0		10	1010		20	10100
1	1		11	1011		21	10101
2	10		12	1100		22	10110
3	11		13	1101		23	10111
4	100		14	1110		24	11000
5	101		15	1111		25	11001
6	110		16	10000		26	11010
7	111		17	10001		27	11011
8	1000		18	10010		28	11100
9	1001		19	10011		29	11101

Decimal representation of an integer:

$$23 = 20 + 3 = 2 \cdot 10^1 + 3 \cdot 10^0$$

$$1729 = 1000 + 700 + 20 + 9 = 1 \cdot 10^3 + 7 \cdot 10^2 + 2 \cdot 10^1 + 9 \cdot 10^0$$

Binary representation of an integer:

$$10111_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 16 + 4 + 2 + 1 = 23$$

$$11011000001_2 = 2^{10} + 2^9 + 2^7 + 2^6 + 2^0 = 1024 + 512 + 128 + 64 + 1 = 1729$$

BINARY-to-DECIMAL Algorithm: To convert a binary integer $B = a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0$ into a decimal integer D where each digit a_i of B is either 0 or 1:

1. Compute the value $D = a^n \cdot 2^n + a_{n-1} \cdot 2^{n-1} + \ldots + a_2 \cdot 2^2 + a_1 \cdot 2^1 + a_0 \cdot 2^0$

Conversion from decimal to binary:

$$23 = 16 + 4 + 2 + 1 = 2^4 + 2^2 + 2^1 + 2^0$$

$$1729 = 1024 + 512 + 128 + 64 + 1 = 2^{10} + 2^9 + 2^7 + 2^6 + 2^0$$

DECIMAL-to-BINARY Algorithm 1 (left to right): To convert a decimal integer D into a binary integer B:

1. Compute largest power of 2 less than or equal to D, i.e. find p such that $2^p \le D$.
2. If $2^p < D$, then replace D by $D - 2^p$ and repeat step 1.
3. Else stop; the values of p indicate positions of the digit 1 in the binary integer B.

Example: Convert the decimal integer 220 to binary.

Solution: We following the above algorithm as described in the table below:

D	2^p	$D-2^p$	b_p
220	128=2^7	92	1
92	64=2^6	28	1
28	16=2^4	12	1
12	8=2^3	4	1
4	4=2^2	0	1

Thus, the binary representation is $\underset{7}{1}\underset{6}{1}0\underset{4}{1}\underset{3}{1}\underset{2}{1}00$.

DECIMAL-to-BASE-b Algorithm 2 (right to left): To convert a decimal integer D into a base-b integer B:

1. Set $i = 0$.
2. Apply Euclid's Division Theorem to express $D = bq + r$, where $r = D \bmod b$. Set $b_i = r$ and replace D by q.
2. If $q \ge b$, then replace D by q, increment i, and repeat step 2.
3. Else set $N = i + 1$ and $b_N = q$; print $B = b_N b_{N-1} \cdots b_1 b_0$ and stop.

Example: (Revisited) Convert the decimal integer 220 to binary using Algorithm 2.

Solution: We following the above algorithm as described in the table below:

i	D	q	$r = b_i$
0	220	110	0
1	110	55	0
2	55	27	1
3	27	13	1
4	13	6	1
5	6	3	0
6	3	1	1
7	1	0	1

Thus, we have $220 = 11011100_2$.

NOTE: A *byte* in computer science is an 8-digit binary string, e.g. 11011100. What is the largest value that can be represented by a byte?

Binary Arithmetic

The notion of a "carry" when adding and multiplying decimal integers is also valid for binary integers. Binary arithmetic essentially relies on the following addition and multiplication tables.

Binary Addition	**Binary Multiplication**
$0+0=0$	$0\cdot 0=0$
$0+1=1$	$0\cdot 1=0$
$1+0=1$	$1\cdot 0=0$
$1+1=10$	$1\cdot 1=1$

2 in decimal

$(1+1)+1=11$

dec

Example: Perform the following calculations by hand:

a) 13749 + 8165

b) 101011_2+1001_2

c) $67\cdot 14$

d) $1011\cdot 101$

Solution:

a)

$$\begin{array}{r} {\scriptstyle 1\ \ 1\ 1}\\ 13749\\ +\ 8165\\ \hline 21914 \end{array}$$

carry & add

b)

$$\begin{array}{r} {\scriptstyle 1\ \ 1\ 1}\\ 101011\\ +\ \ 1001\\ \hline 110100 \end{array}$$

$1+1=10$

$(1+0)+1=10$

c)

$$\begin{array}{r} {\scriptstyle 2}\\ 67\\ \times\ 14\\ \hline 268\\ 67\\ \hline 938 \end{array}$$

4 tens, so shift

d)

$$\begin{array}{r} 1011\\ \times\ 101\\ \hline 1011\\ 0\\ {\scriptstyle 1}\\ 1011\\ \hline 110111 \end{array}$$

← shift

← shift again

add 2 #'s at the time

3.1 Equivalence and Implication

Boolean Logic Algebra

Truth values: T (True or 1), F (False or 0)
Universe: $B = \{T, F\}$
Variables (symbols, literals): s, t, etc.
Binary operations (logical connectives, functions of two-variables): $f : B \times B \to B$

$f(x) = x^2$
$f(3) = 3^2 = 9$
$f(x,y) = x^2 + y^2$
$f(3,4) = 3^2 + 4^2 = 25$
$f : S \to T$ (domain, range)
$B \times B = \{(s,t) : s,t \in B\}$ (4 ways (pairs); Cartesian product)

Special binary operations: AND ($\wedge$), OR ($\vee$), XOR ($\oplus$), NOT ($\neg$), NAND ($\overline{\wedge}$)

1. AND ($\wedge$, &&, conjunction): insert in between 2 inputs

$\text{AND}(T,T) = T \wedge T = T$
$\text{AND}(T,F) = T \wedge F = F$
$\text{AND}(F,T) = F \wedge T = F$
$\text{AND}(F,F) = F \wedge F = F$

2. OR ($\vee$, ||, disjunction)
3. XOR ($\oplus$)
4. NOT ($\neg$,~) single variable

Truth Tables

The special Boolean operations above can also be defined using a truth table to list its values:

conjunction: (this) and (that)
disjunction: (this) or (that)

AND (inputs → $f(s,t)$; output)

s	t	$s \wedge t$
T	T	T
T	F	F
F	T	F
F	F	F

OR

s	t	$s \vee t$
T	T	T
T	F	T
F	T	T
F	F	F

XOR (out carried; if inputs same, comes out to false)

s	t	$s \oplus t$
T 1	T 1	F 0
T	F	T
F	T	T
F	F	F

NOT

s	$\neg s$
T	F
F	T

Analogy with Arithmetic

AND ($\cdot$)

x	y	$x \cdot y$
1	1	1
1	0	0
0	1	0
0	0	0

OR ($+$)

x	y	$x + y$
1	1	1
1	0	1
0	1	1
0	0	0

Properties of Boolean Operations:

1. Commutative: $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$
2. Associative: $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ and $(x \vee y) \vee z = x \vee (y \vee z)$
3. Distributive: $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ and $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
4. DeMorgan's Laws: $\neg(x \wedge y) = (\neg x) \vee (\neg y)$ and $\neg(x \vee y) = (\neg x) \wedge (\neg y)$

NOTE: In general we have $x \wedge (y \vee z) \neq (x \wedge y) \vee z$; thus, the associative property fails to hold in the case where both operations $\wedge$ and $\vee$ are involved.

Proof Technique: To prove that two Boolean expressions are equivalent, it suffices to show that their corresponding truth tables are the same.

Proof of Associative Laws: We make a truth table for the left and right-hand sides of the first law involving AND:

x	y	z	$x \wedge y$	$(x \wedge y) \wedge z$	$y \wedge z$	$x \wedge (y \wedge z)$
T	T	T	T	**T**	T	**T**
T	T	F	T	**F**	F	**F**
T	F	T	F	**F**	F	**F**
T	F	F	F	**F**	F	**F**
F	T	T	F	**F**	T	**F**
F	T	F	F	**F**	F	**F**
F	F	T	F	**F**	F	**F**
F	F	F	F	**F**	F	**F**

Since the columns for $(x \wedge y) \wedge z$ and $x \wedge (y \wedge z)$ are the same, this proves the first law: $(x \wedge y) \wedge z = x \wedge (y \wedge z)$. A similar proof can be applied to the second law involving OR.

Proof of DeMorgan's Laws: We make a truth table for the left and right-hand sides of the first law:

x	y	$x \wedge y$	$\neg(x \wedge y)$	$\neg x$	$\neg y$	$(\neg x) \vee (\neg y)$
T	T	T	**F**	F	F	**F**
T	F	F	**T**	F	T	**T**
F	T	F	**T**	T	F	**T**
F	F	F	**T**	T	T	**T**

Since the columns for $\neg(x \wedge y)$ and $(\neg x) \vee (\neg y)$ are the same, this proves the first law: $\neg(x \wedge y) = (\neg x) \vee (\neg y)$. A similar proof can be applied to the second law.

Implication and If and Only If

"P implies Q", Q follows from P

P: Assumption
Q: Conclusion

Mathematical Statement: If P, then Q $(P \Rightarrow Q)$

Example: Consider the statement: If $\overbrace{n \text{ is a prime number greater than } 3}^{P}$, then $\overbrace{n \text{ is odd}}^{Q}$. What should be the truth table for $P \Rightarrow Q$?

5 is greater than 3 & prime & not odd

n	P	Q	$P \Rightarrow Q$
5	T	T	**T**
-	T	F	**?**
3	F	T	**?**
4	F	F	**?**

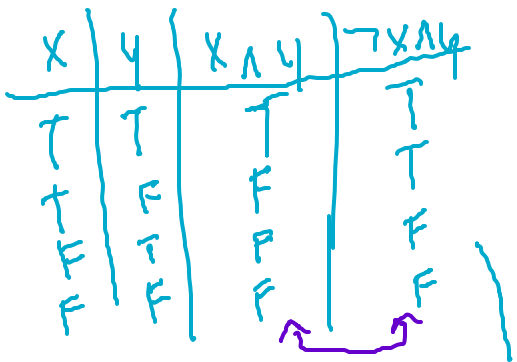
Example: Suppose a person holds a playing card. Without showing you the card, he makes the statement "If this card is a heart, then it is a queen" (If P, then Q). In which of the situations below would this person be lying, i.e. making a false statement:

a. The card is a heart ($P = T$) and a queen ($Q = T$) — T => T = T
b. The card is a heart ($P = T$) and a king ($Q = F$) — T => F = F
c. The card is a diamond ($P = F$) and a queen ($Q = T$) — F => T = T
d. The card is a diamond ($P = F$) and a king ($Q = F$) — F => F = T

not lie not not

└ if condition doesn't hold, so statement doesn't apply, so not lying

1. Implication (If-then/conditional): $\rightarrow$ $(\Rightarrow)$



x	y	$x \rightarrow y$
T	T	**T**
T	F	**F**
F	T	**T**
F	F	**T**

2. If and only if (bi-conditional): $\leftrightarrow (\Leftrightarrow)$

x	y	$x \leftrightarrow y$
T	T	**T**
T	F	**F**
F	T	**F**
F	F	**T**

NOTE: $P \Leftrightarrow Q$ is equivalent to $P \Rightarrow Q$ and $Q \Rightarrow P$.

Exercises:

1. Define the Boolean operation $\overline{\wedge}$ (called NAND) as the composition of NOT and AND: $x \mathbin{\overline{\wedge}} y = \neg(x \wedge y)$. Determine whether or not the two Boolean operations $x \vee y$ (OR) and $(x \mathbin{\overline{\wedge}} x) \mathbin{\overline{\wedge}} (y \mathbin{\overline{\wedge}} y)$ equivalent. NOTE: This shows that OR can be expressed in terms of NAND; moreover, it can be shown that all Boolean operations expressed in terms of NAND.
2. Negate $x \rightarrow y$. HINT: First prove that $x \rightarrow y$ and $(\neg x) \vee y$ are logically equivalent.

Tautologies and Contradictions: A Boolean expression is called a tautology (or contradiction) if its truth-value is always TRUE (or FALSE, respectively).

Conjunctive Normal Form: A conjunction of one or more clauses, where each clause is a disjunction of literals.

Logic Gates and Circuits (See Problem of the Day handout)

3.2 Variables and Quantifiers

Big-O Notation (see textbook Power-point slide presentation on Big-O notation)

Let $f : \mathbb{R} \rightarrow \mathbb{R}$ and $g : \mathbb{R} \rightarrow \mathbb{R}$ be two non-negative functions, i.e. $f(x) \geq 0$ and $g(x) \geq 0$ for all $x \in \mathbb{R}$.

Definition:

(a) We say that $f(x) = O(g(x))$ (big-O) if there exist positive numbers c and n_0 such that $f(x) \leq c \cdot g(x)$ for all $x > n_0$.

(b) We say that $f(x) = \Theta(g(x))$ (big-theta) if $f(x) = O(g(x))$ and $g(x) = O(f(x))$.

NOTE: The values c and n_0 are NOT unique. In fact, there are infinitely many choices for them once it known that there exists at least one.

Example:

(a) Let $f(x) = |x|$ and $g(x) = x^2$. Prove that $f(x) = O(g(x))$.

(b) Let $f(x) = x^2$ and $g(x) = x^2 + 100$. Prove that $f(x) = \Theta(g(x))$.

(c) Let $f(x) = x^2$ and $g(x) = 2^x$. Prove that $f(x) = O(g(x))$.

Solution:

(a) Based on their graphs, we see that $|x| = x < x^2$ for all $x > 1$. We choose $c = 1$ and $n_0 = 1$. It follows that $f(x) \le c \cdot g(x)$ for all $x > n_0$. Thus, $f(x) = O(g(x))$.

(b) It is clear that $f(x) \le g(x)$ for all $x \in \mathbb{R}$. It follows that $f(x) = O(g(x))$ where $c = 1$ and $n_0 = 1$. To prove $g(x) = O(f(x))$, we first choose $c = 2$ (arbitrary). Then

$$g(x) \le c \cdot f(x) \Leftrightarrow x^2 + 100 \le 2x^2 \Leftrightarrow x^2 \ge 100$$
$$\therefore x \ge 10$$

Thus, we can choose $n_0 = 10$ (or larger). Hence, we conclude that $f(x) = \Theta(g(x))$.

(c) If we restrict x to positive integers greater than 4, then the inequality $x^2 < 2^x$ can be proven using the principle of mathematical induction (to be studied later). To prove the inequality for all real values of x greater than 4, one can use the calculus of limits and L'Hôpital's Rule.

Quantifiers

Example: The two statements below contains quantifiers of two different types:

(a) There exists an element x inside $\mathbb{N}$ such that x is perfect.
(b) For all elements x inside $\mathbb{Z}$ there exists an element y inside $\mathbb{Z}$ such that $x + y = 0$.
(c) Euclid's Division Theorem: For all positive integers n, all non-negative integers m, there exists non-negative integers q and r such that $m = qn + r$ with $0 \le r < n$.

Standard Notation for Quantification

$\exists$ - Existential quantifier ("There exists")
$\forall$ - Universal quantifier ("For all")

Example: The statements in the previous example can be rewritten using symbols:

(a) $\exists x \in \mathbb{N}, x$ is perfect
(b) $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, x + y = 0$
(c) $\forall n \in \mathbb{Z}^+ (\forall m \in \mathbb{N} (\exists q \in \mathbb{N} (\exists r \in \mathbb{N} ((r < n) \wedge (m = nq + r)))))$

Statements About Variables

Given variables in a statement, we can introduce additional variables to concisely describe conditions about them.

Definition: Let U denote a universe for a variable x (e.g. $\mathbb{N}$, $\mathbb{Z}$) and $p(x)$ be a statement about x.

(a) We shall write $\forall x \in U(p(x))$ to denote $\forall x \in U, p(x)$.
(b) We shall write $\exists x \in U(p(x))$ to denote $\exists x \in U, p(x)$.

Example:

(a) Define $p(n)$ to be the statement '$n^2 \geq n$'. Then the statements '$\forall n \in \mathbb{N},\ n^2 \geq n$' and '$\forall n \in \mathbb{N}(p(n))$' are equivalent.

(b) Define $p(n)$ to be the statement '$m = nq + r$ with $0 \leq r < n$'. Then Euclid's Division Theorem can be expressed in symbols as '$\forall n \in \mathbb{Z}^+(\forall m \in \mathbb{N}(\exists q \in \mathbb{N}(\exists r \in \mathbb{N}(p(n,m,q,r)))))$'.

Rewriting Statements to Encompass Larger or Smaller Universes

Sometimes it is necessary to rewrite quantified statements to encompass a larger or smaller universe.

Example: Suppose in one programming language the universe $\mathbb{Q}$ (rational numbers) is defined but in another only $\mathbb{Z}$ is defined. How can we rewrite the statement $\exists x \in \mathbb{Q}(x = 1/x)$ to involve the smaller universe $\mathbb{Z}$?

Solution: $\exists m \in \mathbb{Z}(\exists n \in \mathbb{Z}((n \neq 0) \wedge (m/n = n/m)))$

Example: Translate the two statements below to encompass the larger universe $\mathbb{R}$:

(a) $\forall x \in \mathbb{R}^+(x > 1)$

(b) $\exists x \in \mathbb{R}^+(x > 1)$

Solution: Since $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$, we have

(a) $\forall x \in \mathbb{R}(x > 0 \Rightarrow x > 1)$

(b) $\exists x \in \mathbb{R}(x > 0 \wedge x > 1)$

Theorem: Let U_1 be a sub-universe of U_2, i.e. $U_1 \subseteq U_2$. Suppose $q(x)$ is a statement such that $U_1 = \{x \mid q(x) \text{ is true}\}$ and $p(x)$ is a statement about U_2. Then $p(x)$ can also be interpreted as a statement about U_1 and moreover,

(a) $\forall x \in U_1(p(x))$ is equivalent to $\forall x \in U_2(q(x) \Rightarrow p(x))$

(b) $\exists x \in U_1(p(x))$ is equivalent to $\exists x \in U_2(q(x) \wedge p(x))$

Proving Quantified Statements True or False

Example: Determine whether or not the following statements are true:

a) $\exists x \in \mathbb{N}$, x is perfect

b) $\forall x \in \mathbb{Z},\ \exists y \in \mathbb{Z},\ x + y = 0$

Solution:

a) Let $x = 6$. Since the proper divisors of 6 are 1, 2, 3, we have $1 + 2 + 3 = 6$. Therefore, x is perfect. Thus, the statement is true.

b) Let $x \in \mathbb{Z}$. Set $y = -x$. Then $x + y = x + (-x) = 0$. Thus, the statement is true.

Negation of Quantified Statements

Consider the following statements involving negative quantifiers:

- Not all integers are prime
- There is no integer that is both even and odd

Sometimes it is easier to prove such statements by converting them to an equivalent statement where the negation is passed through to the assertions of the statement:

- There exists an integer that is composite
- All integers are either odd or even

Theorem:
(a) $\neg(\exists x \in U,\ p(x))$ is equivalent to $\forall x \in U,\ \neg p(x)$
(b) $\neg(\forall x \in U,\ p(x))$ is equivalent to $\exists x \in U,\ \neg p(x)$

Example:

a) $\neg(\exists x \in \mathbb{Z}, x \text{ is even and } x \mid 15) = \forall x \in \mathbb{Z},\ \neg(x \text{ is even and } x \mid 15)$
$= \forall x \in \mathbb{Z},\ \neg(x \text{ is even}) \text{ or } \neg(x \mid 15)$ (DeMorgan's Law)
$= \forall x \in \mathbb{Z},\ (x \text{ is odd or } x \nmid 15)$

b) $\neg(\forall x \in \mathbb{Z}, x \text{ is prime}) = \exists x \in \mathbb{Z},\ \neg(x \text{ is prime}) = \exists x \in \mathbb{Z},\ (x \text{ is composite})$

Implicit Quantification

Example: Consider the statement S = "The sum of two even integers is even", which implicitly involves quantifiers. We can rewrite it in the form of a quantified statement as follows. Define $p(n)$ to be the statement "n is even". Then S is equivalent to

$$\forall m \in \mathbb{Z}(\forall n \in \mathbb{Z}(p(m) \wedge p(n) \Rightarrow p(m+n)))$$

or, if we make explicit the definition of an even integer,

$$\forall m \in \mathbb{Z}(\forall n \in \mathbb{Z}((\exists j \in \mathbb{Z}(m = 2j)) \wedge (\exists k \in \mathbb{Z}(n = 2k)) \Rightarrow ((\exists l \in \mathbb{Z}(m+n = 2l)))))$$

3.3 Inference

Direct Inference and Proofs

Principle of Direct Inference (Modus Ponens): From p and $p \Rightarrow q$, we may conclude q.

Example: Consider the statement '$\overbrace{n \text{ is an even integer}}^{p} \Rightarrow \overbrace{n^2 \text{ is an even integer}}^{q}$. Suppose we set $\overbrace{n = 4}^{p}$. Then given that $p \Rightarrow q$ is true (which we will prove later), it follows from direct inference that $\overbrace{n^2 = 16}^{q}$ must be even (so that there is no need to explicitly verify this).

Rules of Inference for Direct Proofs

We make certain inferences when proving mathematical statements, which can be formalized into rules. Consider the following example.

Example: Give a direct proof of the statement: If m is an even integer, then m^2 is an even integer, or in symbols, $\forall m \in \mathbb{Z}(p(m) \Rightarrow p(m^2))$, where $p(m)$ denotes the statement 'm is even'.

NOTE: We make use of the definition: m even $\Leftrightarrow$ there exists an integer k such that $m = 2k$.

Proof: Let m be an integer. Suppose that m is even. By definition, m is even if and only if there is an integer k with $m = 2k$. It follows by modus ponens there is an integer k such that $m = 2k$. Thus, by squaring this equation, we have that there is an integer k such that $m^2 = 4k^2$. Therefore, there is an integer $h = 2k^2$ (introducing a name for $2k^2$) such that $m^2 = 2h$. Again, by modus ponens (definition of an even integer), m^2 is even. Therefore, we have proven that for all integers m, if m is even, then m^2 is even.

Some Rules of Inference (see textbook for all rules):

RULE 6: (Modus ponens) From $p(x)$ and $p(x) \Rightarrow q(x)$, we may conclude $q(x)$.

RULE 8: If we can derive $q(x)$ from the hypothesis that x satisfies $p(x)$, we may conclude $p(x) \Rightarrow q(x)$.

RULE 9: If we can derive $p(x)$ from the hypothesis that x is a (generic) member of our universe U, we may conclude $\forall x \in U(p(x))$.

Indirect Proofs

Contrapositive Rule of Inference

p	q	$p \Rightarrow q$	$\neg q$	$\neg p$	$\neg q \Rightarrow \neg p$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Example: Consider the two statements, which we would say are equivalent to each other:
(a) If the sky rains, then the ground is wet.
(b) Contrapositive: If the ground is dry (NOT wet), then the sky did NOT rain.
The second statement is called the contrapositive of the first, forms the first rule of inference.

Theorem: The statement '$p \Rightarrow q$' is equivalent to '$\neg q \Rightarrow \neg p$' (contrapositive).

RULE 11: (Contrapositive) From $\neg q(x) \Rightarrow \neg p(x)$ we may conclude $p(x) \Rightarrow q(x)$.

RULE 11(b): (Modus tollens) From $p(x) \Rightarrow q(x)$ and $\neg q(x)$ we may conclude $\neg p(x)$.

Example: Let m and n be integers. Prove that if $m+n \geq 100$, then $m \geq 50$ or $n \geq 50$.

Proof: (by contraposition) Let $p(x)$ denote the statement $m+n \geq 100$ and $q(x)$ be the statement $m \geq 50$ or $n \geq 50$. Then

$\neg p(x) = \neg(m+n \geq 100) = m+n < 100$

$\neg q(x) = \neg(m \geq 50 \text{ or } n \geq 50) = \neg(m \geq 50) \text{ and } \neg(n \geq 50) = m < 50 \text{ and } n < 50$

Using contraposition, suppose that $m < 50$ and $n < 50$. Then

$$m+n < 50+50 = 100.$$

This completes the proof.

NOTE: The statement $q(x) \Rightarrow p(x)$ (called the converse) is NOT true in this example. Consider the counterexample: $m = 70$, $n = 20$ but $m+n = 90$ (less than 100).

Proof by Contradiction or Reduction to Absurdum (reductio ad absurdum)

The Principle of the Excluded Middle claims that a statement $r(x)$ is either true or false, exclusively, i.e. $r(x)$ cannot be both true and false. This is the basis for the technique of proof by contradiction.

RULE 12: (Contradiction) If from assuming $p(x)$ and $\neg q(x)$, we can derive both $r(x)$ and $\neg r(x)$ for some statement $r(x)$, we may conclude $p(x) \Rightarrow q(x)$.

Example: Prove that $\sqrt{2}$ is irrational, i.e. if $x^2 = 2$, then x is irrational.

Proof: (By contradiction) Suppose on the contrary that $x = \sqrt{2}$ is rational (NOT q). Then $\sqrt{2}$ can be expressed a fraction in lowest terms, i.e. $\sqrt{2} = m/n$, where m and n are relatively prime integers (no common factor greater than 1). Squaring both sides yields $2 = m^2/n^2$, or $m^2 = 2n^2$. This shows that m^2 is even and thus m must also be even (see previous example). Write $m = 2k$ so that

$$2n^2 = m^2 = (2k)^2 = 4k^2$$

$$\Rightarrow n^2 = 2k^2$$

By the same argument, we conclude that n^2, and thus n, must be even. But then m and n are not relatively prime integers since they have 2 as a common factor (being both even). This is absurd since it contradicts the assumption that m and n *are* relatively prime. Hence, the assumption that $\sqrt{2}$ cannot be true (since it leads to a contradiction) and thus $\sqrt{2}$ must be irrational.

NOTE: Why isn't a proof by contraposition useful here?

Contraposition or Contradiction: When to use which?

1. In a proof by contraposition, you know exactly what you need to prove, but it may be more difficult to prove.
2. In a proof by contradiction, you don't know in advance what the contradiction will be, but it may be easier to prove.