Discrete Mathematics

Contents

1 Sets

1.1 Set definition

A set is an unordered collection of distinct objects. A set can be defined by a list of its members $A = \{1, 2, 3\}$ or using set comprehensions

$$A = \{x \mid \text{predicate on } x\}$$

For example $\{2x \mid x \in \mathbb{Z}\}$ is the set of even numbers, as is $\{x \in \mathbb{Z} \mid x/2 \in \mathbb{Z}\}$.

1.2 Standard Sets

Some standard sets include

1. $\emptyset = \{\}$ – The empty set
2. $\mathbb{N} = \{0, 1, 2 \ldots\}$ – The natural numbers (including 0)
3. $\mathbb{N}_+ = \{1, 2, 3 \ldots\}$ – The natural numbers excluding 0
4. $\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2 \ldots\}$ – The integers
5. $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ – The integers modulo n where $n \in \mathbb{N}$ and $n \geq 2$
6. $\mathbb{Q} = \{\frac{n}{d} \mid n \in \mathbb{Z} \text{ and } d \in \mathbb{N}_+\}$ – The rational numbers
7. $\mathbb{R}$ – The real numbers
8. $\mathcal{U}$ – The Universal set. This can be redefined depending on the sets of numbers in use.
9. Intervals are subsets of $\mathbb{R}$. Square brackets indicate that the limit is included, parentheses indicate that the limit is not.
   $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$
   $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$
   $(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$
   $[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$
   $(-\infty, b] = \{x \in \mathbb{R} \mid x \leq b\}$
   $(-\infty, b) = \{x \in \mathbb{R} \mid x < b\}$
   $(a, \infty) = \{x \in \mathbb{R} \mid x > a\}$
   $[a, \infty) = \{x \in \mathbb{R} \mid x \leq a\}$

1.3 Comparing Sets

For the sets A and B

- If two sets are identical, then $A = B$.
- If A is contained within B then $A \subseteq B$
- If A is contained within B *and* B has extra elements, then $A \subset B$

1.4 Set Operations

- $A \cup B$ is the set containing all the elements in A or B. Using set comprehensions, this is $\{x \mid x \in A \text{ or } x \in B\}$. This can be extended to a list of sets $A_1, A_2, \ldots, A_n$ as

$$\bigcup_{i=1}^{n} A_i = \{x \mid x \in A_i \text{ for some } i\}$$

This can also be extended to an infinite list of sets.

- $A \cap B$ is the set containing all the elements in A and B. Using set comprehensions, this is $\{x \mid x \in A \text{ and } x \in B\}$. This can be extended to a list of sets $A_1, A_2, \ldots, A_n$ as

$$\bigcap_{i=1}^{n} A_i = \{x \mid x \in A_i \text{ for every } i\}$$

  This can also be extended to an infinite list of sets.
- $A \setminus B$ is the set containing all the elements in A and not B. Using set comprehensions, this is $\{x \mid x \in A, x \notin B\}$
- $A \oplus B$ is the set containing all the elements in A or B, but not the elements in A and B. Using set comprehensions, this is $\{x \mid x \in A, x \in B, x \notin (A \cap B)\}$. This may also be written as $A \Delta B$ or $A \triangle B$.
- $A \times B$ is the set containing the possible pairs of elements from A and B. Using set comprehensions, this is $\{(x, y) \mid x \in A, y \in B\}$. This can be extended to n sets forming tuples of size n. $\times_{i=1}^{n}$. This is different to $(A \times B) \times C$ which in turn is different to $A \times (B \times C)$.
- A^c or $\bar{A}$ or A' is the set containing the elements not in A, but in $\mathcal{U}$. Using set comprehensions, this is $\{x \mid x \notin A\}$, (under the assumption that all things under consideration are members of the universe).
- $|A|$ is the size or cardinality of A. $\#A$ may also be used.
- $\mathcal{P}(A)$ is the power set, or set of all subsets of A. Using set comprehensions, this is $\{B \mid B \subseteq A\}$. For a set $|A| = n$, $|\mathcal{P}(A)| = 2^n$.

1.5 Algebraic Laws

For the sets A, B and C:

Idempotence $A \cup A = A$
$A \cap A = A$
Commutative $A \cup B = B \cup A$
$A \cap B = B \cap A$
Associative $(A \cup B) \cup C = A \cup (B \cup C)$
$(A \cap B) \cap C = A \cap (B \cap C)$
Distributive $A \cup (B \cap C) = (A \cap B) \cup (A \cap C)$
$A \cap (B \cup C) = (A \cup B) \cap (A \cup C)$
One and Zero $A \cup \emptyset = A$
$A \cap \emptyset = \emptyset$
Cancellation $A \setminus A = \emptyset$
$A \setminus \emptyset = A$
Involution $A \setminus (A \setminus B) = A \cap B$
De Morgan's $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
$A \setminus (B \cap C) = (A \setminus) \cup (A \setminus C)$
Right-Distributive $(A \cup B) \setminus C = (A \setminus C) \cup (A \setminus B)$
$(A \cap B) \setminus C = (A \setminus C) \cap (A \setminus B)$

2 Functions

2.1 Definition

A function is made up of its domain, co-domain and map. The domain is the set the function draws from as its input, the co-domain is the set of possible outputs, and the map describes the way the function acts upon its input to produce an output. A function f is usually defined in two parts. $f : A \to B$ where A and B are the domain and co-domain respectively. Then $f(x) = \ldots$ is the map.

Two functions, f and g are equal if their domains, co-domains and map are all equivalent. As a trivial example, $f(x) = 2x$ and $g(x) = x + x$ are equivalent.

2.2 Function Set Laws

A partial function maps every element of its domain to at most one element of B – or not every element of the domain is mapped to the codomain. For example, $1/x$ is a partial function as it is not defined for $x = 0$

For a function $f : A \to B$, the image of the function is given as $\{b \in B \mid b = f(a) \text{ for each } a \in A\}$ or, more succinctly $\{f(a) \mid a \in A\}$

A function is *onto* if every element of B is a possible output from f or $\text{Im}(f) = B$. More formally, this is $\forall b \in B(\exists a \in A : f(a) = b)$. This may also be referred to as a surjective function, or a surjection.

A function is *1-1* if no two different elements of the domain produce the same output. More formally, $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2), \forall a_1, a_2 \in A$. This may also be referred to as an injective function, or an injection.

If a function is both onto and 1-1, it is a bijective function, or a bijection.

2.3 Function Composition

If $f : A \to B$ and $g : B \to C$ then their composition is given as $g \circ f : A \to C$ and can be thought of as "g after f" or $g(f(x))$. The set B associated with f and the set B associated with g must match exactly, otherwisethe function is invalid. Additionally, even if $g \circ f$ and $f \circ g$ map the same sets onto each other, this does not mean that they are the same. For example, $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2; g : \mathbb{R} \to \mathbb{R}, g(x) = \sin x$ then $f \circ g : \mathbb{R} \to \mathbb{R}$ and $f(g(x)) = \sin^2 x$ but $g \circ f : \mathbb{R} \to \mathbb{R}$ and $g(f(x)) = \sin x^2$. Composition is therefore *not always* commutative, but in some cases can be. Composition can be seen to be associative, i.e. $(f \circ g) \circ h = f \circ (g \circ h)$

2.4 Inverse Functions

A function $f : A \to B$ has an inverse $f^{-1} : B \to A$ iff it is bijective.

2.5 Binary Functions and their Properties

Binary operators are commonly written infix $(x \cdot y)$ and are defined as $\cdot : A \times A \to A$. For example, $+$ is a binary operator, defined as $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$. The generic binary operator $\cdot$ operating on A is:

- idempotent if $x \cdot x = x; \forall x \in A$
- commutative if $x \cdot y = y \cdot x; \forall x, y \in A$
- associative if $(x \cdot y) \cdot z = x \cdot (y \cdot z); \forall x, y, z \in A$
- has an identity if $\exists e \in A \mid x \cdot e = e \cdot x = x; \forall x \in A$

3 Counting

3.1 Laws of Sum and Product

These laws all dervie from the fact that, for the sets A and B, $|A \cup B = |A| + |B|$ where $A \cap B = \emptyset$, $|A \setminus B| = |A| - |B|$ and $|A \times B| = |A||B|$

3.1.1 Addition

Assuming the properties P_1 and P_2 are exclusive, then the number of elements in a set satifsfying P_1 or P_2 is the sum of the elements satisfying P_1 plus the number of elements satisfying P_2.

3.1.2 Subtraction

Assuming that, in order for P_2 to be true, P_1 must be as well, but P_1 can be true without P_2, then the number of elements in a set satisfying P_1 but not P_2 is the number satisfying P_1 minus the number satisfying P_2.

3.1.3 Multiplication

Given a series of independent choices, then the total number of choices at each stage is the product of all the previous choices.

3.2 Arrangements of n objects

The number of arrangements of the n objects

$$\underbrace{x_1, x_1, x_1 \ldots, x_1}_{m_1 \text{ times}}, \underbrace{x_2, x_2, x_2 \ldots, x_2}_{m_2 \text{ times}}, \ldots, \underbrace{x_k, x_k, x_k \ldots, x_k}_{m_k \text{ times}}$$

where x_i appears m_i times is

$$\frac{n!}{m_1! m_2! \ldots m_k!}$$

If just 2 tpes of object are present (or two states are to be used, i.e. chosen and unchosen), then the binomial co-efficient may be used. $m_1 + m_2 = n \Rightarrow = \frac{n!}{m_1! m_2!} \binom{n}{m_1} = \binom{n}{m_2}$

3.2.1 Vandermonde's Identity

$$\binom{m+n}{k} = \sum_{j=0}^{k} \binom{m}{j} \binom{n}{k-j}$$

where $\binom{m}{j} = 0$ for $j > m$.

3.3 Double Counting

It may be easier to count twice and remove elements than try counting distinct elements. For example, to count factors of 3 and 5, it is easier to add the number of factors of 3 and the number of factors of 5 and remove the factors of 15. It also prevents undercounting. This can be generalised to the inclusion-exclusion formula, also seen in probability.

$$\begin{aligned} |A_1 \cup A_2 \cup \ldots \cup A_n| = \quad & (|A_1| + |A_2| + \ldots + |A_n|) \\ & - (|A_1 \cap A_2| + \ldots + |A_{n-1} \cap A_n|) \\ & \ldots \\ & + (-1)^n |A_1 \cap A_2 \cap + \ldots + A_n| \end{aligned}$$

Or

$$\left| \bigcup_{1 \le i \le n} A_i \right| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| + \ldots + (-1)^n \left| \bigcap_{1 \le i \le n} A_i \right|$$

4 Relations

4.1 Definition

A relation R on a set A is a subset of $A \times A$ and can be expressed as $R = \{(a, a') \mid a \in A, P(a, a')\}$ where a' may be an element of A or a function on $a \in A$. Relations are normally written as $a\,R\,b$ if $(a, b) \in R$. Similarly, $a \not R b$ indicates that the pair $(a, b) \notin R$

4.2 Properties

A relation R on a set A can have the following properties:

- reflexive $\Leftrightarrow a\,R\,a\ \forall a \in A$
- symmetric $\Leftrightarrow a\,R\,b \Rightarrow b\,R\,a\ \forall a, b \in A$
- antisymmetric $\Leftrightarrow a\,R\,b$ and $b\,R\,a \Rightarrow b = a\ \forall a, b \in A$
- transitive $\Leftrightarrow a\,R\,b$ and $b\,R\,c \Rightarrow a\,R\,c\ \forall a, b, c \in A$
- irreflexive $\Leftrightarrow a \not R a\ \forall a \in A$
- serial $\Leftrightarrow \forall a \in A\,(\exists b \in A \mid a\,R\,b)$

4.3 Equivalence Relations

An equivalence relation on A must be reflexive, transitive and symmetric. $[a] = \{a' \in A \mid a' \sim a\}$ defines equivalence classes on A.

4.3.1 Example

Taken from problem sheet 3:

Let $m \sim n$ be an equivalence relation defined on $\{x \mid x \in \mathbb{Z}, 1 \le x \le 16\}$ as $m \sim n$ if $n = 2^k m$ for some $k \in \mathbb{Z}$.

To prove $\sim$ is an equivalence relation, we must show $\sim$ is relexive, transitive and symmetric.

$a \sim a\ \forall a \in A$ as $a = 2^0 a$

$a \sim b \Rightarrow b\,R\,a\ \forall a, b \in A$ as $a \sim b \Rightarrow a = 2^k b$ so $b = 2^{-k} a$

$a \sim b$ and $b \sim c \Rightarrow a \sim c$ as $a = 2^k b$ and $b = 2^l c \Rightarrow a = 2^k 2^l c$

The equivalence classes are given as follows: $2\ [1] = \{1, 2, 4, 8, 16\}$
$[3] = \{3, 6, 12\}$
$[5] = \{5, 10\}$
$[7] = \{7, 14\}$
$[9] = \{9\}$
$[11] = \{11\}$
$[13] = \{13\}$
$[15] = \{15\}$

4.4 Operations

4.4.1 Converse

For a relation R on A, the *converse* is the relation, such that, given $a\,R\,b$, $b\,R^{-1}\,a$ holds.

4.4.2 Composition

For the relations R and S on A, the composition $a(S \circ R)b$ exists if there is some x such that $a\,R\,x$ and xSb holds.

4.4.3 Closure

The transitive closure R^+ exists if, for some collection of $x_0, x_1, \ldots x_{n-1}, x_n$ with $n \ge 1$ such that $x_0\,R\,x_1, x_1\,R\,x_2 \ldots x_{n-1}\,R\,x_n$.

The reflexive transitive closure R^* is similarly defined, but with $n \ge 0$, or the initial element can be related to itself.

4.5 Drawing Relations

Relations can be drawn using digraphs, where each node is an element of the set A and each connection is an element of the set R. Composite relations can be shown by labelling each edge and allows you to easily determine the set defined by the relation.

4.6 Counting Relations

On a set A with size n, the total number of relations is 2^{n^2}. The number of symmetric relations is $2^{\frac{n(n+1)}{2}}$. The total number of antisymmetric relations is $2^n 3^{\binom{n}{2}}$

4.7 Partitions

4.7.1 Definition

A partition of a set A is a collection of subsets with an indexing set I satisfying the following:

- $\bigcup_{i \in I} B_i = A$
- $B_i \cap B_j = \emptyset$ for $i \ne j$ (i.e. pairwise disjoint)
- $B_i \ne \emptyset, \forall i \in I$

5 Sequences

5.1 Definition

A function whose domain is $\mathbb{N}$, with the argument of the function written as a subscript (i.e. f_n), and can also be used to model the time complexity of a function. In this case, the subscript notation may be dropped and brackets used as usual (i.e. $T(n)$ instead of t_n).

A sequence will have boundary conditions, either as given numerical constants, in the case of the Fibonacci sequence, for example; or as limits, such as N in the gambler's ruin problem.

Recursively defined sequences are defined in terms of lower steps in the sequence, and solving these recurrence relations yields a function in terms of n (or whatever letter is used to denote each term).

There are also a number of special sequences which you are expected to know. The Bell numbers are the number of partitions of a set. For a set of size $(n+1)$, the $(n+1)^{\text{th}}$ Bell number, B_{n+1} is given as

$$B_{n+1} = \sum_{i=0}^{n} \binom{n}{i} B_i$$

where the smallest Bell number, $B_0 = 1$ (trivial as the only partition of the empty set is the empty set). The associated proof looks at the size of each of the partitions and the number of each size of partition.

The number of derangements of n objects is given as $d_1 = 0$, $d_2 = 1$ and $d_n = (d_{n-1} + d_{n-2})$ for $n \geq 2$. This can be explained as, for n objects, swapping n to i causes there to be $n-1$ options for i and two mutually exclusive cases: swapping n and i leads to the first $n-1$ objects forming a derangement or not. There are d_{n-1} ways the former can happen and d_{n-1} options for the latter, hence the equation for d_n.

6 Modular Arithemtic

6.1 Definition

Let $x \pmod n$ be a function that finds the remainder of $x \div n$.

Begin by taking a relation on $\mathbb{Z}$, such that, for some $n \in \mathbb{N}, x \equiv y \pmod n$ if $n \mid (x-y)$.

6.2 Properties

If $x_1 \equiv x_2 \pmod n$ and $y_1 \equiv y_2 \pmod n$ then $x_1 + y_1 \equiv (x_2 + y_2) \pmod n$ and $x_1 y_1 = (x_2 y_2) \pmod n$.

If $x_1 \equiv x_2 \pmod n$ and $y \in \mathbb{Z}$ then $x_1^y \equiv (x_2^y) \pmod n$.

These two properties can be combined to solve problems such as $2^{600} \pmod{11}$ by a series of reductions.

$$\begin{aligned}
2^{600} &\equiv 4^{300} && \equiv 16^{150} && \equiv 5^{150} && \pmod{11}\\
&\equiv 25^{75} && \equiv 3^{75} && \equiv 3 \cdot 9^{37} && \pmod{11}\\
&\equiv 3 \cdot 9 \cdot 81^{18} && \equiv 27 \cdot 4^{18} && \equiv 5 \cdot 4^{18} && \pmod{11}\\
&\equiv 5 \cdot 16^{9} && \equiv 5 \cdot 5^{9} && \equiv 25^{5} && \pmod{11}\\
&\equiv 3^{5} && \equiv 3 \cdot 9^{2} && \equiv 3 \cdot 4 && \pmod{11}\\
&\equiv 12 && \equiv 1 && && \pmod{11}
\end{aligned}$$

7 Asymptotic Notation

7.1 Big-O Notation

For two functions $f, g : \mathbb{R} \to \mathbb{R}$, we say that $f(x) = O(g(x))$ (f is *asymptotically bounded* by g) if $\exists c \in \mathbb{R}$ and $N \in \mathbb{N}$ such that $|f(n)| \leq c\,|g(n)| \ \forall n \geq N$.

7.2 Big-Omega Notation

For two functions $f, g : \mathbb{R} \to \mathbb{R}$, we say that $f(x) = \Omega(g(x))$ (f *asymptotically bounds* g) if $\exists c \in \mathbb{R}$ and $N \in \mathbb{N}$ such that $|f(n)| \geq c\,|g(n)| \ \forall n \geq N$.

7.3 Big-Theta Notation

Big-Theta can be though of as a stricter bound on two functions, and is only used if $f(n) = O(g(n))$ and $g(n) = O(f(n))$.

7.4 The Master Theorem

For the recurrence $t_n = a t_{\frac{n}{b}} + f(n)$ where $a, b \in \mathbb{R}; n \in \mathbb{N}$ and $t_{\frac{n}{b}}$ can be thought of as $t_{\lfloor \frac{n}{b} \rfloor}$ or $t_{\lceil \frac{n}{b} \rceil}$ then

- If $f(n) = O(n^k)$ with $k < \log_b a$ then $t_n = \Theta(n^{\log_b a})$
- If $f(n) = \Theta(n^k)$ with $k = \log_b a$, then $t_n = \Theta(n^{\log_b a} \log n)$
- If $f(n) = \Omega(n^k)$ with $k > \log_b a$, then $t_n = \Theta(f(n))$

8 Orders

8.1 Definition

These are types of relation that focus on the idea of one object being comparable and therefore slightly more intuitive.

There are three types of order:

1. Pre-order: reflexive and transitive relation
2. Partial order: antisymmetric and inherits from pre-order
3. Linear order: antisymmetric, transitive relation with totality (that is, where D is the domain of the relation, $\forall x, y \in D, x\,R\,y$ or $y\,R\,x$.)

For $\preceq$ as an order on A, $x, y \in A$ are said to be comparable if $x \preceq y$ or $y \preceq x$, otherwise, they are incomparable. When $\preceq$ is a partial order on A, for the subset $S \subseteq A$, we say it is a chain if $\forall x, y \in S$, $x \preceq y$ or $y \preceq x$; and an antichain if $\forall x, y \in S$, $x \npreceq y$ and $y \npreceq x$.

8.2 Ordering Cartesian products

There are two methods for ordering Cartesian products: lexicographic order and product order.

For the order $\preceq$ on A, the lexicographic order on $A \times A$ is given as $(x, y) \preceq_L (x', y') \Leftrightarrow x \prec x'$ or $(x = x')$ and $y \preceq y'$. If $\preceq$ is a pre-, partial or linear order on A, then $\preceq_L$ is also a pre-,partial or linear order on $A \times A$.

For the order $\preceq$ on A, the product order on $A \times A$ is given as $(x, y) \preceq_P (x', y') \Leftrightarrow x \preceq x'$ and $y \preceq y'$. If $\preceq$ is a pre-, or partial order on A, then $\preceq_L$ is also a pre-, or partial order on $A \times A$, but the property of being a linear order is not necessarily conserved. $\preceq_P$ can be thought of as being more strict than $\preceq_L$ as $(x, y) \preceq_P (x', y') \Rightarrow (x, y) \preceq_L (x', y')$ but not vice versa.

8.3 Drawing Orders

Orders are drawn top-to-bottom, with the "largest" entry at the top, and the "smallest" at the bottom. If a is connected to b, the element a can be thought of as being the larger element if it is above b, and also that there is no element x such that $a \preceq x \preceq b$. If there is an element x such that $a \preceq x \preceq b$, then a is connected to x which is connected to b, without a direct connection between a and b, as this can be deduced through the transitive property of orders.

8.4 Bounds

m is the upper bound of a set A compared with $\preceq$ if, $\forall x \in A, x \preceq m$; similarly m is a lower bound if $m \preceq x$. *m does not have to be in A*

m is the maximum of a set A compared with $\preceq$ if, $\forall x \in A, x \preceq m$ and $m \in A$; similarly, m is a minimum if $m \preceq x$. *m must be in A.*

The least upper bound is the lowest value that is also an upper bound. For example, using the order $\leq$ on the set $[0, 2]$, the set of upper bounds is $[2, \infty)$, with the least upper bound being 2. For m as the least upper bound on A, we write this as $m = \operatorname{lub} A$, similarly for the greatest lower bound, we write $m = \operatorname{glb} A$.

9 Methods of Proof

9.1 Proof by Contrapositive

If asked to prove $A \Rightarrow B$, it is often easier to try and prove $\neg B \Rightarrow \neg A$. For example, it may be easier to prove "it is raining, so there are clouds overhead" by stating "there are no clouds overhead, so it is not raining".

9.2 Proof by Contradiction

In a similar vein to the proof by contrapositive, it may be easier to prove $A \Rightarrow B$ by supposing A is false and proving a contradiction.

The proof of $\sqrt{2} \notin \mathbb{Q}$ is often proven using contradiction. Additionally, each case must be shown to be contradictory for a proof by contradiction to hold. Some schools of thought believe that proof by contradiciton should be avoided unless absolutely necessary.

9.3 Proof by Induction

The statement $S(n)$ is a statement involving the natural number n. To prove that $S(n)$ $\forall n \in \mathbb{N}$, we must show that $S(0)$ holds (the base case), and that $S(k+1)$ is true whenever $S(k)$ is true (the inductive hypothesis). As the natural numbers are defined as either 0 or Suc(k), the case $S(n)$ will be true eventually.

In order to prove something in the form $S(k) \Rightarrow S(k+2)$, two base cases must be proven, $S(0)$ and $S(1)$, however, proofs of this type are less commonly seen.

9.4 Proof by Strong Induction

For the statement $S(n)$, proving $S(0)$ and $S(j)$ for all $j \leq k$, this also proves $S(k+1)$ and hence $S(n)$ $\forall n \in \mathbb{N}$.

9.5 Proof by Minimal Counter-example

Using a similar reasoning to proof by contradiction, a statement is assumed to be false, for a minimal n. By a series of steps, a "smaller" n is usually found, thus giving a contradiction. Therefore, the original statement is true.

9.6 The Pigeonhole Principle

For some i holes, it is not possible to fit more than i values into said holes without overlap.

In principle, this is most often used to prove that for a set of n numbers with at most m possible values where $m < n$ implies that at least two values must be equal.

9.7 Proving statements in the form $\exists x \forall y.P$

In this case, it is often easiest to find values for x and show that they hold for all y. However, the value for x may not be immediately apparent, so a series of steps must be followed to obtain it. In this case the proof must either be constructed backwards (using $\Leftarrow$) or the proof must be able to be followed in both directions $\Leftrightarrow$. This method is often used to prove that $f(x) = O(g(x))$ by showing that c and N exist for $|f(n)| \leq c\,|g(n)|\,, \forall n \geq N$.

9.8 Proving statements in the form $\forall x \exists y.P$

The examples given often feature the negation of this statement ($\forall x \nexists y.P$). It's often easiest to attempt a proof by contradiction: y does (or does not) exist and then derive a contradiction.