Discrete Mathematics (Part B)

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

Computer Science Tripos Part 1A
Mathematics Tripos 1A (CS Option)

Glynn Winskel

Lent 2002

William Gates Building
JJ Thomson Avenue
Cambridge
CB3 0FD

http://www.cl.cam.ac.uk/

Introduction

This course will develop the idea of formal proof by way of examples involving simple objects such as integers and sets. The material enables academic study of Computer Science and will be promoted with examples from the analysis of algorithms and cryptography.

Syllabus

These notes cover the second half of the course.

Sets, relations and functions

- Sets, subsets and Boolean operations. Indicator (characteristic) functions and their algebra. Principle of inclusion-exclusion, with applications to Euler's function. Boolean logic. [2 lectures]
- Binary relations. Composition of relations. Equivalence relations and quotients of sets. Closures and Warshall's algorithm. Partial orders and total orders. Hasse diagrams. Well founded relations and well ordering. Well founded induction. [3 lectures]
- Functions; Injective, surjective and bijective functions. Numbers of such functions between sets. Sorting. The Schröder-Bernstein theorem. Countability. A countable union of countable sets is countable. The uncountability of $\mathbb{R}$. Existence of transcendental numbers. [3 lectures]

The course and these notes are based on the course previously given by Peter Robinson.

Objectives

On completing the course, students should be able to:

- Analyse problems using set theory.
- Explain and use the principle of inclusion and exclusion.
- Recognise relations and discuss their properties.
- Describe and analyse Warshall's algorithm.
- State, prove and apply the Schröder-Bernstein theorem.
- Differentiate countable and uncountable sets.

These notes do not constitute a complete transcript of all the lectures and they are not a substitute for text books. They are intended to give a reasonable synopsis of the subjects discussed, but they give neither complete proofs of all the theorems nor all the background material.

Sets

A set is just a collection of objects, or *elements*. We write $x \in \mathrm{A}$ when an element x is in the set A and $x \notin \mathrm{A}$ when it isn't.

Sets can be finite or infinite. (Indeed, there are many different infinite sizes.) If they are finite, you can define them explicitly by listing their elements, otherwise a pattern or restriction can be used:

$\mathrm{L} = \{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$
$\mathrm{M} = \{\mathrm{alpha}, \mathrm{bravo}, \mathrm{charlie}\}$
$\mathbb{N} = \{1, 2, 3, \ldots\}$
$\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$
$\mathrm{P} = \{x \in \mathbb{N} \mid x > 1 \text{ and } 1 < y < x \Rightarrow (x, y) = 1\}$

Given a finite set, A, write $|\mathrm{A}|$ for the number of elements in A.

Write $\varnothing$ for the empty set, $\{\}$. So $|\varnothing| = 0$.

One set, A, is a *subset* of another set, B, if every element of A is also a member of B. We write this with a rounded less-than-or-equal sign: $\mathrm{A} \subseteq \mathrm{B}$. So $\mathbb{N} \subseteq \mathbb{Z}$. When the containment is strict (as in this case), we write $\mathbb{N} \subset \mathbb{Z}$ for a *proper* subset.

Two sets, A and B, are equal if they contain the same elements. This will often be proved by showing that each is a subset of the other: $\mathrm{A} \subseteq \mathrm{B}$ and $\mathrm{B} \subseteq \mathrm{A}$.

Sets can themselves be members of other sets. There is an important distinction between, for example, $\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$ and $\{\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}\}$, or between $\varnothing$ and $\{\varnothing\}$.

Again, patterns can be used:

$$\mathrm{S} = \{\mathrm{X} \subseteq \mathrm{L} \mid \mathrm{a} \in \mathrm{X}\} = \{\{\mathrm{a}\}, \{\mathrm{a}, \mathrm{b}\}, \{\mathrm{a}, \mathrm{c}\}, \{\mathrm{a}, \mathrm{b}, \mathrm{c}\}\}$$

then $\mathrm{L} \in \mathrm{S}$ but $\mathrm{a} \notin \mathrm{S}$.

The power set, $\mathcal{P}(\mathrm{X})$, is the set of all subsets of X. So, for the set L above:

$$\mathcal{P}(\mathrm{L}) = \{\varnothing, \{\mathrm{a}\}, \{\mathrm{b}\}, \{\mathrm{c}\}, \{\mathrm{a}, \mathrm{b}\}, \{\mathrm{a}, \mathrm{c}\}, \{\mathrm{b}, \mathrm{c}\}, \{\mathrm{a}, \mathrm{b}, \mathrm{c}\}\}$$

It is important to specify the *universe of discourse* when discussing sets. This is the set of all possible elements that might be considered. It is often written as Ω.

Russell's paradox

Consider $\mathrm{R} = \{\mathrm{X} \mid \mathrm{X} \notin \mathrm{X}\}$. Then $\mathrm{L} \in \mathrm{R}$ and $\mathrm{S} \in \mathrm{R}$, but is $\mathrm{R} \in \mathrm{R}$?

Combining sets

There are several ways of combining existing sets to make new ones:

The *complement* of a set, A, is the collection, A^c or $\overline{\mathrm{A}}$, of elements (within the universe of discourse) that are not in A. $\mathrm{A}^c = \{\mathrm{x} \in \Omega \mid \mathrm{x} \notin \mathrm{A}\}$. This is a case where it is necessary to be particularly clear about the universe.

Other operations include:

Union	$\mathrm{A} \cup \mathrm{B} = \{x \mid x \in \mathrm{A} \text{ OR } x \in \mathrm{B}\}$
Intersection	$\mathrm{A} \cap \mathrm{B} = \{x \mid x \in \mathrm{A} \text{ AND } x \in \mathrm{B}\}$

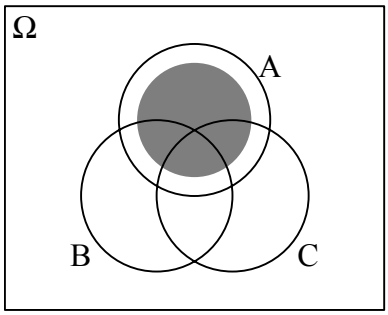
Difference	$A \setminus B$	$= \{x \mid x \in A \text{ AND } x \notin B\}$ $= A \cap B^c$
Symmetric difference	$A \Delta B$	$= (A \setminus B) \cup (B \setminus A)$

These operations satisfy various properties:

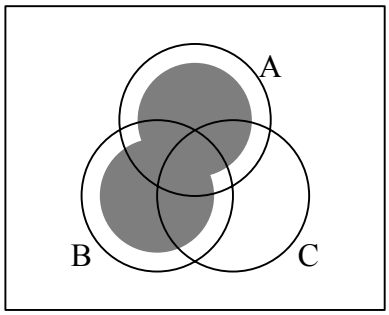
Idempotence	$A \cup A = A$	$A \cap A = A$
Complements	$A \cup A^c = \Omega$	$A \cap A^c = \varnothing$
	$(A^c)^c = A$	
Commutativity	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associativity	$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$
De Morgan's Laws	$(A \cup B)^c = A^c \cap B^c$	$(A \cap B)^c = A^c \cup B^c$
Distributivity	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Empty set	$A \cup \varnothing = A$	$A \cap \varnothing = \varnothing$
Universal set	$A \cup \Omega = \Omega$	$A \cap \Omega = A$
Absorption	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$

Venn diagrams

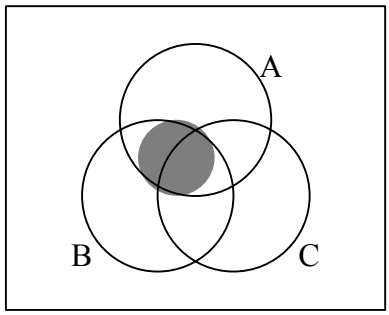
Venn diagrams provide a way of showing combinations of sets:



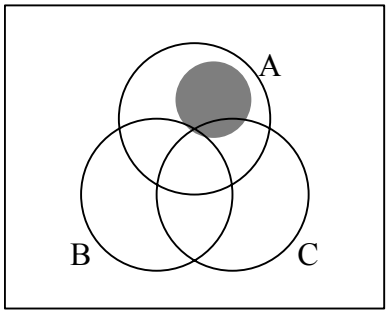
A



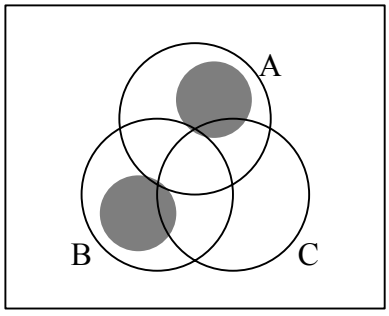
$A \cup B$



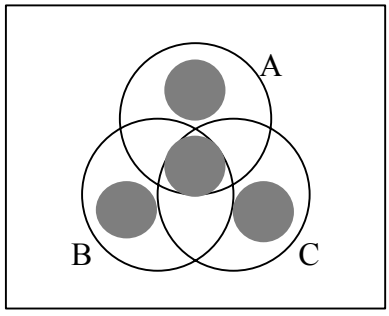
$A \cap B$



$A \setminus B$



$A \Delta B$



$A \Delta B \Delta C$

Normal form

Symmetric difference can be expressed as a union of differences and each difference can be expressed as an intersection of sets and complements of sets. De Morgan's Laws can be used to expand complemented expressions and distributivity can be used to expand intersections into

unions. Together these transformations allow any expression to be reduced to a union of terms each of which is the intersection of the underlying sets and their complements.

This expression is unique (up to the order of the terms and the factors within each term) so two expressions can be checked for equality by reducing them to this normal form.

Partitions

A *partition* of a set Ω is just a division of the whole of Ω into non-overlapping subsets.

Mathematically a partition P of a set Ω is a subset $\mathrm{P} \subseteq \mathcal{P}(\Omega)$ such that

1. $\bigcup_{S \in P} S = \Omega$ (P *covers* Ω) and
2. If $\mathrm{S}, \mathrm{T} \in \mathrm{P}$ then $\mathrm{S} \cap \mathrm{T} \neq \varnothing$ implies that $\mathrm{S} = \mathrm{T}$ (the elements of P are *disjoint*).

Examples:

- $\{\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}\}$ and $\{\{\mathrm{a}\}, \{\mathrm{b}, \mathrm{c}\}\}$ are both partitions of $\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$.
- Neither $\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$ nor $\{\{\mathrm{a}, \mathrm{b}\}, \{\mathrm{b}, \mathrm{c}\}\}$ are partitions of $\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$.

Product sets

The *product* of two sets A and B is the set of pairs of elements from A and B:

$$\mathrm{A} \times \mathrm{B} = \{(a, b) \mid a \in \mathrm{A} \text{ AND } b \in \mathrm{B}\}$$

So $\{\mathrm{a}, \mathrm{b}\} \times \{\mathrm{b}, \mathrm{c}\} = \{(\mathrm{a}, \mathrm{b}), (\mathrm{a}, \mathrm{c}), (\mathrm{b}, \mathrm{b}), (\mathrm{b},\mathrm{c})\}$

This can be extended to ordered n-tuples:

$$\mathrm{A}^1 = \mathrm{A}$$
$$\mathrm{A}^n = \mathrm{A} \times \mathrm{A}^{n-1} \text{ for } n > 1$$

For convenience, we write elements as $(\mathrm{a}, \mathrm{b}, \mathrm{c})$ rather than $(\mathrm{a}, (\mathrm{b}, \mathrm{c}))$. This gives the usual notation for Euclidean space, $\mathbb{R}^3$.

Disjoint sums

The *disjoint sum* of two sets A and B is $\mathrm{A} + \mathrm{B} = (\{0\} \times \mathrm{A}) \cup (\{1\} \times \mathrm{B})$.

So $\{\mathrm{a}, \mathrm{b}\} + \{\mathrm{b}, \mathrm{c}\} = \{(0, \mathrm{a}), (0, \mathrm{b}), (1, \mathrm{b}), (1, \mathrm{c})\}$ while $\{\mathrm{a}, \mathrm{b}\} \cup \{\mathrm{b}, \mathrm{c}\} = \{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$.

Indicator functions

Given a set $\mathrm{A} \subseteq \Omega$, define the *indicator* or *characteristic* function for A for $\mathrm{x} \in \Omega$ by

$$I_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{otherwise} \end{cases}.$$

Observations

- $I_{\mathrm{A} \cup \mathrm{B}}(x) = \text{MAX}\,(I_{\mathrm{A}}(x), I_{\mathrm{B}}(x))$
- $I_{\mathrm{A} \cap \mathrm{B}}(x) = \text{MIN}\,(I_{\mathrm{A}}(x), I_{\mathrm{B}}(x)) = I_{\mathrm{A}}(x)\, I_{\mathrm{B}}(x)$
- $I_{\mathrm{A}^{\mathrm{c}}}(x) = 1 - I_{\mathrm{A}}(x)$
- $\mathrm{A} = \{x \in \Omega \mid I_{\mathrm{A}}(x) = 1\}$
- $|A| = \sum_{x \in \Omega} I_A(x)$

Inclusion and exclusion

Observe

$|\mathrm{A} \cup \mathrm{B}| = |\mathrm{A}| + |\mathrm{B}| - |\mathrm{A} \cap \mathrm{B}|$
and
$|\mathrm{A} \cup \mathrm{B} \cup \mathrm{C}| = |\mathrm{A}| + |\mathrm{B}| + |\mathrm{C}| - |\mathrm{A} \cap \mathrm{B}| - |\mathrm{A} \cap \mathrm{C}| - |\mathrm{B} \cap \mathrm{C}| + |\mathrm{A} \cap \mathrm{B} \cap \mathrm{C}|.$

This leads to the general *principle of inclusion and exclusion*. Given a collection, $\mathscr{C}$, of sets, say $\mathscr{C} = \{\mathrm{A}_s \mid s \in \mathrm{S}\}$ for some index set, $\mathrm{S} = \{1, 2, \ldots, n\}$. Then write $\bigcup_{s\in S} A_s = A_1 \cup A_2 \cup \cdots \cup A_n$. The principle states that $\left|\bigcup_{s\in S} A_s\right| = -\sum_{\phi\neq T\subseteq S} (-1)^{|T|}\left|\bigcap_{t\in T} A_t\right|$.

Proof: Write $A_T = \bigcap_{t\in T} A_t = \{x \in \Omega \mid x \in A_t \text{ for every } t \in T\}$ with $A_\varnothing = \Omega$ and use indicator functions, observing that $I_{A_T} = \prod_{t\in T} I_{A_t}$:

$$\begin{aligned} I_{\overline{A_1}\cap\overline{A_2}\cap\cdots\cap\overline{A_n}}(x) &= I_{\overline{A_1}}(x) I_{\overline{A_2}}(x)\cdots I_{\overline{A_n}}(x) \\ &= (1 - I_{A_1}(x))(1 - I_{A_2}(x))\cdots(1 - I_{A_n}(x)) \\ &= \sum_{T\subseteq S}(-1)^{|T|}\left(\prod_{t\in T} I_{A_t}(x)\right) \\ &= \sum_{T\subseteq S}(-1)^{|T|} I_{A_T}(x) \end{aligned}$$

Now sum over all $x \in \Omega$ to give $\left|\bigcap_{s\in S}\overline{A_s}\right| = \sum_{T\subseteq S}(-1)^{|T|}|A_T|$ and observe:

$$\begin{aligned} \left|\bigcup_{s\in S} A_s\right| &= |\Omega| - \left|\overline{\bigcup_{s\in S} A_s}\right| \\ &= |\Omega| - \left|\bigcap_{s\in S}\overline{A_s}\right| \\ &= -\sum_{\phi\neq T\subseteq S}(-1)^{|T|}\left|\bigcap_{t\in T} A_t\right| \end{aligned}$$

Application

Recall Euler's totient function $\varphi(m)$ which counts the natural numbers less than m and co-prime to m. We can now show again that $\varphi(m) = m\prod_{\text{prime } p|m}\left(1 - 1/p\right)$.

Proof: Write $m = p_1^{k_1} p_2^{k_2}\cdots p_n^{k_n}$ as a product of distinct primes.

Let $\mathrm{A}_i = \{x \in \mathbb{N} \mid 0 < x \le m \text{ and } p_i \mid x\}$ for $1 \le i \le n$ so $|\mathrm{A}_i| = m / p_i$. Moreover, $\left|\mathrm{A}_i \cap \mathrm{A}_j\right| = \dfrac{m}{p_i p_j}$ and, more generally, $\left|\mathrm{A}_T\right| = \left|\bigcap_{t\in T}\mathrm{A}_t\right| = \dfrac{m}{\prod_{t\in T} p_t}$.

Now

$$\begin{aligned} \varphi(m) &= \left|\bigcap_{1\le i\le n}\overline{\mathrm{A}_i}\right| \\ &= \sum_{T\subseteq\{1,2,\cdots n\}}(-1)^{|T|}\left|\mathrm{A}_T\right| \end{aligned}$$

$$= \sum_{T \subseteq \{1,2,\cdots n\}} (-1)^{|T|} \frac{m}{\prod_{t \in T} p_t}$$

$$= m \sum_{T \subseteq \{1,2,\cdots n\}} \prod_{t \in T} \left(\frac{-1}{p_t} \right)$$

$$= m \prod_{s \in \{1,2,\cdots n\}} \left(1 - \frac{1}{p_s} \right)$$

Boolean logic

Propositions are statements that can be either true (T) or false (F). They will often include a symbol, x say, which can be thought of as an argument; the proposition $\mathrm{P}(x)$ will be true for some values of x and false for other values.

Propositions can be combined to make new ones:

P	Q	NOT P $\neg \mathrm{P}, \sim \mathrm{P}$	P AND Q $\mathrm{P} \wedge \mathrm{Q}$	P OR Q $\mathrm{P} \vee \mathrm{Q}$	P IMPLIES Q $\mathrm{P} \Rightarrow \mathrm{Q}$	P EQUIVALENT TO Q $\mathrm{P} \Leftrightarrow \mathrm{Q}$
F	F	T	F	F	T	T
F	T	T	F	T	T	F
T	F	F	F	T	F	F
T	T	F	T	T	T	T

Note that OR is *inclusive* - P OR Q is true if either or both of P and Q are true.

$\mathrm{P} \Rightarrow \mathrm{Q}$ means P *implies* Q. This is the same as saying, "If P is true then Q is true." If P is false, it says nothing about Q. It is actually equivalent to (NOT P) OR Q. It is also equivalent to $\neg \mathrm{Q} \Rightarrow \neg \mathrm{P}$.

Boolean logic enjoys a collection of properties that are similar to the ones shown above for sets. These can be used to prove statements by reducing them to a standard "sum of products" form.

Quantifiers

Given a proposition, $\mathrm{P}(x)$, involving a variable, x, in some set, S, $\mathrm{P}(x)$ may be true for some values of x and false for others. If it is true for *every* x, we write $\forall\, x \in \mathrm{S}\,.\, \mathrm{P}(x)$ to mean "For all x in S, $\mathrm{P}(x)$ is true". If there is *at least one* x for which $\mathrm{P}(x)$ is true, we write $\exists\, x \in \mathrm{S}\,.\, \mathrm{P}(x)$ to mean "There exists an x in S such that $\mathrm{P}(x)$ is true."

Exercises

1. Let $\mathrm{A} = \{1, 3, 5\}$ and $\mathrm{B} = \{2, 3\}$. Write down explicit sets for:
   - $\mathrm{A} \cup \mathrm{B}$ and $\mathrm{A} \cap \mathrm{B}$
   - $\mathrm{A} \setminus \mathrm{B}$ and $\mathrm{B} \setminus \mathrm{A}$
   - $(\mathrm{A} \cup \mathrm{B}) \setminus \mathrm{B}$ and $(\mathrm{A} \setminus \mathrm{B}) \cup \mathrm{B}$
   - $\mathrm{A} \,\Delta\, \mathrm{B}$ and $\mathrm{B} \,\Delta\, \mathrm{A}$

- $A \times B$, $B \times A$ and $A \times \varnothing$
- $A + B$, $B + A$ and $A + \varnothing$

2. Let A, B and C be sets. Prove or find counter-examples to:
   - $A \cup (B \cup C) = (A \cup B) \cup C$
   - $A \cup (B \cap C) = (A \cap B) \cup C$
   - $A \cup (B \cap C) = (A \cap B) \cup (A \cap C)$
   - $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
   - $A \setminus (B \Delta C) = (A \setminus B) \Delta (A \setminus C)$
   - $(A \times C) \cup (B \times D) = (A \cup B) \times (C \cup D)$
   - $(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D)$
3. What is the difference between $\forall x \,.\, (\exists y \,.\, P(x, y))$ and $\exists y \,.\, (\forall x \,.\, P(x, y))$? You might like to consider the universe to be the set of people and $P(x, y)$ to mean "x loves y".
4. If $|A| = m$ and $|B| = n$, what are the sizes of $A \times B$ and $A + B$? How big is $\mathcal{P}(A)$?
5. Of 100 students, 35 play football, 36 row and 24 play tiddlywinks. 13 play football and row, 2 play football and tiddlywinks but never row, 12 row and play tiddlywinks while 4 play every game in sight to avoid work of any form. How many students participate in none of these three vices?
6. There are n students at St Botolph's College, each with an individual pigeon hole in the Porters' Lodge. Because of the University policy on anonymous candidature, the porters are obliged to deliver examination results by posting n letters randomly, one in each of the n pigeon holes. Of course, there are $n!$ ways of doing this. How many of them result in no student receiving the correct letter?

   Hint: This is a question about inclusion and exclusion.
7. Simplify the Boolean expression $\neg(\neg(a \wedge \neg(a \wedge b)) \wedge \neg(\neg(a \wedge b) \wedge b))$.
8. Use Boolean simplification to show that $\{[(a \Rightarrow b) \vee (a \Rightarrow d)] \Rightarrow (b \vee d)\} = a \vee b \vee d$.
9. Consider the argument: "If Anna can cancan or Kant can't cant, then Greville will cavil vilely. If Greville will cavil vilely, Will will want. But Will won't want. Therefore Kant can cant." By rewriting the statement inside the double quotes as a single Boolean expression in terms of four variables and simplifying, show that it is true and hence that the argument is valid.

Relations

A *relation*, R, between two sets, A and B, is just a subset $\mathrm{R} \subseteq \mathrm{A} \times \mathrm{B}$. A relation, R, on a single set, A, is just a subset $\mathrm{R} \subseteq \mathrm{A} \times \mathrm{A}$.

We write $a \ \mathrm{R} \ b$ as shorthand for $(a, b) \in \mathrm{R}$.

Write $\mathcal{R}(\mathrm{A}, \mathrm{B})$ for the collection of all relations between two sets, A and B. Obviously $\mathcal{R}(\mathrm{A}, \mathrm{B}) = \mathcal{P}(\mathrm{A} \times \mathrm{B})$.

Composition of relations

Suppose $\mathrm{R} \subseteq \mathrm{A} \times \mathrm{B}$ is a relation between A and B, and $\mathrm{S} \subseteq \mathrm{B} \times \mathrm{C}$ is a relation between B and C, then we define the *composition* of R and S to be the relation between A and C defined by $\mathrm{R} \circ \mathrm{S} = \{(a, c) \mid \exists\, b \in \mathrm{B} \,.\, (a, b) \in \mathrm{R} \wedge (b, c) \in \mathrm{S}\} \subseteq \mathrm{A} \times \mathrm{C}$. Sometimes this is written as $\mathrm{S} \circ \mathrm{R}$, which may seem confusing but is actually sensible for reasons that will become apparent later.

This can be extended to n-fold composition. Given a relation R on a set, A, write:

$\mathrm{R}^1 = \mathrm{R}$
$\mathrm{R}^n = \mathrm{R}^{n-1} \circ \mathrm{R}$ for $n > 1$.

We can also define the *inverse* of a relation: $\mathrm{R}^{-1} = \{(b, a) \mid (a, b) \in \mathrm{R}\}$, which is a relation between B and A. Observe that $(\mathrm{R} \circ \mathrm{S})^{-1} = \mathrm{S}^{-1} \circ \mathrm{R}^{-1}$.

Equivalence relations

An *equivalence relation* is a relation, R, on a set, A, satisfying three properties:

- Reflexive: $\forall\, a \in \mathrm{A} \,.\, (a, a) \in \mathrm{R}$
- Symmetric: $(a, b) \in \mathrm{R} \Rightarrow (b, a) \in \mathrm{R}$
- Transitive: $(a, b) \in \mathrm{R} \wedge (b, c) \in \mathrm{R} \Rightarrow (a, c) \in \mathrm{R}$

Intuitively, we can think of an equivalence relation as a sort of weak equality - $(a, b) \in \mathrm{R}$ means that a and b are indistinguishable within some framework.

Examples

- Given $n \in \mathbb{N}$, define R on $\mathbb{Z}$ by $(a, b) \in \mathrm{R} \Leftrightarrow n \mid (b - a)$.
- Define S on $\mathbb{Z} \times \mathbb{N}$ by $((z_1, n_1), (z_2, n_2)) \in \mathrm{S} \Leftrightarrow z_1 n_2 = z_2 n_1$.

Equivalence classes

Given an equivalence relation R on a set, A, define the *equivalence class* of an element $a \in \mathrm{A}$ to be the set of elements of A related to a: $[a] = \{b \in \mathrm{A} \mid (a, b) \in \mathrm{R}\} = \{b \in \mathrm{A} \mid a \ \mathrm{R} \ b\}$.

The set of equivalence classes $\{[a] \mid a \in \mathrm{A}\}$ forms a partition of A, that is:

- The classes cover A: $\bigcup_{a \in \mathrm{A}} [a] = \mathrm{A}$.

  Proof: Given any $a \in \mathrm{A}$, $a \ \mathrm{R} \ a$ by reflexivity so $a \in [a]$ and $a \in \bigcup_{a \in \mathrm{A}} [a]$.

- They are disjoint (or equal): $\forall\, a, b \in \mathrm{A}\,.\, [a] \cap [b] \neq \varnothing \Rightarrow [a] = [b]$.

  Proof: Suppose $x \in [a] \cap [b]$, so $a\ \mathrm{R}\ x$ and $b\ \mathrm{R}\ x$. Then $x\ \mathrm{R}\ b$ by symmetry. Given any $v \in [b]$, observe $b\ \mathrm{R}\ v$. Now $a\ \mathrm{R}\ x$, $x\ \mathrm{R}\ b$ and $b\ \mathrm{R}\ v$, so $a\ \mathrm{R}\ v$ by transitivity. Therefore $v \in [a]$ and so $[b] \subseteq [a]$. But $[a] \subseteq [b]$ similarly, so $[a] = [b]$.

The set of equivalence classes is called the *quotient set*, $\mathrm{A}_{/\mathrm{R}}$.

In the two examples above, $\mathbb{Z}_{/\mathrm{R}}$ represents the integers *modulo n* and $(\mathbb{Z} \times \mathbb{N})_{/\mathrm{S}}$ represents the rational numbers.

Closures

Given a set, Ω, a property, P, of subsets of Ω and a particular subset $\mathrm{S} \subseteq \Omega$, which may or may not satisfy P, we might ask the question, "What is the smallest subset of Ω containing S which does satisfy P?" That is, find $\mathrm{C} \subseteq \Omega$ such that:

- $\mathrm{S} \subseteq \mathrm{C}$.
- $\mathrm{P}(\mathrm{C})$ is true.
- If $\mathrm{D} \subseteq \Omega$ also satisfies $\mathrm{S} \subseteq \mathrm{D}$ and $\mathrm{P}(\mathrm{D})$, then $\mathrm{C} \subseteq \mathrm{D}$.

Such a set, C, is called the P-*closure* of S. Such a closure need not necessarily exist. However, there is one particular class of properties for which closures *will* always exist. These are the *intersection-closed* properties.

Let $\mathscr{C} = \{\mathrm{S} \subseteq \Omega \mid \mathrm{P}(\mathrm{S}) \text{ is true}\}$ be the collection of all subsets of Ω satisfying P. P is intersection-closed if, for any subset $\mathscr{B} \subseteq \mathscr{C}$, the intersection of all the subsets in $\mathscr{B}$ also satisfies P. That is, if $I = \bigcap_{S \in B} S$, then $\mathrm{P}(I)$ is true.

We can now calculate the P-closure of a given subset $\mathrm{S} \subseteq \Omega$ as $\bigcap \{B \subseteq \Omega \mid S \subseteq B \wedge P(B) \text{ is true}\}$ as long as $\mathrm{P}(\Omega)$ is true.

If we consider relations on a set A, which are just subsets of $\Omega = \mathrm{A} \times \mathrm{A}$, it turns out that reflexivity, symmetry and transitivity are all intersection-closed properties. Given a relation, $\mathrm{R} \subseteq \mathrm{A} \times \mathrm{A}$, this allows us to form the:

- Reflexive closure: $\mathrm{r}(\mathrm{R}) = \mathrm{R} \cup \mathrm{I}_{\mathrm{A}}$ where $\mathrm{I}_{\mathrm{A}} = \{(a, a) \mid a \in \mathrm{A}\}$
- Symmetric closure: $\mathrm{s}(\mathrm{R}) = \mathrm{R} \cup \mathrm{R}^{-1}$
- Transitive closure: $\mathrm{t}(\mathrm{R}) = \mathrm{R}^{+}$ where $\mathrm{R}^{+} = \mathrm{R} \cup \mathrm{R}^{2} \cup \mathrm{R}^{3} \cup \mathrm{R}^{4} \cup \ldots$

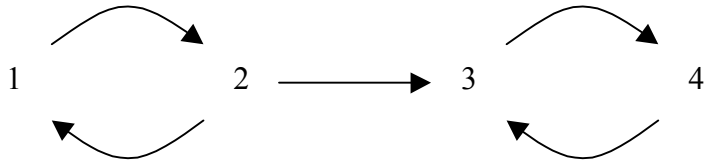
  Observe that $(a, b) \in \mathrm{t}(\mathrm{R}) \Leftrightarrow \exists\, n \in \mathbb{N}$ and $x_0 = a, x_1, x_2, \ldots x_n = b$ with $(x_i, x_{i+1}) \in \mathrm{R}$ for $0 \leq i < n$.

Warshall's algorithm

It is helpful to regard calculating the transitive closure as a route finding problem in a graph. Consider the elements of A to be locations identified by natural numbers, two of which are related by R if they are directly connected. Two locations are related by R^2 if they are connected via a path with two steps, by R^3 if they are linked via a path with three steps and so on. Two locations are related by the transitive closure of R if they are indirectly connected via an arbitrarily long sequence of intermediate steps.

Suppose that A is finite with $|\mathrm{A}| = n$. Then R can be represented as an $n \times n$ array of Boolean values. Calculating R^2 is rather like a matrix multiplication requiring n^2 values to be found, each of which is the sum of n products, which makes it an O(n^3) operation. It turns out that, when $|\mathrm{A}| = n$, the union of powers of R in the transitive closure can stop at R^n (no path will require more than n intermediate steps), so forming the transitive closure naïvely is an O(n^4) operation.

For example, consider the following graph:



$m = \begin{bmatrix} \cdot & t & \cdot & \cdot \\ t & \cdot & t & \cdot \\ \cdot & \cdot & \cdot & t \\ \cdot & \cdot & t & \cdot \end{bmatrix}$, $m^2 = \begin{bmatrix} t & \cdot & t & \cdot \\ \cdot & t & \cdot & t \\ \cdot & \cdot & t & \cdot \\ \cdot & \cdot & \cdot & t \end{bmatrix}$, $m^3 = \begin{bmatrix} \cdot & t & \cdot & t \\ t & \cdot & t & \cdot \\ \cdot & \cdot & \cdot & t \\ \cdot & \cdot & t & \cdot \end{bmatrix}$ and $m^4 = \begin{bmatrix} t & \cdot & t & \cdot \\ \cdot & t & \cdot & t \\ \cdot & \cdot & t & \cdot \\ \cdot & \cdot & \cdot & t \end{bmatrix}$ so

$t(\mathrm{R}) = m \vee m^2 \vee m^3 \vee m^4 = \begin{bmatrix} t & t & t & t \\ t & t & t & t \\ \cdot & \cdot & t & t \\ \cdot & \cdot & t & t \end{bmatrix}$. (In fact, the m^4 term is unnecessary for this example because the longest path is only three steps long.)

However, we can do better than this.

The outer loop of the naïve algorithm iterates over the length of the path linking two locations. Warshall's algorithm has a different structure in which the outer loop iterates over highest numbered intermediate point encountered along a path.

Suppose that $\mathrm{A} = \{1, 2, 3, \ldots, n\}$ and represent R by the Boolean matrix $[m(i, j)]$ where $m(i, j) = ((i, j) \in \mathrm{R})$. Now define $m_k(i, j)$ to be true if an only if there is a path from i to j using only intermediate locations numbered between 1 and k. So $m_0 = m$ representing direct connections that do not require any intermediate locations.

In order to get from i to j using only intermediate locations numbered between 1 and k+1, either we can do it using only locations between 1 and k or we must visit location k+1, but there will be at most one such visit. So $m_{k+1}(i, j) = m_k(i, j)) \vee (m_k(i, k{+}1) \wedge m_k(k{+}1, j))$. Finally m_n will be the transitive closure, allowing any intermediate locations.

For the above example, $m_0 = m = \begin{bmatrix} \cdot & t & \cdot & \cdot \\ t & \cdot & t & \cdot \\ \cdot & \cdot & \cdot & t \\ \cdot & \cdot & t & \cdot \end{bmatrix}$, $m_1 = \begin{bmatrix} \cdot & t & \cdot & \cdot \\ t & t & t & \cdot \\ \cdot & \cdot & \cdot & t \\ \cdot & \cdot & t & \cdot \end{bmatrix}$, $m_2 = \begin{bmatrix} t & t & t & \cdot \\ t & t & t & \cdot \\ \cdot & \cdot & \cdot & t \\ \cdot & \cdot & t & \cdot \end{bmatrix}$,

$m_3 = \begin{bmatrix} t & t & t & t \\ t & t & t & t \\ \cdot & \cdot & \cdot & t \\ \cdot & \cdot & t & t \end{bmatrix}$ and $m_4 = \begin{bmatrix} t & t & t & t \\ t & t & t & t \\ \cdot & \cdot & t & t \\ \cdot & \cdot & t & t \end{bmatrix} = t(\mathrm{R})$. In this case, all the steps are necessary because the only route from 3 to 3 is via 4 which appears only at the last iteration.

It is necessary to iterate over i, j and k (in the right order), so this is an O(n^3) operation.

Partial orders

A *partial order* is a relation R on a set, A, satisfying three properties:

- Reflexive: $\forall\, a \in \mathrm{A} \,.\, (a, a) \in \mathrm{R}$
- Anti-symmetric: $(a, b) \in \mathrm{R} \wedge (b, a) \in \mathrm{R} \Rightarrow a = b.$
- Transitive: $(a, b) \in \mathrm{R} \wedge (b, c) \in \mathrm{R} \Rightarrow (a, c) \in \mathrm{R}$

Intuitively, we can think of $(a, b) \in \mathrm{R}$ as meaning $a \leq b$. The notation $a\ \mathrm{R}\ b$ meaning $(a, b) \in \mathrm{R}$ may have seemed strange for arbitrary relations, but $a \leq b$ reads more easily than $(a, b) \in \leq$. The order is partial because it is possible to have pairs of elements that are not comparable - $(a, b) \notin \mathrm{R}$ and $(b, a) \notin \mathrm{R}$.

It is possible to have two different partial orders on a single set so it may be necessary to refer to the pair (A, R) or $(\mathrm{A}, \leq)$ to avoid ambiguity.

Total order

A partially ordered set, $(\mathrm{A}, \leq)$, is *totally ordered* if any pair of elements of A can be compared using $\leq$. That is, $\forall\, a, b \in \mathrm{A} \,.\, (a \leq b) \vee (b \leq a)$.

Examples

- Conventional numerical order on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$, all of which are total.
- Division order on $\mathbb{N}$ or $\mathbb{N}_0$: $(a, b) \in \mathrm{D} \Leftrightarrow a \mid b$. This is partial, for example 2 and 3 can not be compared.
- However, the division order on $\mathbb{Z}$ is *not* a partial order.
- Division order on $\mathrm{D}_n = \{x \in \mathbb{N} \mid x \mid n\}$ for any $n \in \mathbb{N}$.
- For any set A, the power set of A ordered by subset inclusion, $(\mathcal{P}(\mathrm{A}), \subseteq)$. Again, this is partial.
- For any two partially ordered sets $(\mathrm{A}, \leq_\mathrm{A})$ and $(\mathrm{B}, \leq_\mathrm{B})$ there are two important orders on the product set $\mathrm{A} \times \mathrm{B}$.
  - *Product* order: $(a_1, b_1) \leq_\mathrm{P} (a_2, b_2) \Leftrightarrow (a_1 \leq_\mathrm{A} a_2) \wedge (b_1 \leq_\mathrm{B} b_2)$.
  - *Lexicographic* order: $(a_1, b_1) \leq_\mathrm{L} (a_2, b_2) \Leftrightarrow (a_1 <_\mathrm{A} a_2) \vee (a_1 = a_2 \wedge b_1 \leq_\mathrm{B} b_2)$.

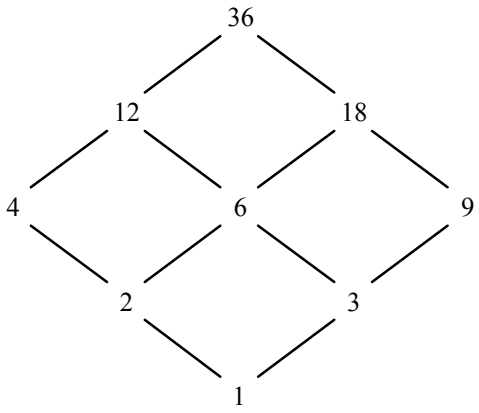
  If $(\mathrm{A}, \leq_\mathrm{A})$ and $(\mathrm{B}, \leq_\mathrm{B})$ are both total orders, then the lexicographic order on $\mathrm{A} \times \mathrm{B}$ will be total, but the product order will generally only be partial.

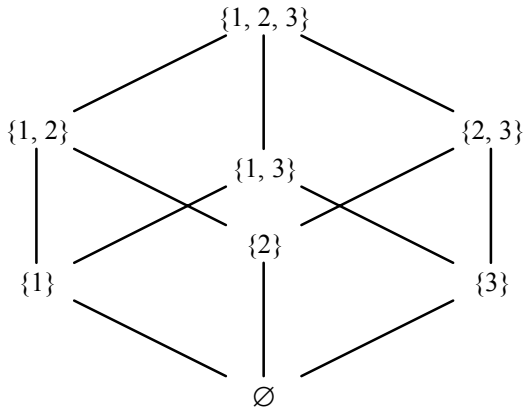
  $(a_1, b_1) \leq_\mathrm{P} (a_2, b_2) \Rightarrow (a_1, b_1) \leq_\mathrm{L} (a_2, b_2)$, so the product order (consider as a subset of $(\mathrm{A} \times \mathrm{B}) \times (\mathrm{A} \times \mathrm{B})$) is a subset of the lexicographic order.
- For any totally ordered (finite) alphabet A, $\mathrm{A}^* = \{\varepsilon\} \cup \mathrm{A} \cup \mathrm{A}^2 \cup \mathrm{A}^3 \cup \ldots$ is the set of all strings made from that alphabet, where ε is the empty string. The *full lexicographic* order, $\leq_\mathrm{F}$, on A^* is defined recursively as follows. Given two words $u, v \in \mathrm{A}^*$, if $u = \varepsilon$ then $u \leq_\mathrm{F} v$ and if $v = \varepsilon$ then $v \leq_\mathrm{F} u$. Otherwise, both u and v are non-empty so we can write $u = u_1 x$ and $v = v_1 y$ where u_1 and v_1 are the first letters of u and v respectively. Now $u \leq_\mathrm{F} v \Leftrightarrow (u = \varepsilon) \vee (u_1 <_\mathrm{A} v_1) \vee (u_1 = v_1 \wedge x \leq_\mathrm{F} y)$

Hasse diagrams

A *Hasse diagram* represents a partial order pictorially as a directed graph with nodes for the elements of the underlying set and arcs between pairs of elements related by the order but with no intermediate elements in the order. For simplicity, we omit the arcs for reflexivity and even omit the arrows on the arcs if they point up the page.

Here are the Hasse diagrams for D_{36} and $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$:





Well founded relations

A relation R on a set A is *well founded* if there is no infinite sequence $a_1, a_2, a_3, \ldots$ of elements in A with $(a_2, a_1) \in \mathrm{R}$, $(a_3, a_2) \in \mathrm{R}$, ...

Note that R can not be reflexive and it need not be transitive. Note also that the definition is asymmetric: it says nothing about ascending sequences.

When discussing well founded relations, it is convenient to use the notation $<$ for a relation on the set A. Then we can write $\leq$ for the relation on A defined by:

$$a_1 \leq a_2 \Leftrightarrow a_1 = a_2 \text{ or } a_1 < a_2$$

for all $a_1, a_2 \in \mathrm{A}$. Again, neither $<$ nor $\leq$ need be transitive. We can also write $>$ and $\geq$ for the inverse relations defined by:

$$a_1 > a_2 \Leftrightarrow a_2 < a_1$$
$$a_1 \geq a_2 \Leftrightarrow a_2 \leq a_1$$

for all $a_1, a_2 \in \mathrm{A}$.

Proposition

Let $<$ be a relation on a set A. The relation $<$ is well founded if and only if every infinite sequence $a_1, a_2, a_3, \ldots$ of elements in A with $a_1 \geq a_2 \geq a_3 \geq \ldots$ is ultimately constant, so there is some $M \in \mathbb{N}$ such that $a_m = a_M$ for all $m \geq M$.

Examples

- Conventional numerical order $<$ on $\mathbb{N}$ but *not* on $\mathbb{Z}$.

- If two relations $<_A$ on A and $<_B$ on B are well founded, then the lexicographic relation $<_L$ on $A \times B$ defined by:
  $(a_1, b_1) <_L (a_2, b_2) \Leftrightarrow (a_1 <_A a_2) \vee (a_1 = a_2 \wedge b_1 <_B b_2)$
  is also well founded

  Proof: Suppose $(a_1, b_1) \geq_L (a_2, b_2) \geq_L (a_3, b_3) \geq_L \ldots$. Then $a_1 \geq_A a_2 \geq_A a_3 \geq_A \ldots$ by the definition of lexicographic order, so the sequence is ultimately constant because $(A, \leq_A)$ is well founded. So $\exists M \in \mathbb{N}$ such that $\forall m \geq M \,.\, a_m = a_M$. Now $b_M \geq_B b_{M+1} \geq_B b_{M+2} \geq_B \ldots$, so this sequence is also ultimately constant because $(B, \leq_B)$ is well founded. So $\exists N \in \mathbb{N}$ such that $\forall n \geq N \,.\, b_n = b_N$. But $N \geq M$, so $\forall n \geq N \,.\, (a_n, b_n) = (a_N, b_N)$ and the original sequence is ultimately constant.

  Now, if $(a_1, b_1) \geq_P (a_2, b_2) \geq_P (a_3, b_3) \geq_P \ldots$ then $(a_1, b_1) \geq_L (a_2, b_2) \geq_L (a_3, b_3) \geq_L \ldots$, so again the sequence is ultimately constant.

- The full lexicographic order on A^* is *not* well founded if A has more than one element. Consider the sequence $b, ab, aab, aaab, \ldots$.

Proposition

Let $<$ be a relation on a set A. The relation $<$ is well founded if and only if any non-empty subset $S \subseteq A$ contains a $<$-minimal element. That is, there is an element $m \in S$ such that

$$\forall a \in A \,.\, a < m \Rightarrow a \notin S$$

In other words, if a set with a well-founded relation $<$ contains a counterexample to some property, then it contains a $<$-minimal counterexample. (Just let S be the set of all counterexamples.)

Well ordering

A total order $(A, \leq)$ is a *well ordering* if $<$ is well founded. This is equivalent to saying that every subset of A contains a minimal element with respect to $\leq$. That is, $\forall \emptyset \neq S \subseteq A \,.\, \exists s \in S \,.\, \forall t \in S \,.\, t \leq s \Rightarrow t = s$. The minimal element will be unique since $\leq$ is total. This is the characterisation of well ordering in the natural numbers that was used in the first half of this course.

A *chain* in a partially ordered set $(A, \leq)$ is a subset $C \subseteq A$ that is totally ordered by $\leq$. An infinite descending chain is a sequence of elements $a_1 > a_2 > a_3 > \ldots$. $(A, \leq)$ is well ordered precisely when there are no infinite descending chains of elements in A.

Topological sorting

Suppose that $(A, \leq)$ is partially ordered but is not totally ordered. Can we find a *topological sort* of A, that is, a total order on A that respects $\leq$? If A is finite then $\leq$ is necessarily well-founded and we can develop an algorithm as follows.

A is itself a subset of A and so it contains a minimal element. Put this first in the total order. Now take the rest of A, find a minimal element and put it second. Continue in this way to build up a total order on the whole of A.

In fact there is a slight subtlety. At the each step there may be more than one minimal element. These can not be compared with each other, so it does not matter what order they have in the total order. Instead of putting just one of them into the total order we could include all of them in some arbitrary order before going on to the next step and finding the minimal elements in the remainder of A.

The former is a *depth first* algorithm, the latter a *breadth first* one, and they may well give rise to two different total orders, each of which respects the original partial order.

Complete ordering

A partially ordered set, $(\mathrm{A}, \leq)$, is *complete* if every (ascending) chain in A has a least upper bound in A. The least upper bound need not appear in the chain itself. This will prove useful in giving a mathematical meaning to the behaviour of programs.

Well founded induction

Given a well founded relation, $<$, on a set A and a Boolean proposition, P, involving elements of A, let M be the set of minimal elements in A (with respect to $<$). The *principle of well founded induction* states that, if

- $\forall\, m \in \mathrm{M} \,.\, \mathrm{P}(m)$ is true, and
- $\forall\, b \in \mathrm{A} \,.\, [(\forall\, c \in \mathrm{A} \,.\, c < b \Rightarrow \mathrm{P}(c)) \Rightarrow \mathrm{P}(b)]$,

then $\forall\, a \in \mathrm{A} \,.\, \mathrm{P}(a)$. These are rather like the base case and inductive step in mathematical induction. In fact we can even omit the first condition if we understand $c < b \Rightarrow \mathrm{P}(c)$ to be true if $b \in \mathrm{M}$ (so there is no $c < b$).

Examples

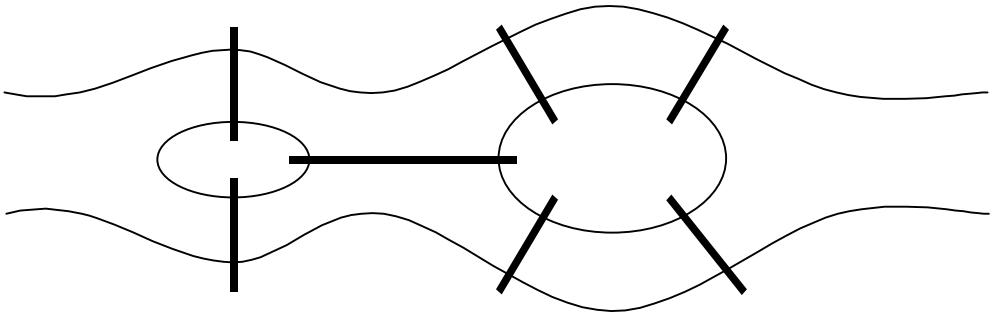
- Ackermann's function is defined by

```
fun ack (0, n) = n + 1
  | ack (m, 0) = ack (m-1, 1)
  | ack (m, n) = ack (m-1, ack (m, n-1));
```

  Is `ack` well defined for all values of `m` and `n` ≥ 0? The answer is "yes" and the proof uses well founded induction on the arguments in $\mathbb{N}_0 \times \mathbb{N}_0$ under the lexicographic order.

  Given an argument pair `(m, n)`, observe that the definition only uses applications of `ack` with argument pairs that come earlier in the lexicographic order, so `ack (m, n)` is well defined if they are. However, `ack` is well defined for the (unique) minimal argument pair `(0, 0)`, so it is well defined for all argument pairs.

- The town of Königsberg spans a river with two islands linked to the banks and each other by seven bridges:



  Is it possible to set out from any point in the town and cross each bridge exactly once, returning to the starting point? In this case the answer is "no".

  In general, this is the problem of finding an *Eulerian circuit* in a graph. A graph consists of a set of *nodes* or *vertices* (the two river banks and the two islands in Königsberg) linked by *arcs* or *edges* (the bridges). Formally, $\mathrm{G} = (\mathrm{V}, \mathrm{E})$ where V is the set of vertices, E the set of edges and $\mathrm{E} \subseteq \mathrm{V} \times \mathrm{V}$ so E is just a relation on V. Often we will consider directed graphs, but in this case E is symmetric and the arcs are not directed. A connected graph has an Eulerian circuit if (and only if) every vertex has even degree, that is, it has an even number of edges connected to it.

Clearly this condition is necessary, and the proof that it is also sufficient uses induction on the set of graphs under the product order: $G_1 \leq G_2 \Leftrightarrow (V_1 \subseteq V_2) \wedge (E_1 \subseteq E_2)$, which will be well founded if V_1 and V_2 are finite.

Observe that the empty graph $G = (\varnothing, \varnothing)$ is uniquely minimal with respect to this ordering and satisfies the theorem.

Consider a connected graph G where every node has even degree. Pick a random vertex and set out on a circuit. Every vertex has even degree, so we only stop when we have returned to the start. Delete the edges in this circuit from G. The resulting graph will have a number of connected components, each of which precedes the original graph in the product order and so each has an Eulerian circuit (or is an isolated vertex). Link each of these into the original circuit to give an Eulerian circuit for the whole graph.

Exercises

1. Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ and $C = \{x, y, z\}$, and let $R = \{(1, a), (2, d), (3, a), (3, b), (3, d)\}$ and $S = \{(b, x), (b, z), (c, y), (d, z)\}$. What is the composition of R and S, $R \circ S$?

2. Let $A = \{1, 2, 3, 4\}$ and consider the relation $R = \{(1, 1), (2, 2), (2, 3), (3, 2), (4, 2), (4, 4)\}$ on A. Is R reflexive, symmetric, anti-symmetric or transitive? Find the reflexive, symmetric and transitive closures of R.

3. If $|A| = k$ and $|B| = m$, how many relations are there between A and B?

   If further $|C| = n$, how many ternary relations are there in $A \times B \times C$? [*Hint:* a binary relation is just a subset of $A \times B$, so a ternary relation is just a subset of $A \times B \times C$.]

4. Let $A = \{1, 2, 3\}$. List all the partitions of A. How many equivalence relations are there on A? How many relations are there on A?

5. Let R and S be relations between A and B. Show that, if $R \subseteq S$, then $R^{-1} \subseteq S^{-1}$. Prove that $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$ and $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$.

6. Give an example of a relation R on a set A with $|A| = n$ such that $t(R) \neq R^1 \cup R^2 \cup \ldots \cup R^{n-1}$.

7. Show that the smallest equivalence relation containing the two equivalence relations R and S on a set A is $t(R \cup S)$.

8. Define a relation R on $\mathbb{N}$ by $(x, y) \in R \Leftrightarrow \exists$ prime $p \,.\, y = px$. Describe in words the reflexive, symmetric and transitive closures of R.

   Which of the following are true:

   - $r(s(R)) = s(r(R))$
   - $r(t(R)) = t(r(R))$
   - $s(t(R)) = t(s(R))$

   Which of them hold for all relations on $\mathbb{N}$?

   Express the smallest equivalence relation containing an arbitrary relation using the symmetric, reflexive and transitive closures.

   What is the smallest partial order containing R? Is it possible to find the smallest partial order containing an arbitrary relation?

9. Give two topological sorts of $\mathbb{N} \times \mathbb{N}$ that respect the product order. One should have the property that, given any point $(x, y) \in \mathbb{N} \times \mathbb{N}$, any infinite subset of $\mathbb{N} \times \mathbb{N}$ should include a point (x', y') with $(x, y) < (x', y')$ and the other should cause this property not to hold in general.

Functions

A (*total*) *function* f from a set A to a set B, written $f\colon \mathrm{A} \to \mathrm{B}$, is a relation $f \subseteq \mathrm{A} \times \mathrm{B}$ that satisfies:

- Uniquely defined: $(a, b_1) \in f \wedge (a, b_2) \in f \Rightarrow b_1 = b_2$
- Everywhere defined: $\forall\, a \in \mathrm{A} \;\exists\, b \in \mathrm{B} \;.\; (a, b) \in f$

We write $f(a)$ for the unique element $b \in \mathrm{B}$ with $(a, b) \in f$ to give the usual notation.

If only the first of these two properties holds, then f is a *partial function* from A to B which is undefined for certain elements of A. It is sometimes convenient to refer to this undefined value explicitly as $\perp$ (pronounced *bottom*). A partial function from A to B is the same as a total function from A to $(\mathrm{B} + \{\perp\})$.

A is called the *domain* of f, and B is called its *range*.

The set $f(\mathrm{A}) = \{b \in \mathrm{B} \mid \exists\, a \in \mathrm{A} \;.\; f(a) = b\}$ is the *image* of A under f.

Given two functions $f\colon \mathrm{A} \to \mathrm{B}$ and $g\colon \mathrm{B} \to \mathrm{C}$, the *composition* of f and g is the function $h\colon \mathrm{A} \to \mathrm{C}$ defined by $h(a) = g(f(a))$. This is just $f \circ g$ the composition of f and g as relations, and explains why $g \circ f$ is a sensible notation for that composition.

It is sometimes convenient to write $\mathrm{A} \to \mathrm{B}$ for the set of all functions from A to B.

Counting functions

If A and B are finite sets with $|\mathrm{A}| = m$ and $|\mathrm{B}| = n$, then $|\mathrm{A} \to \mathrm{B}| = n^m$.

$\mathrm{A} \to \mathrm{B}$ is sometimes written as B^{A}, so $|\mathrm{B}^{\mathrm{A}}| = |\mathrm{B}|^{|\mathrm{A}|}$.

Classifications of functions

A function $f\colon \mathrm{A} \to \mathrm{B}$ is *injective* (also described as *one-to-one* or *1-1*) if $\forall\, a_1, a_2 \in \mathrm{A}$. $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$.

Example: $f\colon \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x^2$ is injective, but $f\colon \mathbb{Z} \to \mathbb{Z}$ defined the same way would not be.

A function $f\colon \mathrm{A} \to \mathrm{B}$ is *surjective* (also described as *onto*) if $\forall\, b \in \mathrm{B} \;.\; \exists\, a \in \mathrm{A} \;.\; f(a) = b$.

Example: $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x + 1$ is surjective, but $f\colon \mathbb{N} \to \mathbb{N}$ defined the same way would not be.

A function $f\colon \mathrm{A} \to \mathrm{B}$ is *bijective* (also described as a *one-to-one correspondence*) if it is both injective and surjective. A bijection from a set to itself is a *permutation*.

If a function $f\colon \mathrm{A} \to \mathrm{B}$ is injective, then its inverse as a relation $f^{-1} \subseteq \mathrm{B} \times \mathrm{A}$ satisfies the uniquely defined criterion for a function. If f is surjective, then f^{-1} satisfies the everywhere defined criterion. So, given a bijection $f\colon \mathrm{A} \to \mathrm{B}$, its inverse as a relation is also a function $f^{-1}\colon \mathrm{B} \to \mathrm{A}$. In fact f^{-1} is also a bijection.

Given a universe Ω, define a relation on $\mathcal{P}(\Omega)$ by $\mathrm{A} \approx \mathrm{B}$ if and only if there is a bijection from A to B. This is an equivalence relation and two sets are said to have the same *cardinality* if they are related by it. For finite sets this means that they have the same number of elements and it is reasonable to extend the definition to infinite sets.

Observe that $\mathbb{N}_0 \approx \mathbb{N}$ (map $n \to n + 1$). Indeed, $\mathbb{Z} \approx \mathbb{N}$ (map $z \to 2z + 1$ if $z \geq 0$ and $-2z$ otherwise) and $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$ (map $(m, n) \to \frac{1}{2}(m+n-1)(m+n-2) + n$). In fact, $\mathbb{Q} \approx \mathbb{N}$ as well, but proving that requires a little preparation.

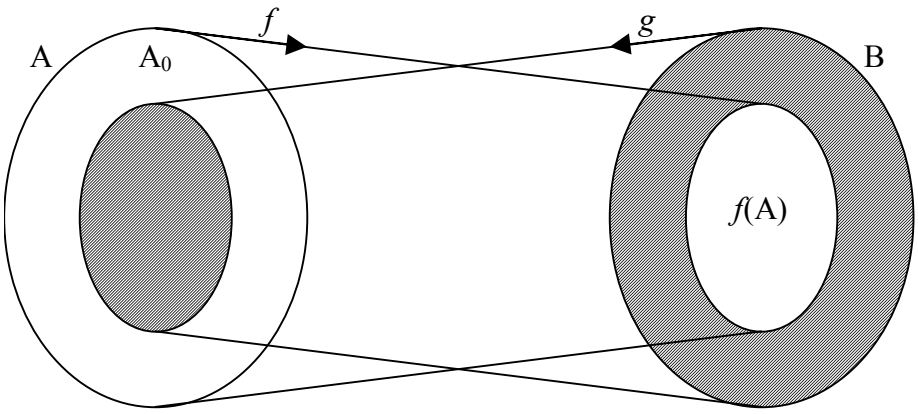
Sorting

If A is a finite, totally ordered set with $|\mathrm{A}| = m$, there are $m!$ permutations of A. Sorting A involves choosing the single permutation from these $m!$ that makes a chain in A. Encoding this in binary would require $\log_2(m!) \approx m \log_2(m)$ bits of information. Any algorithm to sort A would yield one bit of information for each comparison of two elements and so we should not expect to do better than $\mathrm{O}(m \log_2(m))$ comparisons.

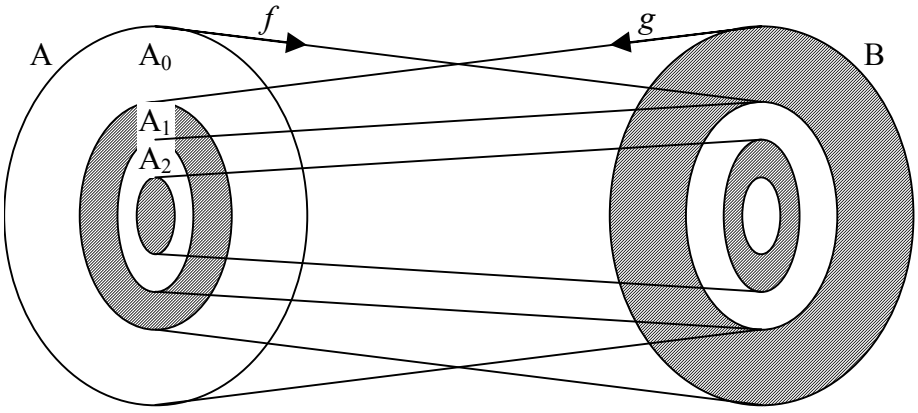
Schröder-Bernstein theorem

Suppose $f\colon \mathrm{A} \to \mathrm{B}$ and $g\colon \mathrm{B} \to \mathrm{A}$ are injections. Then there is a bijection from A to B.

Proof: Let $\mathrm{B}_0 = \mathrm{B} \setminus f(\mathrm{A})$ and $\mathrm{A}_0 = \mathrm{A} \setminus g(\mathrm{B})$.



Define $\mathrm{B}_n = f(\mathrm{A}_{n-1})$ and $\mathrm{A}_n = g(\mathrm{B}_{n-1})$ for $n > 0$. Observe that $f\colon \mathrm{A}_{n-1} \to \mathrm{B}_n$ and $g\colon \mathrm{B}_{n-1} \to \mathrm{A}_n$ are bijections.



Now define $\mathrm{A}_{\text{even}} = \mathrm{A}_0 \cup \mathrm{A}_2 \cup \mathrm{A}_4 \cup \cdots = \bigcup_{\text{even } n} \mathrm{A}_n$ and define A_{odd}, B_{even} and B_{odd} similarly.

Let $\mathrm{A}_\infty = \mathrm{A} \setminus (\mathrm{A}_{\text{even}} \cup \mathrm{A}_{\text{odd}})$ so $\mathrm{A} = \mathrm{A}_{\text{even}} \cup \mathrm{A}_{\text{odd}} \cup \mathrm{A}_\infty$ and these three sets are disjoint. Proceed similarly for B.

Define $h\colon \mathrm{A} \to \mathrm{B}$ to be equal to f on A_{even}, to g^{-1} on A_{odd} and to either on A_∞, which gives the desired bijection.

Countability

Recall that two sets have the same cardinality if there is a bijection between them. A set is *countably infinite* if it has the same cardinality as $\mathbb{N}$. This cardinality is known as $\aleph_0$ (the Hebrew letter Aleph with a subscript of 0). A *countable* set is either finite or countably infinite.

The Schröder-Bernstein theorem shows that any set, A, is countable if, and only if, there is an injection $\mathrm{A} \to \mathbb{N}$ or, equivalently, there is a surjection $\mathbb{N} \to \mathrm{A}$.

Example: $\mathbb{Q}$ is countable. We can construct injections $\mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$, $\mathbb{Z} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ and $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, which can be composed to form an injection $\mathbb{Q} \to \mathbb{N}$ and so $\mathbb{Q}$ is countable.

Countable union of countable sets

Suppose that $\{\mathrm{A}_i \mid i \in \mathrm{I}\}$ is a countable collection of countable sets. That is, the index set I is countable and for each $i \in \mathrm{I}$ the set A_i is countable. Then $\bigcup_{i \in I} A_i$ is countable.

Proof: I is countable, so there is an injection $f\colon \mathrm{I} \to \mathbb{N}$. For each $i \in \mathrm{I}$ the set A_i is countable, so there is an injection $g_i\colon \mathrm{A}_i \to \mathbb{N}$. Define $h\colon \cup \mathrm{A}_i \to \mathbb{N}$ as follows. For any $x \in \cup \mathrm{A}_i$, let m be the minimal element of $\{ f(i) \mid x \in \mathrm{A}_i \}$ and let j be $f^{-1}(m)$. Now let $h(x) = p_m^{g_j(x)}$ where p_m is the m^{th} prime. Then h is an injection and so $\cup \mathrm{A}_i$ is countable.

Uncountability of $\mathcal{P}(\mathbb{N})$

Suppose that $\mathcal{P}(\mathbb{N})$ is countable, so there is a bijection $f\colon \mathbb{N} \to \mathcal{P}(\mathbb{N})$.

Let $\mathrm{A} = \{n \in \mathbb{N} \mid n \notin f(n)\} \subseteq \mathbb{N}$ so $\mathrm{A} \in \mathcal{P}(\mathbb{N})$, and let $a \in \mathbb{N}$ be such that $f(a) = \mathrm{A}$.

Now ask whether or not $a \in \mathrm{A}$? Suppose so, then $a \notin f(a) = \mathrm{A}$, a contradiction. Suppose not, then $a \in f(a) = \mathrm{A}$, another contradiction. Hence f could not exist and so $\mathcal{P}(\mathbb{N})$ is not countable.

Uncountability of $\mathbb{R}$

Suppose that $\mathbb{R}$ is countable, so there is a bijection $g\colon \mathbb{R} \to \mathbb{N}$. Define $h\colon \mathcal{P}(\mathbb{N}) \to \mathbb{R}$ as follows. Given $\mathrm{A} \subseteq \mathbb{N}$, let $h(\mathrm{A}) = \sum_{a \in \mathrm{A}} 10^{-a}$, giving a decimal number between 0 and 1 with ones in digit positions corresponding to members of A and zeroes elsewhere. h is an injection, so the composition $h \circ g\colon \mathcal{P}(\mathbb{N}) \to \mathbb{N}$ is also an injection. But this would imply that $\mathcal{P}(\mathbb{N})$ were countable which gives a contradiction, so $\mathbb{R}$ is not countable.

Investigating cardinality

We have now seen two ways to investigate the cardinality of a set:

- To prove that the set A is countable, we must construct an injection from A into a set that is known to be countable. For example, $\mathbb{Q}$ was shown to be countable by constructing an injection into $\mathbb{N}$.
- To prove that the set A is uncountable, we must construct an injection from a set that is known to be uncountable into A. For example, $\mathbb{R}$ was shown to be uncountable by construction an injection from $\mathcal{P}(\mathbb{N})$.

Algebraic and transcendental numbers

An *algebraic* number is a real number, x, that is the root of a polynomial with integer coefficients: $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots + a_n x^n = 0$ with $a_i \in \mathbb{Z}$ and for some $n \in \mathbb{N}$.

There are only countably many such equations and each has only a finite number of roots, so there are only countably many algebraic numbers. However, there are uncountably many real numbers. Therefore there exist *transcendental* numbers which are not algebraic. Indeed, most (in some sense) numbers are transcendental. π and e (the base of natural logarithms) are both examples, but proving that they (or any other numbers) are transcendental is harder…

Exercises

1. Let $\mathrm{A}_2 = \{1, 2\}$ and $\mathrm{A}_3 = \{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$. List the elements of the four sets $\mathrm{A}_i \to \mathrm{A}_j$ for $i, j \in \{2, 3\}$. Annotate those elements which are injections, surjections and bijections.
2. Let B be a fixed subset of the set A. Define a relation R on the subsets of A in $\mathcal{P}(\mathrm{A})$ by $(\mathrm{X}, \mathrm{Y}) \in \mathrm{R} \Leftrightarrow \mathrm{X} \cap \mathrm{B} = \mathrm{Y} \cap \mathrm{B}$. Show that R is an equivalence relation and describe a bijection between $\mathcal{P}(\mathrm{A})_{/\mathrm{R}}$ and $\mathcal{P}(\mathrm{B})$.
3. Suppose that $f\colon \mathrm{A} \to \mathrm{B}$ and $g\colon \mathrm{B} \to \mathrm{C}$ are both injective. Show that their composition is also injective. Suppose instead that they are both surjective; show that their composition is surjective too. What can be deduced if f and g are both bijections?
4. If possible, find explicit bijections between the following pairs of sets. If this is not possible in general, explain why and say if any special cases can have bijections.
   - $\mathrm{A} \times (\mathrm{B} \times \mathrm{C}) \leftrightarrow (\mathrm{A} \times \mathrm{B}) \times \mathrm{C}$
   - $\mathrm{A} \times \mathrm{A} \leftrightarrow \mathrm{A}$
   - $\mathrm{A} \times \mathrm{A} \leftrightarrow \mathrm{A} + \mathrm{A}$
   - $[(\mathrm{A} \times \mathrm{B}) \to \mathrm{C}] \leftrightarrow [\mathrm{A} \to (\mathrm{B} \to \mathrm{C})]$
   - $[(\mathrm{A} \to \mathrm{B}) \to \mathrm{C}] \leftrightarrow [\mathrm{A} \to (\mathrm{B} \to \mathrm{C})]$
   - $[(\mathrm{A} + \mathrm{B}) \to \mathrm{C}] \leftrightarrow (\mathrm{A} \to \mathrm{C}) \times (\mathrm{B} \to \mathrm{C})$
5. Let R and S be equivalence relations on A and B respectively with p and q the natural mappings of A and B into $\mathrm{A}_{/\mathrm{R}}$ and $\mathrm{B}_{/\mathrm{S}}$. Suppose that $f\colon \mathrm{A} \to \mathrm{B}$ is an arbitrary function. Show that the following two statements are equivalent:
   - $\exists\, g\colon \mathrm{A}_{/\mathrm{R}} \to \mathrm{B}_{/\mathrm{S}}$ with $p \circ g = f \circ q$.
   - $\forall\, a_1, a_2 \in \mathrm{A}\ .\ (a_1, a_2) \in \mathrm{R} \Rightarrow (f(a_1), f(a_2)) \in \mathrm{S}$.
6. A function $f\colon \mathrm{A} \to \mathrm{B}$ between two partially ordered sets is *monotonic* if it respects the ordering in A and B, that is, $a_1 \leq_{\mathrm{A}} a_2 \Rightarrow f(a_1) \leq_{\mathrm{B}} f(a_2)$. Two partially ordered sets, A and B, are *isomorphic* if there is a monotonic bijection $f\colon \mathrm{A} \to \mathrm{B}$ whose inverse f^{-1} is also monotonic. Show that $(\mathcal{P}(\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}), \subseteq)$ and $(\{0, 1\}^3, \leq_{\mathrm{P}})$ are isomorphic.
7. If A and B are finite sets with $|\mathrm{A}| = m$ and $|\mathrm{B}| = n$, how many partial functions are there $\mathrm{A} \to \mathrm{B}$?
8. Show that the collection of all finite subsets of $\mathbb{N}$ is countable but that the collection of all subsets of $\mathbb{N}$ is not countable.

9. By considering indicator functions or otherwise, find a bijection from the set of functions $\{f\colon \mathbb{N} \to \{0, 1\}\}$ to $\mathcal{P}(\mathbb{N})$ and so deduce that the former is uncountable.

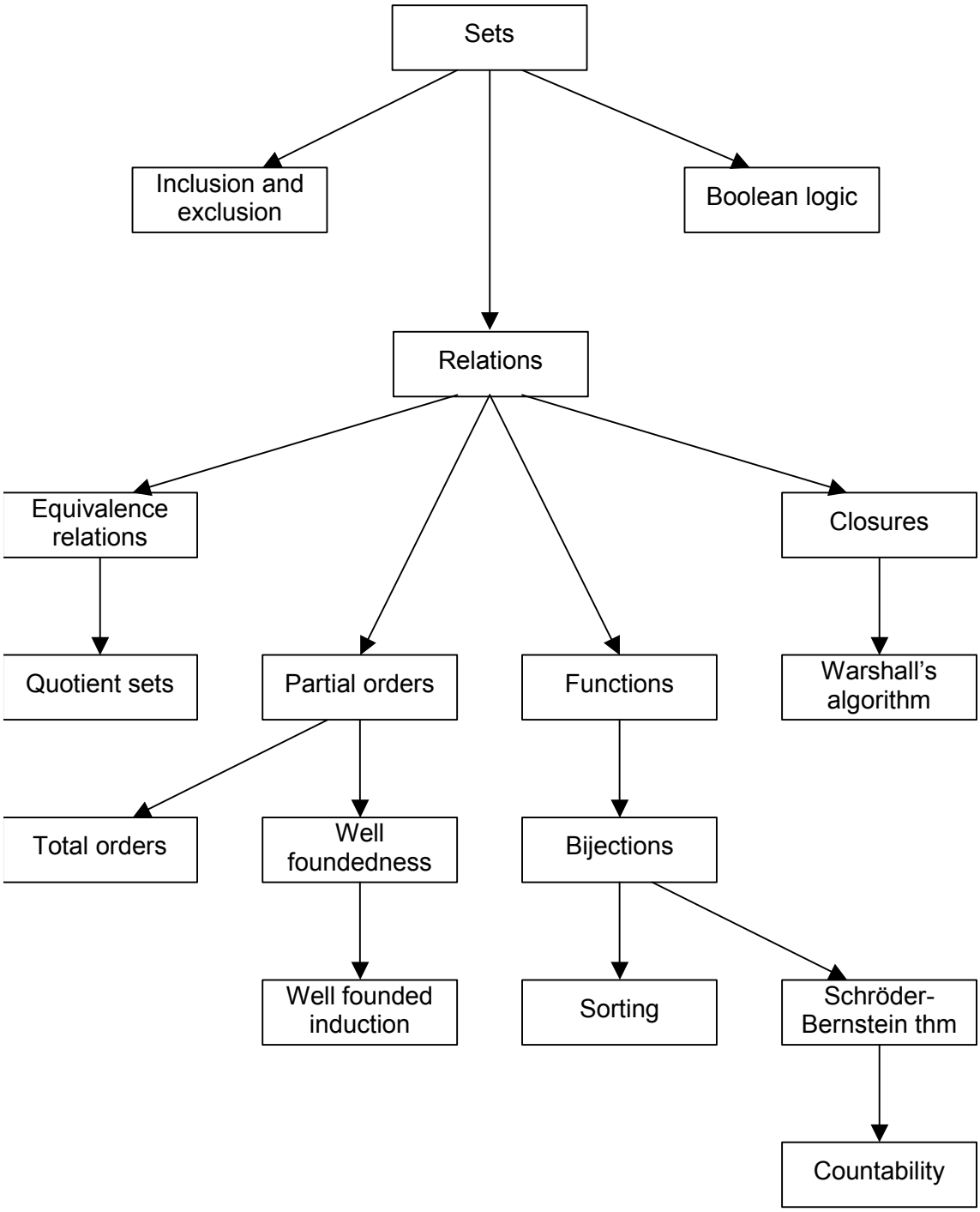
10. Which of the following sets are finite, which are countably infinite and which are uncountable?

    - $\{f\colon \mathbb{N} \to \{0, 1\} \mid \forall\, n \in \mathbb{N} \,.\, f(n) \leq f(n+1)\}$
    - $\{f\colon \mathbb{N} \to \{0, 1\} \mid \forall\, n \in \mathbb{N} \,.\, f(2n) \neq f(2n+1)\}$
    - $\{f\colon \mathbb{N} \to \{0, 1\} \mid \forall\, n \in \mathbb{N} \,.\, f(n) \neq f(n+1)\}$
    - $\{f\colon \mathbb{N} \to \mathbb{N} \mid \forall\, n \in \mathbb{N} \,.\, f(n) \leq f(n+1)\}$
    - $\{f\colon \mathbb{N} \to \mathbb{N} \mid \forall\, n \in \mathbb{N} \,.\, f(n) \geq f(n+1)\}$

11. Show that $\mathbb{Q} \times \mathbb{Q}$ is countable and deduce that any collection of disjoint discs (that is, circular areas) in the plane $\mathbb{R}^2$ is countable. Is the same true if "discs" is replaced by "circles" (that is, just the perimeters of the circles)?

Revision guide

The following diagram shows the development of the key ideas presented in the second half of the course:



Lecture review form

If high lecturing standards are to be maintained and lower standards to be raised, it is important for lecturers to receive feedback about their lectures. Consequently, we would be grateful if you would complete this questionnaire and return it to the Student Administration Office. A digest of the information will be passed to the Staff-Student Liaison and Teaching Committees.

Discrete Mathematics (Part B)
Lent 2002

Please tick the boxes below:

Interest

Tedious	Uninteresting	Interesting	Exciting

Level of material

Much too basic	Too basic	Slightly basic	About right	Slightly complicated	Too complicated	Much too complicated

Breadth of coverage

Much too general	Too general	Slightly general	About right	Slightly specific	Too specific	Much too specific

Organisation of lectures

Chaotic	Confused	Adequate	Brilliant

Assumptions

Assumed too little	About right	Assumed too much

Ease of understanding

Incomprehensible	Confused	Adequate	Clear

Speed

Much too slow	Too slow	Slightly slow	About right	Slightly fast	Too fast	Much too fast

Delivery

Incoherent	Halting	Adequate	Fluent

Notes

Poor	Adequate	Excellent

Supervision

Poor	Adequate	Excellent

PTO

Best thing about the course

Worst thing about the course

Further comments