Discrete Mathematics

	topic
week 1	***Sets***
week 2	***Functions***
week 3	***Counting***
week 4	***Relations***
week 5	***Sequences***
week 6	***Modular Arithmetic***
week 7	***Asymptotic Notation***
week 8	***Orders***

Jonathan Barrett
jonathan.barrett@cs.ox.ac.uk

Material by Andrew Ker
University of Oxford
Department of Computer Science

Discrete Mathematics

Jonathan Barrett
jonathan.barrett@cs.ox.ac.uk
Material by Andrew Ker
University of Oxford
Department of Computer Science

Chapter 8: Orders

Definitions

Relations like $\leq$ and $|$ put the elements of the set on which they are defined into **order**.

- A **preorder** is a reflexive, transitive relation.
- A **partial order** is a reflexive, antisymmetric, transitive relation.
- A **linear order** is an antisymmetric, transitive, **total** relation.

$\textbf{for all } a\&b,\ a\,R\,b \textbf{ or } b\,R\,a$

Definitions

Relations like $\leq$ and $|$ put the elements of the set on which they are defined into **order**.

- A **preorder** is a reflexive, transitive relation.
- A **partial order** is a reflexive, antisymmetric, transitive relation.
- A **linear order** is an antisymmetric, transitive, **total** relation.

for all $a \& b$, $a\,R\,b$ or $b\,R\,a$

Linear orders are also known as **total orders**. The "order" can indicate just the relation, but usually also includes the set on which the relation is defined. Some people write **poset** for "partially ordered set".

Relationship:

linear order $\Rightarrow$ partial order $\Rightarrow$ preorder

Definitions

Relations like $\leq$ and $|$ put the elements of the set on which they are defined into **order**.

- A **preorder** is a reflexive, transitive relation.
- A **partial order** is a reflexive, antisymmetric, transitive relation.
- A **linear order** is an antisymmetric, transitive, **total** relation.

for all $a \& b$, $a\,R\,b$ or $b\,R\,a$

Linear orders are also known as **total orders**. The "order" can indicate just the relation, but usually also includes the set on which the relation is defined. Some people write **poset** for "partially ordered set".

Relationship:

linear order $\Rightarrow$ partial order $\Rightarrow$ preorder

Fact: the converse of a preorder (partial order, linear order) is still a preorder (partial order, linear order).

Chains and Antichains

Fix a set A and an order $\preceq$ on A.

If $a \preceq b$ or $b \preceq a$ we say that a and b are **comparable**.

Chains and Antichains

Fix a set A and an order $\preceq$ on A.

If $a \preceq b$ or $b \preceq a$ we say that a and b are **comparable**.

A **chain** is a subset of A of which all pairs are comparable.
An **antichain** is a subset of A of which no pairs are comparable.

In a linear order, all elements are comparable and so all sets are chains. This is not necessarily so in partial orders.

An interesting challenge is to find the largest antichain (i.e. largest set of pairwise incomparable elements) for various finite orders.

Orders on Cartesian Products

If we have an order $\preceq$ on a set A we can create orders on $A \times A$ in a number of ways:

The **product order**

$$(x, y) \preceq_P (x', y') \quad \Leftrightarrow \quad x \preceq x' \text{ and } y \preceq y'.$$

Orders on Cartesian Products

If we have an order $\preceq$ on a set A we can create orders on $A \times A$ in a number of ways:

The **product order**

$$(x, y) \preceq_P (x', y') \quad \Leftrightarrow \quad x \preceq x' \text{ and } y \preceq y'.$$

The **lexicographic order**

$$(x, y) \preceq_L (x', y') \quad \Leftrightarrow \quad x \prec x' \text{ or } (x \simeq x' \text{ and } y \preceq y').$$

where
$$x \prec x' \ means\ x \preceq x' \ and\ x' \not\preceq x$$
$$x \simeq x' \ means\ x \preceq x' \ and\ x' \preceq x$$

NB In the case where $\preceq$ is a partial order, or a linear order:
$\prec$ is equivalent to: $x \preceq x'$ and $x \neq x'$,
$x \simeq x'$ is the same as $x = x'$.

Orders on Cartesian Products

If we have an order $\preceq$ on a set A we can create orders on $A \times A$ in a number of ways:

The **product order**

$$(x, y) \preceq_P (x', y') \quad \Leftrightarrow \quad x \preceq x' \text{ and } y \preceq y'.$$

The **lexicographic order**

$$(x, y) \preceq_L (x', y') \quad \Leftrightarrow \quad x \prec x' \text{ or } (x \simeq x' \text{ and } y \preceq y').$$

<u>Claim</u> If $\preceq$ is a (preorder/partial order/linear order) on A then $\preceq_L$ is also a (preorder/partial order/linear order) on $A \times A$

If $\preceq$ is a (preorder/partial order) on A then $\preceq_P$ is also a (preorder/partial order) on $A \times A$

If $\preceq$ is a linear order on A then $\preceq_P$ **might not be** a linear order on $A \times A$

Hasse Diagrams

We can **draw** a partial or linear order $\preceq$ on a set A more concisely than showing the full digraph of all related pairs.

A **Hasse diagram** is a graph, drawn in the plane, with vertices corresponding to the elements of A and an edge going **up** from a to b if $a \prec b$ and there is no element x with $a \prec x \prec b$.

Hasse Diagrams

We can **draw** a partial or linear order $\preceq$ on a set A more concisely than showing the full digraph of all related pairs.

A **Hasse diagram** is a graph, drawn in the plane, with vertices corresponding to the elements of A and an edge going **up** from a to b if $a \prec b$ and there is no element x with $a \prec x \prec b$.

This construction, which removes reflexive loops and all edges which follow by transitivity, is known as the <u>cover relation</u>.

(Hasse diagrams of infinite orders cannot be drawn in their entirety. We don't try to draw Hasse diagrams of non-antisymmetric preorders, because they have cycles.)

Upper and Lower Bounds

Let A be a set, ordered by a partial order $\preceq$, and let $S \subseteq A$.

An element $m \in A$ is an **upper bound** for S if $x \preceq m$ for all $x \in S$.
An element $m \in A$ is a **lower bound** for S if $m \preceq x$ for all $x \in S$.

m is the **maximum** of S if it is an upper bound and $m \in S$.
m is the **minimum** of S if it is a lower bound and $m \in S$.

Upper and Lower Bounds

Let A be a set, ordered by a partial order $\preceq$, and let $S \subseteq A$.

An element $m \in A$ is an **upper bound** for S if $x \preceq m$ for all $x \in S$.
An element $m \in A$ is a **lower bound** for S if $m \preceq x$ for all $x \in S$.

m is the **maximum** of S if it is an upper bound and $m \in S$.
m is the **minimum** of S if it is a lower bound and $m \in S$.

Warnings:

- *A set need not have an upper or lower bound.*
- *When they exist, upper/lower bounds are not usually unique.*
- *A set might have an upper/lower bound but no maximum/minimum.*

LUB and GLB

Let A be a set, ordered by a partial order $\preceq$, and let $S \subseteq A$.

An element $m \in A$ is a **least upper bound (lub)** for S if

- m is an upper bound for S: $x \preceq m$ for all $x \in S$, and
- if m' is any other upper bound for S, then $m \preceq m'$.

a.k.a. supremum (sup) or join

LUB and GLB

Let A be a set, ordered by a partial order $\preceq$, and let $S \subseteq A$.

An element $m \in A$ is a **least upper bound (lub)** for S if

- m is an upper bound for S: $x \preceq m$ for all $x \in S$, and
- if m' is any other upper bound for S, then $m \preceq m'$.

a.k.a. supremum (sup) or join

An element $m \in A$ is a **greatest lower bound (glb)** for S if

- m is a lower bound for S: $m \preceq x$ for all $x \in S$, and
- if m' is any other lower bound for S, then $m' \preceq m$.

a.k.a. infimum (inf) or meet

LUB and GLB

Let A be a set, ordered by a partial order $\preceq$, and let $S \subseteq A$.

An element $m \in A$ is a **least upper bound (lub)** for S if

a.k.a. supremum (sup) or join

– m is an upper bound for S: $x \preceq m$ for all $x \in S$, and

– if m' is any other upper bound for S, then $m \preceq m'$.

An element $m \in A$ is a **greatest lower bound (glb)** for S if

a.k.a. infimum (inf) or meet

– m is a lower bound for S: $m \preceq x$ for all $x \in S$, and

– if m' is any other lower bound for S, then $m' \preceq m$.

- *A set need not have a lub/glb, even if it does have a lower/upper bound.*
- *When they exist, the lub/glb are unique.*

LUB and GLB

Let A be a set, ordered by a partial order $\preceq$, and let $S \subseteq A$.

An element $m \in A$ is a **least upper bound (lub)** for S if

- m is an upper bound for S: $x \preceq m$ for all $x \in S$, and
- if m' is any other upper bound for S, then $m \preceq m'$.

a.k.a. supremum (sup) or join

An element $m \in A$ is a **greatest lower bound (glb)** for S if

- m is a lower bound for S: $m \preceq x$ for all $x \in S$, and
- if m' is any other lower bound for S, then $m' \preceq m$.

a.k.a. infimum (inf) or meet

- ***A set need not have a lub/glb, even if it does have a lower/upper bound.***
- ***When they exist, the lub/glb are unique.***

If every **pair** has a lub & glb then the order is called a **lattice**. The lub and glb binary operators can be written $\sqcup$ and $\sqcap$.

If every **set** has a lub & glb then the order is a **complete lattice**.

LUB and GLB in Linear Orders

If $\preceq$ is a **linear** order on A, there is an equivalent definition of lub/glb.

An element $m \in A$ is a **least upper bound (lub)** for S if

- m is an upper bound for S: $x \preceq m$ for all $x \in S$, and
- if $a \prec m$ then there is an element $x \in S$ with $a \prec x$.

LUB and GLB in Linear Orders

If $\preceq$ is a **linear** order on A, there is an equivalent definition of lub/glb.

An element $m \in A$ is a **least upper bound (lub)** for S if

- m is an upper bound for S: $x \preceq m$ for all $x \in S$, and
- if $a \prec m$ then there is an element $x \in S$ with $a \prec x$.

An element $m \in A$ is a **greatest lower bound (glb)** for S if

- m is a lower bound for S: $m \preceq x$ for all $x \in S$, and
- if $m \prec a$ then there is an element $x \in S$ with $x \prec a$.

This can be more convenient, particularly for proving algebraic properties of lub and glb.

LUB and GLB in Linear Orders

If $\preceq$ is a **linear** order on A, there is an equivalent definition of lub/glb.

An element $m \in A$ is a **least upper bound (lub)** for S if

- m is an upper bound for S: $x \preceq m$ for all $x \in S$, and
- if $a \prec m$ then there is an element $x \in S$ with $a \prec x$.

An element $m \in A$ is a **greatest lower bound (glb)** for S if

- m is a lower bound for S: $m \preceq x$ for all $x \in S$, and
- if $m \prec a$ then there is an element $x \in S$ with $x \prec a$.

This can be more convenient, particularly for proving algebraic properties of lub and glb.

Claim In the usual linear order on $\mathbb{R}$, if lub $A = m$ then

$$\text{lub}\{2x \mid x \in A\} = 2m.$$

Sentences of the Form $\forall x . \exists y . P$

To prove something like:

Claim   For any object (x) there is another (y) such that P is true.

Imagine that we are **given** x: we must find a corresponding y (which will probably depend on x) which makes P true, and then prove that it works.

We often begin the proof without knowing what y will work, hoping to fill it in later.

Sentences of the Form $\forall x.\exists y.P$

To prove something like:

<u>Claim</u> For any object (x) there is another (y) such that P is true.

Imagine that we are **given** x: we must find a corresponding y (which will probably depend on x) which makes P true, and then prove that it works.

We often begin the proof without knowing what y will work, hoping to fill it in later.

<u>Claim</u> With respect to the linear order $\leq$ on $\mathbb{Q}$,
$\mathbb{Q} \cap (0, \sqrt{2})$ has upper bounds but no lub.

Diversion: Order Isomorphisms

Let A and B be sets, with orders $\preceq_A$ and $\preceq_B$.

An **order isomorphism** between A and B is a bijection $f : A \to B$ satisfying

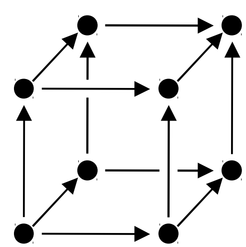
$$a \preceq_A a' \quad \Leftrightarrow \quad f(a) \preceq_B f(a').$$

Diversion: Order Isomorphisms

Let A and B be sets, with orders $\preceq_A$ and $\preceq_B$.
An **order isomorphism** between A and B is a bijection $f : A \to B$ satisfying

$$a \preceq_A a' \quad \Leftrightarrow \quad f(a) \preceq_B f(a').$$

<u>Example</u> Vertices of a cube ordered by



and $\mathcal{P}(\{1,2,3\})$ ordered by $\subseteq$

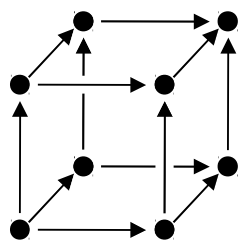
Diversion: Order Isomorphisms

Let A and B be sets, with orders $\preceq_A$and $\preceq_B$

An **order isomorphism** between A and B is a bijection $f : A \to B$ satisfying

$$a \preceq_A a' \quad \Leftrightarrow \quad f(a) \preceq_B f(a').$$

Example Vertices of a cube ordered by



and $\mathcal{P}(\{1, 2, 3\})$ ordered by $\subseteq$

The existence of an order isomorphism between A, ordered by $\preceq_A$, and B, ordered by $\preceq_B$, forces them to share certain properties:

If $\preceq_A$ is a partial order, so is $\preceq_B$ (and vice versa).

If $\preceq_A$ is a linear order, so is $\preceq_B$ (and vice versa).

If $\preceq_A$ is a lattice, so is $\preceq_B$ (and vice versa).

Discrete Mathematics

Jonathan Barrett
jonathan.barrett@cs.ox.ac.uk
Material by Andrew Ker
University of Oxford
Department of Computer Science

End of Chapter 8

Course Aims

- Learn terminology of discrete maths, for computer science applications.

1-1, antisymmetric, associative, bag, base case, bijection, binary operator, binomial coefficients, cancellation, cardinality, cartesian product, ceiling, characteristic polynomial, closed interval, codomain, commutative, com-plement, component, composition, contrapositive, converse, counterexample, derangement, digraph, disjoint, distributivity, domain, edge, element, empty set, equivalence class, equivalence relation, exclusive, factorial, floor, function, greatest common divisor, idempotent, identity, image, independent, induction, inductive hypothesis, infix, injective, integers, intersection, interval, inverse, involution, irrational, irreflexive, member, minimal counterexample, modulus, monoid, multinomial coefficients, natural numbers, node, onto, open interval, ordered pair, parity, partial function, partition, permutation, power set, prefix, proof by contradiction, proper subset, range, rational, recurrence relation, recursive, reflexive, relation, relative complement, restriction, sequence, serial, set, subset, superset, surjective, symmetric difference, total, transitive, transitive closure, tuple, union, universe, zero, …

Discrete Mathematics

Jonathan Barrett
jonathan.barrett@cs.ox.ac.uk
Material by Andrew Ker
University of Oxford
Department of Computer Science

The End