Chapter 1: Ordered Sets

Victor Lagerkvist (based on lecture notes by Ulf Nilsson & Wlodek Drabent)

Basic Notions

We briefly summarize basic notions and notation used later on in these notes. For a more elaborate and verbose exposition, see e.g. Grimaldi [1].

[1] R. Grimaldi. *Discrete and Combinatorial Mathematics*. Addison-Wesley, 4th edition, 2000

The set of all natural numbers $\{0, 1, 2, \ldots\}$ is denoted $\mathbb{N}$. The set of all integers is denoted $\mathbb{Z}$, and the subset of all positive integers is denoted $\mathbb{Z}^+$. (So $\mathbb{Z}^+ = \mathbb{N} \setminus \{0\}$.) The rational numbers are denoted by $\mathbb{Q}$ and the real numbers by $\mathbb{R}$. The cardinality of a set A is denoted $|A|$. So when A is finite, $|A| \in \mathbb{N}$ is the number of elements in A. We use an abbreviation "iff" for a common phrase "if and only iff".

Additionally, we assume that the reader is familiar with basic notions from set theory and if A and B are sets then we write $A \cap B$, $A \cup B$, $A \setminus B$, $\bar{A}$, $\mathcal{P}(A) = 2^A$ for intersection, union, difference, complement, and powerset. Sets are frequently defined via set-builder notation, e.g., $\{n \mid n = 2k, k \in \mathbb{N}\}$ would define the set of all even natural numbers[2].

[2] If one does not restrict the types of sets constructible in this way then the resulting (inconsistent) theory is called *naive set theory*. This can be patched by carefully specifying the sets that one is allowed to construct, and the most frequently used theory is known as *Zermelo–Fraenkel set theory with the axiom of choice* (ZFC).

Relations

By $A \times B$ we mean the Cartesian product of two sets A and B. That is, the set of pairs $\{(a, b) \mid a \in A \wedge b \in B\}$. Note that (a, b) and (b, a) are distinct pairs (while $\{a, b\}$ and $\{b, a\}$ is the same set).

Example 1. *We may assume a pair to be a basic notion, but it is interesting to define it by a construction, using basic concepts of set theory. We follow Kuratowski, and by an ordered pair (a, b) of a and b we mean the set $pair_{a,b} = \{\{a\}, \{a, b\}\}$. Note for $b = a$ it is $pair_{a,a} = \{\{a\}\}$ (as $\{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$). Note that x is the first element of a pair p iff $\forall X \in p : x \in X$. It is the second element of p iff $(\exists X \in p : x \in X) \wedge (\forall X_1, X_2 \in p : X_1 \neq X_2 \rightarrow (x \notin X_1 \vee x \notin X_2))$.*

A natural generalization of the notion of a pair is introducing triples (like (a, b, c)), quadruples (e.g. (a, b, a, b)) and, generally, n-tuples $(a_1, \ldots, a_n)$, for $n \geq 0$. (Later on we present a precise construction of n-tuples.) The Cartesian product is naturally generalized: $A_1 \times \ldots \times A_n = \{ (a_1, \ldots, a_n) \mid a_i \in A_i \text{ for } i = 1, \ldots n \}$. When all A_i are equal A we write simply A^n ($n \geq 0$). By A^1 we mean just A, and by A^0 the one-element set $\{\emptyset\}$.

By a (finite) *string* (or *word*) over some alphabet Σ we mean an element u in Σ^n, for some $n \in \mathbb{N}$. In such context the elements of

Σ are called *symbols*, and we require that Σ is finite. (So a string is a tuple of symbols.) The *length* $|u|$ of a string $u \in \Sigma^n$ is n. The set of all finite-length strings is denoted Σ^* and is defined as

$$\Sigma^* := \bigcup_{i \in \mathbb{N}} \Sigma^i.$$

The *empty* string (the only element in Σ^0) is denoted ϵ; its length is 0. Given two strings $u, v \in \Sigma^*$ we write the *concatenation* of u and v as uv. (If $u = (a_1, \ldots, a_n)$ and $v = (b_1, \ldots, b_m)$ then $uv = (a_1, \ldots, a_n, b_1, \ldots, b_m)$.) The length of uv is clearly the sum of the lengths of u and v; $|uv| = |u| + |v|$.

A *relation* (binary relation) R on A and B is a subset of $A \times B$. When $A = B$ we say simply that R is a relation on A. If $(a, b) \in R$ we say that a is related to b (by R). We usually write $R(a, b)$ or $a \; R \; b$ when a is related to b by R. An n-ary relation (where $n \geq 0$) is simply a subset of the Cartesian product $A_1 \times \ldots \times A_n$.

Definition 1. *A binary relation $R \subseteq A \times A$ is said to be*

- *reflexive iff $R(x, x)$ for every $x \in A$,*
- *irreflexive iff $R(x, x)$ for no $x \in A$,*
- *antisymmetric iff $x = y$ whenever $R(x, y)$ and $R(y, x)$,*
- *symmetric iff $R(x, y)$ whenever $R(y, x)$,*
- *transitive iff $R(x, z)$ whenever $R(x, y)$ and $R(y, z)$.*

The *identity relation* on A, i.e. the relation such that $R(x, y)$ iff $x = y$ and $x \in A$, is denoted $\textsc{id}_A$. The *composition* $R_1 \circ R_2$ of two binary relations $R_1 \subseteq A \times B$ and $R_2 \subseteq B \times C$ is a binary relation on $A \times C$ defined by

$$R_1 \circ R_2 := \{(a, c) \in A \times C \mid \exists b \in B \; (R_1(a, b) \wedge R_2(b, c))\}.$$

Relation composition is associative: $(R_1 \circ R_2) \circ R_3 = R_1 \circ (R_2 \circ R_3)$ (prove this).

The identity relation acts as left and right identity for relational composition; if $R \subseteq A \times B$ then $\textsc{id}_A \circ R = R \circ \textsc{id}_B = R$. We adopt the standard notation for iterated composition of a relation $R \subseteq A \times A$. Hence[3]

$$\begin{array}{lcl} R^0 & := & \textsc{id}_A, \\ R^{n+1} & := & R^n \circ R \quad (n \in \mathbb{N}), \\ R^+ & := & \bigcup_{n \in \mathbb{Z}^+} R^n, \\ R^* & := & \bigcup_{n \in \mathbb{N}} R^n. \end{array}$$

[3] Notice that the notation is ambiguous; A^n can denote both an n-fold Cartesian product of a set, or an n-fold composition of a relation A. One has to take care that each time it is clear which reading of the notation is meant.

We refer to R^+ as the *transitive closure* of R, and R^* as the *reflexive and transitive closure* of R. The *inverse* of R is defined as

$$R^{-1} := \{ \, (b, a) \mid R(a, b) \, \}.$$

We leave as an exercise proving that R^+, R^* are transitive relations.

Example 2. *Consider the set $\mathcal{R} = \{R \mid R \subseteq A \times A\}$ of all binary relations over a set A. We may observe that the aforementioned operation of composing two binary relations may be seen as a function which takes two relations $R_1, R_2 \in \mathcal{R}$ and returns a relation $R_1 \circ R_2 \in \mathcal{A}$. Similarly, $R^{-1} \in \mathcal{R}$ for any $R \in \mathcal{R}$, meaning that $^{-1}$ can be seen as a unary function over the set of all binary relations. More generally, one may view $\mathcal{R}$ together with the operations $\circ, {}^{-1}, \cap, \cup, \bar{}$, as forming an* algebra *where $\emptyset$ and A^2 acts as 0 and 1, and where the identity relation ID_A acts as a "relational 1". Such algebras are known as* relation algebras[4] *and occur naturally in e.g. reasoning tasks in artificial intelligence, where the basic relations describe relationships between individual objects such as "a region in $\mathbb{R}^2$ is contained in another region". With these observations we can formulate the aforementioned properties of binary relations in a very succinct way. A binary relation R is:*

[4] Not to be confused with relational algebras in database theory.

- *reflexive iff $\mathrm{ID}A \subseteq R$,*
- *irreflexive iff $R \cap \mathrm{ID}A = \emptyset$,*
- *antisymmetric iff $R \cap R^{-1} = \emptyset$*
- *symmetric iff $R = R^{-1}$,*
- *transitive iff $R \circ R \subseteq R$.*

An advantage to definitions in this algebraic style is that it makes it very easy to generalize to other classes of "similar" algebraic structures.

Example 3. *A transition system is a pair $(C, \Rightarrow)$ where C is a set of configurations, and $\Rightarrow \subseteq C \times C$ is a so-called transition relation. Transition systems provide abstractions of computations; a step-wise process where we move from one configuration to the next as described by the transition relation: $c_0 \Rightarrow c_1 \Rightarrow c_2 \Rightarrow \ldots$. The reflexive and transitive closure of $\Rightarrow$, that is $\Rightarrow^*$, expresses reachability: if $c_0 \Rightarrow^* c_n$ then c_n is reachable, in zero or more steps, from c_0.*

A transition system may also be equipped with a set of initial configurations, a set of terminal configurations, and occasionally also with labelled transitions (the label typically modelling an action corresponding to the transition). In case of labelled transitions the transition relation is ternary, instead of binary, one often writes $c \overset{a}{\Rightarrow} c'$ to state that (c, a, c') is in the relation.

We now define an important class of binary relations.

Definition 2. *A relation which is reflexive, symmetric and transitive is called an* equivalence *relation (or simply* equivalence*).*

Any equivalence $\equiv$ on a set A defines *equivalence classes* (called also *abstraction classes*). The equivalence class $[x]_\equiv$ of an element $x \in A$ is

$$[x]_\equiv = \{\, y \in A \mid y \equiv x \,\}$$

(i.e. the set of elements related to x by $\equiv$). Two distinct equivalence classes are disjoint (prove that if $[x]_\equiv$ and $[y]_\equiv$ have a common element then $[x]_\equiv = [y]_\equiv$). Thus an equivalence $\equiv$ on A induces a *partition* of A into equivalence classes; each element of A is in exactly one equivalence class, and A is the union of the equivalence classes: $A = \bigcup_{x\in A}[x]_\equiv$. The set of equivalence classes of $\equiv$, denoted $A/\equiv$, is called the quotient set: $A/\equiv = \{\, [x] \mid x \in A \,\}$.

Example 4. *The identity relation* $\mathrm{ID}A$ *is trivially an equivalence relation on any set A. For a more interesting example, consider addition modulo k over the natural numbers* $\mathbb{N}$ *for some* $k \geq 1$*, and the equivalence relation* $x \equiv y (\mathrm{mod} k)$ *over* $\mathbb{N}$*, i.e., two natural numbers x and y are related if and only if the remainder when performing integer division with k is the same. Then*

$$\mathbb{N} = [0]_\equiv \cup \ldots \cup [k-1]_\equiv,$$

i.e., $\equiv$ *induces a finite amount of equivalence classes (prove this).*

Example 5. *In geometry, a* bound vector *is a pair of points. Consider a plane, which may be seen as* $\mathbb{R} \times \mathbb{R}$*. Let us introduce a relation* $\sim$ *on bound vectors*

$$((x_1, y_1), (x_2, y_2)) \sim ((x_1', y_1'), (x_2', y_2')) \text{ iff } x_2 - x_1 = x_2' - x_1' \text{ and } y_2 - y_1 = y_2' - y_1'.$$

(Prove that it is an equivalence relation.) It makes vectors with the same length and direction equivalent (but which may have distinct initial points). The equivalence classes of $\sim$ *are called* free vectors*. The equivalence class of a vector* $\vec{v}$ *may be understood as an abstraction of* $\vec{v}$ *in which we consider only its direction and its length, but we abstract from its placement on the plane.*

Functions

A relation $f \subseteq A \times B$ is called a *partial function* from A to B when any $a \in A$ is related by f to at most one element of B. More formally, if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$, for any $a \in A,\ b, c \in B$. Instead of writing $(a, b) \in f$, we sometimes write $(a \mapsto b) \in f$, $a \overset{f}{\mapsto} b$, or use the standard notation $f(a) = b$. For instance, the partial function

$$\{\, 2 \mapsto 1, 4 \mapsto 2, 6 \mapsto 3, 8 \mapsto 4 \,\} \subseteq \mathbb{N} \times \mathbb{N}$$

provides the halves of one-digit even positive numbers. Note that the notation $f(a)$ does not make sense for an a which is not related by f

to some element of B. The set

$$\{\, a \in A \mid (a,b) \in f \text{ for some } b \,\}$$

of those elements for which $f(A)$ is defined is called the *domain* of f (written Domain(f)).

Definition 3. *A partial function $f \subseteq A \times B$ is a* total function*, or simply* function*, when Domain$(f) = A$.*

In other words, when $f(a)$ is defined for any $a \in A$. We write $f\colon A \to B$ to state that f is a function from A to B. Analogically, we introduce notation $f\colon A \twoheadrightarrow B$ for partial functions. Also, $A \to B$, sometimes written B^A, denotes the set of all functions from A to B.

An n-tuple ($n \geq 0$) may be defined as a function from $\{0,\ldots,n-1\}$ to A. For instance, $(5,4,2)$ as $\{0 \mapsto 5, 1 \mapsto 4, 2 \mapsto 2\}$.[5] Hence a Cartesian product A^n may be seen as the space of all functions from $\{0,\ldots,n-1\}$ to A. Similarly, a Cartesian product of distinct sets may be seen as a set of functions $A_0 \times \ldots \times A_{n-1} = \{\, f\colon \{0,\ldots,n-1\} \to A \mid f(a_i) \in A_i \text{ for } i = 0,\ldots n-1 \,\}$ (where $A = \bigcup_{i=0}^{n-1} A_i$). The function space $\mathbb{N} \to A$ can thus be thought of as an infinite product "A^∞", but for reasons to be explained later we usually denote this by A^ω.

A multi-argument function (an *n-ary function*, an n-place function) can be understood as a function whose arguments are n-tuples, i.e. a function $f\colon A_1 \times \cdots \times A_n \to B$ from a Cartesian product.

The *image* of a set $C \subseteq A$ under a (partial) function f from A to B is

$$f(C) = \{\, f(a) \mid a \in C \text{ and } f(a) \text{ exists} \,\}$$

– the set of those elements of B which f assigns to some elements of C.

We say that a set $C \subseteq A$ is *closed* under $f\colon A \to A$ iff $f(x) \in C$ for all $x \in C$, or put alternatively if $f(C) \subseteq C$. Set C is closed under an n-ary function $g\colon A^n \to A$ iff $g(a_1,\ldots,a_n) \in C$ for any elements $a_1,\ldots,a_n \in C$ (alternatively, when $g(C^n) \subseteq C$).

Example 6. *Consider subsets of Σ^*, i.e. all sets of finite strings over some finite alphabet Σ, or languages as we usually refer to them. The set of all regular languages is closed under complementation; for any regular language $L \subseteq \Sigma^*$ we have that its complement $\Sigma^* \setminus L$ is regular. Regular languages are also closed under intersection and union. (Actually this notion can be used to define regular languages: The set of regular languages is the smallest set containing certain basic languages, and closed under certain operations.)*

A subset $B \subseteq A$ corresponds to the function $\mathbf{1}_B\colon A \to \{0,1\}$ given by

$$\mathbf{1}_B = \{\, a \mapsto 0 \mid a \notin B \,\} \cup \{\, a \mapsto 1 \mid a \in B \,\}.$$

[5] Note that we have now two ways of viewing pairs: as 2-tuples, and as defined previously. They are equivalent; to each pair (a,b), i.e. $\{\{a\},\{a,b\}\}$, there corresponds the 2-tuple $\{0 \mapsto a, 1 \mapsto b\}$, and vice versa. We say that the set of 2-tuples $\{0,1\} \to A$ and the set of pairs $A \times A$ are isomorphic. We usually do not need to distinguish 2-tuples from pairs. Similarly, the set $\{0\} \to A$ of 1-tuples is isomorphic with A, and we often do not distinguish a 1-tuple $\{0 \mapsto a\}$ from a. Note also that the 0-tuple is the empty function (i.e. the empty set $\emptyset$) – the only element of $\emptyset \to A$.

(prove that it is indeed a function.) The function is called the *characteristic function* of B. Conversely, any function from A to $\{0,1\}$ is the characteristic function of an exactly one subset of A. For instance, if A equals $\{a,b,c\}$ then $\{b,c\} \in 2^A$ can be seen as the Boolean function $\{a \mapsto 0, b \mapsto 1, c \mapsto 1\}$, and $\emptyset \in 2^A$ can be seen as the Boolean function $\{a \mapsto 0, b \mapsto 0, c \mapsto 0\}$. These notions also provide an explanation of the powerset notation 2^A since 2^A may be viewed as functions from A to a binary set, e.g. $\{0,1\}$ (recall that B^A denotes the function space $A \to B$).

Example 7. *A Boolean valuation (interpretation or model) is a mapping from an alphabet of propositional variables Var to a binary set* **Bool** $:= \{0,1\}$. *If* $Var := \{x,y,z\}$ *then* $Var \to$ **Bool** *is the set of all Boolean functions from Var to* **Bool**. *There are obviously* $2^{|Var|} = 8$ *such functions, for instance*

$$\begin{array}{lcl} \sigma_0 & := & \{x \mapsto 0, y \mapsto 0, z \mapsto 0\} \\ \sigma_1 & := & \{x \mapsto 1, y \mapsto 0, z \mapsto 0\} \\ \sigma_2 & := & \{x \mapsto 0, y \mapsto 1, z \mapsto 0\} \\ \sigma_3 & := & \{x \mapsto 1, y \mapsto 1, z \mapsto 0\} \\ \textit{etc.} & & \end{array}$$

Note that a Boolean valuation is a characteristic function (of a subset of Var). So such valuations may be equivalently represented as such subsets, e.g. σ_3 *by the set* $\{x,y\} \in 2^{Var}$. *We refer to the latter as the set-representation of a Boolean valuation or interpretation.*

Basic orderings

We next consider some well-known and useful classes of relations. In particular relations which allow us to order (in an intuitive sense) elements.

Definition 4. *A relation* $R \subseteq A \times A$ *is called a preorder (or quasi ordering) if it is reflexive and transitive.*

Example 8. *The standard ordering* $\leq$ *on the natural numbers is a preorder. So is the standard subset relation* $\subseteq$ *on every powerset* 2^A.

Example 9. *Let us consider a few more examples of preorders.*

1. *Let A be an arbitrary set whose elements are finite sets. Consider the following relation* $\preceq$ *on A:* $B \preceq C$ *iff* $|B| \leq |C|$ *(i.e. B has no more elements than C), for any* $B, C \in A$. *The relation is a preorder.*

2. *The relation* $\preceq$ *on the set* Σ^* *of strings, given by*

$$\begin{array}{lll} x \preceq y & \textit{iff} & \textit{for each symbol } a \\ & & \textit{if } a \textit{ occurs in } x \textit{ then } a \textit{ occurs in } y. \end{array}$$

is a preorder. (In other words, $x \preceq y$ iff the set of symbols occurring in x is a subset of the set of symbols occurring in y.)

3. *Define $\leq_7 \subseteq \mathbb{N} \times \mathbb{N}$ as follows*

$$(x \leq_7 y) \text{ iff } (x \mod 7) \leq (y \mod 7)$$

Then $\leq_7$ is a preorder since it is both reflexive and transitive. Note that $\leq_7$ is not antisymmetric since e.g. $6 \leq_7 13$ and $13 \leq_7 6$ but $6 \neq 13$.

Definition 5. *A preorder $R \subseteq A \times A$ is called a partial order if it is also antisymmetric.*

Example 10. *The relation $\leq$ on the natural numbers is a partial order, and so is $\subseteq$ on 2^A.*

Example 11. *The relation "divides" on $\mathbb{Z}^+$ is a partial order; any positive integer divides itself (reflexivity); if x and y divide each other, then $x = y$ (antisymmetry), and if x divides y and y divides z, then x divides z (transitivity).*

Example 12. *Let Σ be an alphabet, and consider Σ^*, i.e. the set of all finite strings over Σ. Let $\trianglelefteq \subseteq \Sigma^* \times \Sigma^*$ defined by*

$$u \trianglelefteq v \text{ iff there is a } w \in \Sigma^* \text{ such that } uw = v$$

(in other words, iff u is prefix of v). Then $\trianglelefteq$ is a partial order, usually called the prefix order.

Example 13. *Let Σ^* be as previously. Let $\trianglelefteq_s \subseteq \Sigma^* \times \Sigma^*$ defined by*

$$u \trianglelefteq_s v \text{ iff there are } w, z \in \Sigma^* \text{ such that } zuw = v$$

(in other words, iff u is a substring of v). Then $\trianglelefteq$ is a partial order, we may call it the substring order. Note that $\trianglelefteq \subseteq \trianglelefteq_s$.

Example 14. *Let $A \twoheadrightarrow B$ denote the space of all partial functions from A to B. A partial function can be viewed as an under-specified total function; in fact, we may order partial functions depending on how much information they convey. For instance, consider the function space $\mathbb{N} \twoheadrightarrow \mathbb{N}$ and the four partial functions*

$$\begin{aligned}
\sigma_1 &:= \{(0 \mapsto 1), (1 \mapsto 1\}\} \\
\sigma_2 &:= \{(0 \mapsto 1), (1 \mapsto 1), (2 \mapsto 2)\}. \\
\sigma_3 &:= \{(0 \mapsto 1), (1 \mapsto 1), (2 \mapsto 2), (3 \mapsto 6)\}. \\
\sigma_4 &:= \{(0 \mapsto 1), (1 \mapsto 1), (2 \mapsto 1), (3 \mapsto 1)\}.
\end{aligned}$$

Then σ_2 conveys more information than σ_1. Similarly σ_3 contains more information than both σ_2 and σ_1. Now if we compare σ_4 and σ_2 we may say that σ_4 is more defined than σ_2, but it does not contain more information than σ_2; they convey incomparable information since $\sigma_2(2) = 2 \neq \sigma_4(2) =$

1. *Formally we may define our ordering of partial functions (often referred to as the information ordering) simply as set inclusion on on the functions viewed as sets (recall that we defined a partial function as a binary relation). That is, given* $\sigma \colon A \rightharpoonup B$ *and* $\sigma' \colon A \rightharpoonup B$

$$\sigma \leq \sigma' \text{ iff } \sigma \subseteq \sigma'.$$

As we shall see later the information ordering is very important when formally defining e.g. functions with infinite domains; the partial functions $\sigma_1, \sigma_2, \sigma_3$ *are examples of increasingly better approximations of the factorial function. The information ordering is also important when defining semantics of programming languages.*

A partial order is of course always a preorder, but the converse does not generally hold. (Find out which preorders in the examples above are not partial orders.) However, a preorder $\preceq \subseteq A \times A$ induces a partial order if lifted to a relation on equivalence classes. Let

$$x \equiv y \text{ iff } x \preceq y \wedge y \preceq x.$$

The relation $\equiv$ is an equivalence (prove this). Let us denote the equivalence class of x under $\equiv$ by $[x]$, this means

$$[x] = \{\, y \in A \mid y \equiv x \,\}.$$

Let us define

$$[x] \preceq_{\equiv} [y] \text{ iff } x \preceq y.$$

Then $\preceq_{\equiv}$ is a partial order (prove this). We sometimes say that $\preceq$ modulo $\equiv$ is a partial order.

Example 15. *Consider the set of propositional formulas F induced by a finite set Var of propositional variables:*

$$\begin{array}{lcl} F & ::= & \mathit{Var} \\ F & ::= & \neg F \mid (F \wedge F) \mid (F \vee F) \mid (F \to F) \end{array}$$

We say that an interpretation (i.e. a Boolean valuation) σ *is a model of a Boolean formula F if F is true in* σ*, and write* $\mathrm{Mod}(F)$ *for the set of all models of F.*

Now consider F under the entailment ordering: $F_1 \models F_2$ *iff every model of* F_1 *is also a model of* F_2*, or put equivalently iff* $\mathrm{Mod}(F_1) \subseteq \mathrm{Mod}(F_2)$*. The result is a preorder. The relation* $\models$ *is clearly reflexive and transitive, but not antisymmetric since e.g.* $(\neg x \vee y) \models (x \to y)$ *and* $(x \to y) \models (\neg x \vee y)$*. On the other hand, we have the following (logical) equivalence relation*

$$\begin{array}{lll} F_1 \Leftrightarrow F_2 & \textit{iff} & F_1 \textit{ and } F_2 \textit{ have the same set of models} \\ & \textit{iff} & F_1 \models F_2 \textit{ and } F_2 \models F_1. \end{array}$$

If we consider $\models$ *modulo* $\Leftrightarrow$ *then we have a partial order.*

We sometimes encounter an alternative notion of partial order, sometimes called a *strict* partial order to distinguish it from the previous notion:

Definition 6. *A relation $R \subseteq A \times A$ which is irreflexive and transitive is called a strict partial order.*

If $R \subseteq A \times A$ is a partial order then $R \setminus \text{ID}_A$ is a strict partial order (where ID_A is the identity relation on A). Conversely, if $R' \subseteq A \times A$ is a strict partial order then $R' \cup \text{ID}_A$ is a partial order (prove this). Note that a strict partial order is always antisymmetric, vacuously (prove this).

Example 16. *The relation $<$ on $\mathbb{N}$ and the relation $\subset$ on 2^A are examples of strict partial orders.*

NOTATION: From now on we normally use relation symbols like $\leq$, $\preceq$, $\sqsubseteq$ for non-strict partial orders. In such cases we occasionally write $y \geq x$ as an alternative to $x \leq y$, and if $\leq$ is a partial order then $<$ refers to the strict version of $\leq$, i.e. $\leq \setminus \text{ID}_A$, assuming that $\leq \subseteq A \times A$. As usual, the notation $x \not\leq y$ means that x is not related to y by $\leq$, in other words $(x, y) \notin \leq$. We say that two elements x, y are *comparable* whenever $x \leq y$ or $y \leq x$, and *incomparable* otherwise. We write $x \mid\mid y$ when x and y are incomparable (assuming that the order is known).

Definition 7. *If $\leq \subseteq A \times A$ is a partial order then the pair $(A, \leq)$ is called a partially ordered set, or poset.*

By an *ordered set* we henceforth mean a poset or a $(A, <)$, where $< \subseteq A \times A$ is a strict partial order.

Definition 8. *A subset $B \subseteq A$ of a poset $(A, \leq)$ is called a chain (in $(A, \leq)$) if $a \leq b$ or $b \leq a$ for all $a, b \in B$. (In other words, if each two elements of B are comparable by $\leq$.)*

Definition 9. *A poset $(A, \leq)$ such that A is a chain is called a* total order *or* linear order.

Note that if $B \subseteq A$ is a chain in $(A, \leq)$ then $C \subseteq B$ is always a chain in $(A, \leq)$. We now define the dual notion of a chain where we instead require that all elements are incomparable.

Definition 10. *A subset $B \subseteq A$ of a poset $(A, \leq)$ is called an anti-chain if $x \leq y$ implies $x = y$, for all $x, y \in B$.*

Equivalently, each two distinct elements $x \neq y$ in an anti-chain are incomparable, $x \mid\mid y$.

We shall often use the terms chain and anti-chain also in the context of strict partial orders. A (strict) chain is a subset B of a strict

partial order $(A, <)$, where either $x < y$ or $y < x$ for each distinct elements x, y of B. If this holds for $B = A$ then $(A, <)$ is called a strict total (or linear) order. B is called an antichain when $x \mid\mid y$ for each distinct $x, y \in B$.

Example 17. *Consider the poset $(2^{\{0,1,2\}}, \subseteq)$, i.e., subsets of $\{0,1,2\}$ ordered by (non-proper) set inclusion. Then $\{\{0\}, \{0,1\}, \{0,2\}, \{0,1,2\}\}$ is a chain in $(2^{\{0,1,2\}}, \subseteq)$. What is an example of an anti-chain?*

Constructing orders

We survey some useful techniques for constructing posets from existing, usually simpler, posets. However first we consider the opposite; let $\mathcal{A} := (A, \leq)$ be a poset and let $B \subseteq A$. Then $\mathcal{B} := (B, \preceq)$ is called the *poset induced by* $\mathcal{A}$ if

$$x \preceq y \text{ iff } x \leq y \text{ for all } x, y \in B.$$

We prove that $\mathcal{B}$ is indeed a poset.

Theorem 1. *If $\mathcal{A}$ is a poset and $\mathcal{B}$ is induced by $\mathcal{A}$, then $\mathcal{B}$ is a poset.*

Proof. First consider reflexivity: let $x \in B$. Then $x \in A$ and $x \leq x$ since $\mathcal{A}$ is a poset. Hence, $x \preceq x$. Second, consider antisymmetry: Assume $x, y \in B$ and $x \preceq y \preceq x$; hence, $x \leq y \leq x$. Since $\mathcal{A}$ is antisymmetric $x = y$. Transitivity can be shown similarly. □

An analogical property with a similar proof holds for strict partial orders. In most cases we write simply that $(B, \leq)$ is the poset induced by $(A \leq)$ although $\leq$ in the former is different from $\leq$ in the latter (unless of course $A = B$).

Definition 11. *If there is no infinite chain in a poset $(A, \leq)$ then we say that the poset of finite height (or* length*). Otherwise the height of the poset is said to be infinite.*

If $(A, \leq)$ is of finite height then its height *(or length) is $|C| - 1$ where C is the chain in A of the greatest number of elements.*

Example 18. *The height of $(2^{\{0,1,2\}}, \subseteq)$ is 3, since e.g. $\emptyset \subset \{0\} \subset \{0,1\} \subset \{0,1,2\}$ is a largest chain. The height of $(2^{\mathbb{N}}, \subseteq)$ is infinite.*

We next consider so-called *componentwise orderings*.

Theorem 2. *Let $(A, \leq)$ be a poset, and consider a relation $\preceq$ on $A \times A$ defined as follows*

$$(x_1, y_1) \preceq (x_2, y_2) \text{ iff } x_1 \leq x_2 \wedge y_1 \leq y_2.$$

Then $(A \times A, \preceq)$ is a poset.

The proof is left as an exercise. The construction generalizes in a natural way to obtaining a poset $(A_1 \times A_2, \preceq)$ out of a pair of posets $(A_1, \leq_1)$, $(A_2, \leq_2)$, and to constructing $(A_1 \times \cdots \times A_n, \preceq)$ (for $n > 0$). Under such generalization, each componentwise ordering $(A^n, \preceq)$ is a special case of *pointwise ordering*:

Theorem 3. *Let $(A, \leq)$ be a poset, and consider a relation $\preceq$ on $B \to A$ defined as follows*

$$\sigma_1 \preceq \sigma_2 \text{ iff } \sigma_1(x) \leq \sigma_2(x) \text{ for all } x \in B.$$

Then $(B \to A, \preceq)$ is a poset.

The proof is similar to that for componentwise orderings.

Example 19. *Given a set of Boolean variables Var, a (Boolean) valuation is a function σ: Var $\to$ **Bool** (see Example 7). Take the numerical ordering $\leq$ on **Bool** $= \{0, 1\}$. In the pointwise ordering $\sigma_1 \preceq \sigma_2$ iff $\sigma_1(x) \leq \sigma_2(x)$, for all $x \in$ Var. For instance, $\{x \mapsto 1, y \mapsto 0, z \mapsto 0\} \preceq \{x \mapsto 1, y \mapsto 0, z \mapsto 1\}$.*

We finally consider so-called *lexicographical orderings*. Let $\Sigma = \{a_1, \ldots, a_n\}$ be a finite alphabet under some strict total ordering $a_1 < \ldots < a_n$. Let Σ^* be the set of all finite (possibly empty) strings over Σ and define (for $x_1, \ldots, x_i, y_1, \ldots, y_j \in \Sigma$) $x_1 \cdots x_i \sqsubset y_1 \cdots y_j$ to hold iff, for some k such that $0 \leq k \leq i$ and $k \leq j$,

- $x_1 \cdots x_k = y_1 \cdots y_k$ and
- $k = i < j$ (i.e. $x_1 \cdots x_i$ is a proper prefix of $y_1 \cdots y_j$), or $k < i$, $k < j$, and $x_{k+1} < y_{k+1}$.

Note that $y_1 \cdots y_k$ is the longest common prefix of both strings. This is the standard ordering of words that we encounter e.g. in dictionaries. Prove that $\sqsubset$ is a strict total order.

Example 20. *Let $\Sigma = \{a, b, c\}$ with the total ordering $a < b < c$. Then e.g.*

$$\epsilon \sqsubset a \sqsubset aac \sqsubset ab \sqsubset abb \sqsubset ac \sqsubset \cdots$$

As usual ϵ denotes the empty string. Note that the set $\{ w \in \Sigma^* \mid ab \sqsubset w \sqsubset abb \}$ is infinite (there are infinitely many strings between ab and abb), and that there are no string between a and aa.

Minimal Elements and Well-Founded Relations

We next introduce the notion of well-founded relations which provides the basis of many notions in mathematics and computer science; both in the formalization of computation and as a means of proving properties of programs.

Minimal, Maximal, Least, and Greatest elements

We first introduce the following auxiliary notions.

Definition 12. *Consider a relation $R \subseteq A \times A$ and a subset $B \subseteq A$. An element $a \in B$ is called R-minimal in B if there is no $b \in B$ ($b \neq a$) such that $b\ R\ a$.*

In other words, if $b \in B$ and $b\ R\ a$ then $b = a$. Similarly, $a \in B$ is called *R-maximal* in B if there is no $b \in B$ such that $a\ R\ b$. We often skip R- when the relation is clear from the context.

Example 21. *Consider $(2^{\{0,1,2\}}, \subset)$ and the set $B = 2^{\{0,1,2\}} \setminus \{\emptyset\}$. Then $\{0\}, \{1\}$, and $\{2\}$ are all $\subset$-minimal elements in B.*

When defining the notion of a well-founded relation in the forthcoming section we actually only need the notion of R-minimality, but for completeness we also define the following related notions.

Definition 13. *Consider a relation $R \subseteq A \times A$ and a subset $B \subseteq A$. An element $a \in B$ is called least in B if $a\ R\ b$ for all $b \in B$; it is called greatest in B if $b\ R\ a$ for all $b \in B$.*

This definition implies that only reflexive relations admit least and greatest elements. If we wish to speak of least and greatest elements of an irreflexive relation $<$ then we can easily circumvent this by considering the least and greatest elements of $\leq$.

Example 22. *Again, consider $(2^{\{0,1,2\}}, \subset)$ and the set $B = 2^{\{0,1,2\}} \setminus \{\emptyset\}$. Neither $\{0\}, \{1\}$, nor $\{2\}$ is least in B. For example, $\{0\}$ cannot be the least element in B since $\{0\} \subseteq \{1\}$ does not hold. However, clearly, this set admits a greatest element, namely $\{0, 1, 2\}$.*

We have the following relationship between minimal and least elements for antisymmetric relations.

Theorem 4. *If R is antisymmetric then a set has at most one least element, and the least element is its unique minimal element.*

Proof. Assume that b is a least element of B. Note that $a \in B \wedge aRb$ implies $a = b$. (Since b is least, we also have bRa, hence $a = b$ since R is antisymmetric.) By this implication, there is no $a \in B$ such that aRb and $a \neq b$, meaning that b is minimal.

If a is least in B then aRb. By the implication above, $a = b$. This means b is the unique least element of B.

Let c be minimal in B. Since b is least, bRc. Thus $b = c$ (otherwise c not minimal). So, b is the unique minimal element of B. □

An analogical property holds for greatest and maximal elements, the proof is similar. The least element of a poset (if it exists) is sometimes denoted $\bot$ and the greatest element is denoted $\top$.

Example 23. *The poset $(\mathbb{N}, \leq)$ has no maximal element, and no greatest element, 0 is its minimal and its least element.*

Consider the subset $B = \mathbb{N} \setminus \{0, 1\}$ of $\mathbb{N}$ ordered by relation "divides". The prime numbers are minimal elements of B. There is no least element, there are no maximal (and no greatest) elements.

Example 24. *The poset $(2^A, \subseteq)$ has a least and greatest element, namely $\emptyset$ and A. They are the only minimal and, respectively, maximal elements of the poset. In this poset, the subset $2^A \setminus \{\emptyset\}$ has $|A|$ minimal elements; namely all singleton subsets of A.*

Example 25. *Consider the poset $(\mathbf{Bool}, \leq)$ (cf. Example 19). The set $Var \to \mathbf{Bool}$ under the pointwise ordering is a poset; the valuation σ such that $\sigma(x) = 1$ for all $x \in Var$ is the greatest element and the valuation such that $\sigma(x) = 0$ for all $x \in Var$ is the least element.*

Assume that $<$ and $\leq$ are corresponding strict partial order and partial order on A, i.e. $\leq = < \cup \mathrm{ID}_A$. The following property follows immediately from the definition: b is a $<$-minimal element of a set $B \subseteq A$ iff it is a $\leq$-minimal element of B. The same holds for maximal elements.

Well-Founded Relations

We now define the important class of well-founded relations.

Definition 14. *A relation $R \subseteq A \times A$ is said to be well-founded if there for every non-empty set $B \subset A$ exists an element $m \in B$ such that bRm does not hold for any $b \in B$.*

Note that this property is almost the same as requiring that B admits an R-minimal element, but the well-founded property is in the literature typically defined in this way since it implies that R is irreflexive, which is more natural in the context of induction (see chapter 3 in the lecture notes). However, we sometimes wish to apply the definition to reflexive relations $\leq$ in which case we simply say that $\leq$ is well-founded if $<$ is well-founded.

If R is a well-founded relation on A we sometimes say that (A, R) is a well-founded set. And when R is clear from the context, we sometimes say simply that A is a well-founded set.

Example 26. *The relation $<$ on $\mathbb{N}$ is well-founded, while $<$ on $\mathbb{Z}$ is not. Neither is $\{x \in \mathbb{Q} \mid 0 \leq x\}$ under $<$, as e.g. a subset $\{x \in \mathbb{Q} \mid 0 < x < 1\}$ does not have a minimal element The prefix relation $\trianglelefteq$ on Σ^* is well-founded, so is the substring relation $\trianglelefteq_s$ (prove this).*

The lexicographic ordering $\sqsubset$ on Σ^* is not well-founded when $|\Sigma| > 1$. Assume $a, b \in \Sigma$ and $a < b$ (in the underlying ordering of Σ); then the set

$\{ a^i b \mid i \in \mathbb{N} \} \subseteq \Sigma^*$ *has no minimal element:* $\cdots \sqsubset a^{i+1}b \sqsubset a^i b \sqsubset \cdots \sqsubset ab \sqsubset b$.

The subset ordering $\subseteq$ *on* $2^{\mathbb{N}}$ *is not well-founded, as* $\big\{ \{ i \in \mathbb{N} \mid n < i \} \bigm| n \in \mathbb{N} \big\} \subseteq 2^{\mathbb{N}}$ *has no minimal element: for each* $n \in \mathbb{N}$, *we have* $\{ i \in \mathbb{N} \mid n < i \} \supset \{ i \in \mathbb{N} \mid n+1 < i \}$.

We proceed by describing alternative characterizations of well-founded relations. First, we need the following auxilliary notion.

Definition 15. *Let* A *be a set. A sequence over* A *is a function* $f \colon X \to A$ *where* X *is an integer interval, i.e., a set of consecutive integers (possibly infinite).*

For example, if $X = \mathbb{N}$ and f is the successor function $f(x) = x + 1$ we define the sequence $1, 2, \ldots$ of positive natural numbers. A sequence is said to be *finite* if the domain of its defining function is finite, and *infinite* otherwise. Note that a finite sequence with n elements $x_1, x_2, \ldots, x_n$ is nothing else than an n-tuple $(x_1, x_2, \ldots, x_n)$ in slight disguise.

Definition 16. *Let* $<$ *be an irreflexive binary relation over a set* A. *A sequence* $x_0, x_1, x_2, \ldots$ *over* A *such that* $x_0 < x_1 < x_2 < \ldots$ *is called an ascending chain in* A.

A *descending chain* is defined analogically ($\ldots < x_2 < x_1 < x_0$).

Example 27. *The sequence* $\emptyset \subset \{0\} \subset \{0,1\} \subset \{0,1,2\} \subset \ldots$ *is an ascending chain in* $2^{\mathbb{N}}$.

Note that some chains (cf. Definition 8) cannot be represented as ascending (descending) chains. Take for instance $(\mathbb{Q}, \leq)$, and a chain $\{ -1/n \mid n \in \mathbb{N} \} \cup \{0\}$; we have $-1 < -1/2 < -1/3 < \cdots < 0$.

We have the following equivalent characterization of well-founded relations.

Theorem 5. *An irreflexive relation* $< \subseteq A \times A$ *is well-founded iff* $(A, <)$ *contains no infinite descending chains* $\ldots < x_2 < x_1 < x_0$.

Proof. ($\Rightarrow$), by contraposition: Assume that in A there exists an infinite descending chain $\ldots < x_2 < x_1 < x_0$. Then $\{x_0, x_1, x_2, \ldots\} \subseteq A$ contains no minimal element. Thus $(A, <)$ is not well-founded.

($\Leftarrow$), by contraposition: Assume that $(A, <)$ is not well-founded. Hence there is some non-empty $B \subseteq A$ which contains no minimal element. Thus for each $x_i \in B$ there exists $x_{i+1} \in B$ such that $x_{i+1} < x_i$. We then construct our infinite descending chain by picking an (arbitrary) element $x_1 \in B$, then pick an element $x_2 \in B$ such that $x_2 < x_1$, and based on x_2, an $x_3 \in B$ such that $x_3 < x_2$, and so on.[6] □

[6] It is clear that choosing $x_{i+1} < x_i$ can be made for each $i \geq 1$. But can we be sure that this construction actually produces an *infinite* chain? Yes, if we assume either the *axiom of choice* or its weaker variant *axiom of dependent choice* in our underlying theory of sets.

Example 28. *We show that $\subset$ is well founded on any set $\mathcal{A}$ of finite sets. Consider an element $A \in \mathcal{A}$. Any descending chain beginning with A consists of (some) subsets of A. But the set 2^A of (all) subsets of A is finite, hence the chain cannot be infinite.*

The following examples illustrate some uses of well-founded sets.

Example 29. *Consider an inductive definition of a language, e.g. the set of all propositional formulas over some finite alphabet of propositional variables Var:*

$$\begin{array}{lcl} F & ::= & Var \\ F & ::= & \neg F \mid (F \wedge F) \mid (F \vee F) \mid (F \to F) \end{array}$$

Let $\prec$ be the "proper subformula" relation; $G \prec F$ iff G is a proper subformula of a formula F. For instance, x, y, $\neg x$, $\neg y$ and $\neg x \vee y$ are all proper subformulae of $(\neg x \vee y) \vee \neg y$. Then $\prec$ is a well-founded relation.

Note that here we treat inductive definitions rather informally. To prove that $\prec$ is well-founded it is sufficient to note that a proper formula of F is a substring of F, and the substring relation (Example 13) is well-founded; the latter is left as an exercise.

Example 30. *Consider a transition system $(C, \Rightarrow, I)$ with an initial set $I \subseteq C$ of configurations. Let $\prec \subseteq C^+ \times C^+$ be defined as follows*[7]

$$c_1 \dots c_n \prec c_1 \dots c_n c_{n+1} \text{ iff } c_n \Rightarrow c_{n+1}$$

[7] C^+ denotes the set of all non-empty and finite words (i.e. sequences) of configurations.

Now let the set of traces T of $(C, \Rightarrow, I)$ be the smallest set of words such that

- *if $c \in I$ then $c \in T$,*
- *if $t \in T$ and $t \prec t'$ then $t' \in T$.*

Then $\prec$ is a well-founded relation on T. Note that $\prec^+$ is a strict partial order (but $\prec$ is not)

Well-Orders

We have the following important instance of well-founded relations:

Definition 17. *A strict total order $(A, <)$ which is well-founded is called a well-order.*

Example 31. *The following are examples of well-orders.*

- *The natural numbers under $<$.*
- *$(\mathbb{N}, \prec)$, where $0 \prec 2 \prec 4 \prec \cdots 1 \prec 3 \prec 5 \prec \cdots$. More formally,*

$$\begin{array}{lll} i \prec j & \text{iff} & i \text{ is even and } j \text{ is odd, or} \\ & & i < j \text{ and } i, j \text{ are both even or both odd.} \end{array}$$

The following strict partial orders are not well-orders.

- *The non-negative rational numbers* $\{x \in \mathbb{Q} \mid 0 \leq x\}$ *under* $<$*, as the order is not well-founded, as shown in Example 26.*
- $(2^A, \subset)$ *(when* $|A| > 1$*), since* $\subset$ *is not total.*
- *Consider the ordering* $\leq$ *from Example 25 on Boolean valuations* $Var \to \mathbf{Bool}$*, and the corresponding strict ordering* $< = \leq \setminus \mathrm{ID}_{Var \to \mathbf{Bool}}$*. If* $|Var| > 1$ *then* $<$ *is not total, and* $(Var \to \mathbf{Bool}, <)$ *is not a well-order.*
- *The set* Σ^* *under the lexicographical order* $\sqsubset$*. The order is total, but not well-founded, as shown in Example 26.*
- *The set* Σ^* *under the inverse lexicographical ordering* $\sqsubset^{-1}$*, since e.g.*

$$\ldots \sqsubset^{-1} aaa \sqsubset^{-1} aa \sqsubset^{-1} a$$

has no minimal element.

Obviously, any subset $(B, <)$ of a well-order $(A, <)$ is a well-order. (By Definition 14, as each subset of B is a subset of A.) Definitions 14, 17 state that each nonempty subset of a well-order has a minimal element. Actually, there is only one such element:

Lemma 1. *In a total order (or a strict total order), (1) a minimal element of a subset is unique and (2) every non-empty subset of a well-order has a unique minimal element.*

Proof. Let (A, R) be a total order or a strict total order. Assume that $a \neq b$ and that a, b are minimal elements of a $B \subseteq A$. Thus aRb or bRa. Hence b is not minimal, or a is not minimal. Contradiction; the minimal element is unique. Now the second part of the lemma follows from the definition of a well-order. □

We will often write $x_0 < x_1 < x_2 < \ldots$ for a well-order $(A, <)$, where $A = \{x_0, x_1, \ldots\}$ (and may be finite or infinite), and where x_0 is the (unique) minimal element in A, and x_1 is the (unique) minimal element of $A \setminus \{x_0\}$, etc.

Lemma 2. *Let* $<$ *be an arbitrary relation on* A*. If every non-empty subset of* $(A, <)$ *has a unique minimal element then* $<$ *is transitive.*

Proof. Assume that $x < y$ and $y < z$. If $x = y$ then $x < z$ follows immediately. Assume now that $x \neq y$. Note first that $x \neq z$, as otherwise $x < y < x$ and $\{x, y\}$ has no minimal element. Now $\{x, z\}$ must contain a unique minimal element. Hence $x < z$ or $z < x$, as otherwise both x, y are minimal. Assume $z < x$. We have $x < y < z < x$, thus $\{x, y, z\}$ has no minimal element, contradiction. Hence, $z < x$. □

Theorem 6. *The structure $(A, <)$ is a well-order iff every non-empty subset of A has a unique minimal element and $<$ is irreflexive.*

Proof. The direction $\Rightarrow$ is the content of Lemma 1. To prove $\Leftarrow$ we assume that every non-empty subset of A has a unique minimal element. By Lemma 2, $<$ is transitive; thus it is a strict partial order. Assume that it is not total. So there exist two incomparable elements $x, y \in A$. But then $\{x, y\}$ has two minimal elements, contradiction.

Hence, $<$ is a strict total order and since every non-empty subset of a contains a minimal element $(A, <)$ is a well-order. □

Exercises

1.1 Is $R \circ R^{-1}$ the identity relation (for an arbitrary relation $R \subseteq A \times A$)? Does $R \circ R^{-1} = R^{-1} \circ R$?
Prove that the transitive closure of a relation is transitive.

1.2 Draw the Hasse diagram of $\{x, y, z\} \to \mathbf{Bool}$ under the ordering in Example 19. Compare the diagram to the Hasse diagram of the poset $(2^{\{x,y,z\}}, \subseteq)$.

1.3 Let $(A, \leq)$ be a preorder, and let $x \equiv y$ iff $x \leq y$ and $y \leq x$. Prove that it is an equivalence relation and that $\leq$ lifted to the equivalence classes of $\equiv$, defined as $[x] \leq_{\equiv} [y]$ iff $x \leq y$ (see p. 8), is a partial order.

Before the latter, prove that $\leq_{\equiv}$ is well defined; this means that if we have $[x] = [x']$ and $[y] = [y']$ then $[x] \leq_{\equiv} [y]$ iff $[x'] \leq_{\equiv} [y']$.

1.4 Prove Theorem 2.

1.5 Prove Theorem 3.

1.6 Prove that a strict partial order is always antisymmetric.

1.7 Is $\mathbb{Z}$ ordered like this $0 \prec 1 \prec 2 \prec \cdots -3 \prec -2 \prec -1$ a well-order? (Here any positive number precedes any negative one.)

1.8 Prove that $(\mathbb{N}, \prec)$ from Example 31 (even numbers precede odd ones) is a well-order.

1.9 Let (A, R_1) be a well-founded set, and let $R_2 \subseteq R_1$. Prove that (A, R_2) is well-founded.

1.10 Prove Lemma **??** ((A, R) is well-founded iff (A, R^+) is well-founded).

1.11 Consider the prefix ordering and the substring ordering (Examples 12, 13). Show that they are partial orders and are well-founded. It is sufficient to show this for one these relations, the required properties for the other one follow immediately. Choose the right relation.

1.12 Prove that any partial ordering (and any strict partial ordering) on a finite set is well-founded

References

R. Grimaldi. *Discrete and Combinatorial Mathematics*. Addison-Wesley, 4th edition, 2000.