Appendix A

Notation

A.1 Sets, Relations, and Functions

A.1.1 Some notation for sets

If B is a set of sets, we denote by $\bigcup B$ the union of all sets in B. For two natural numbers $n, m \in \mathbb{N}$, we denote by $[n..m] = \{i \in \mathbb{N} \mid n \leq i \leq m\}$ the integers from n to m, extremes included. Given two states A and B, their *disjoint union* is given by $A \uplus B = (A \times \{0\}) \cup (B \times \{1\})$.

A.1.2 Binary relations

Composition. Given three sets A, B, C, a binary relation $\rho \subseteq A \times B$, and a binary relation $\tau \subseteq B \times C$, we denote by $\tau \circ \rho = \{\langle a, c\rangle \in A \times C \mid \exists b \in B \,\mathbf{.}\, \langle a, b\rangle \in \rho \wedge \langle b, c\rangle \in \tau\}$. We will also write $\rho \odot \tau$ for $\tau \circ \rho$, to remedy a historical idiosyncrasy about argument order in relation composition.

Transitive closure. Any binary relation $\sim \subseteq A^2$ can be enlarged and made transitive by computing its *transitive closure* $\sim^+$. The transitive closure $\sim^+$ of $\sim$ is the smallest relation that is transitive, and such that $\sim \subseteq \sim^+$. If A is a finite set, $\sim^+$ can be computed by setting $\sim_0 = \sim$, and $\sim_{k+1} = \sim \circ \sim_k$ for $k \geq 0$; we have then $\sim^+ = \lim_{k \to \infty} \sim_k$, where the limit can be computed in a finite number of iterations (it suffices to stop once an m is reached such that $\sim_m = \sim_{m+1}$). The transitive, reflexive closure $\sim^*$ of $\sim$ is defined by $\sim^* = \sim^+ \cup \{\langle a, a\rangle \mid a \in A\}$.

Inverse. The *inverse* of a binary relation $\sim \subseteq A^2$ is the relation $\sim^{-1}$ defined by $\sim^{-1} = \{\langle a, b\rangle \mid \langle b, a\rangle \in \sim\}$.

Equivalence relations. Given a set A, we say that a binary relation $\simeq \subseteq A^2$ is an *equivalence* relation if the following three conditions hold:

1. *Reflexivity:* For all $a \in A$, we have $a \simeq a$.

2. *Symmetry:* For all $a, b \in A$, if $a \simeq b$, then $b \simeq a$.

3. *Transitivity:* For all $a, b, c \in A$, if $a \simeq b$ and $b \simeq c$, then $a \simeq c$.

A *partition* of a set A is a set $T \subseteq 2^A$ such that $\bigcup T = A$ and, for all $B, C \in T$, such that $B \cap C = \emptyset$. A partition T induces an equivalence relation $\simeq_T \subseteq A^2$ defined by $a \simeq_T b$ iff there is $B \in T$ with $a, b \in B$. If $\simeq$ is an equivalence relation, then we can define for all $a \in A$ the *equivalence class* of a by $[a]_\simeq = \{b \in A \mid a \simeq b\}$. We indicate with $A/\simeq = \{[a]_\simeq \mid a \in A\}$ the *quotient* of A with respect to $\simeq$. This quotient is a partition of A: for all $a, b \in A$, we have that either $[a]_\simeq = [b]_\simeq$, or $[a]_\simeq \cap [b]_\simeq = \emptyset$.

Given two equivalence relations $\simeq_1, \simeq_2 \subseteq A^2$, the relation $\simeq_1 \cap \simeq_2$ is again an equivalence relation. The relation $\simeq_1 \cup \simeq_2$ is not necessarily an equivalence relation, since it may not be transitive. On the other hand, $(\simeq_1 \cup \simeq_2)^+$ is again an equivalence relation, and in fact is the smallest equivalence relation that contains both $\simeq_1$ and $\simeq_2$.

We say that an equivalence relation $\simeq_1$ is *finer* than $\simeq_2$ if $\simeq_1 \subseteq \simeq_2$ (conversely, we may say that $\simeq_2$ is *coarser* than $\simeq_1$). If $\simeq_1$ is finer than $\simeq_2$, we also say that $\simeq_1$ *refines* $\simeq_2$. If $\simeq_1 \subseteq \simeq_2$, then for all $a \in A$ we have $[a]_{\simeq_1} \subseteq [a]_{\simeq_2}$, justifying the finer/coarser terminology. In particular, for all $a \in A$ we have that $[a]_{\simeq_2}$ can be written as

$$[a]_{\simeq_2} = \bigcup \{[b]_{\simeq_1} \mid b \in [a]_{\simeq_2}\}.$$

Problem 1. Give an example of a set A and two equivalence relations $\simeq_1, \simeq_2 \subseteq A^2$ such that $\simeq_1 \cup \simeq_2$ is not an equivalence relation, and another example such that $\simeq_1 \cup \simeq_2$ is an equivalence relation. ∎

Functions. Consider two ordered sets A and B. A function $f : A \mapsto B$ is *monotonic* if, for all $a, a' \in A$, we have that $a \leq a'$ implies $f(a) \leq f(a')$. A function $f : A \mapsto B$ is *strictly monotonic* if, for all $a, a' \in A$, we have that $a < a'$ implies $f(a) < f(a')$. Given a function $f : A \mapsto B$, the *image* of f is the set $\mathrm{Im}(f) = \{b \in B \mid \exists a \in A \,.\, f(a) = b\}$.

A.2 Sequences

Given a set A, we let

$$A^* = \bigcup_{k=0}^{\infty} A^k \qquad\qquad A^+ = \bigcup_{k=1}^{\infty} A^k$$

Thus, A^* is the sets of finite sequences of A, and A^+ is the set of finite non-empty sequences of A. Given a sequence $\sigma \in A^*$, if $\sigma \in A^k$ then we say that the *length* of σ is k, written $|\sigma| = k$. For $0 \leq i < |\sigma|$, we denote by $\sigma[i]$ the i-th element of σ (starting from the left); hence, the first element of σ is $\sigma[0]$. We denote by ε the empty sequence of elements.

Concatenation. For $\sigma_1, \sigma_2 \in A^*$, we denote by $\sigma_1 \cdot \sigma_2 \in A^*$ the *concatenation* of the sequences σ_1 and σ_2. Formally, $\sigma_1 \cdot \sigma_2$ is defined by

$$\begin{aligned} &|\sigma_1 \cdot \sigma_2| = |\sigma_1| + |\sigma_2|, \\ &(\sigma_1 \cdot \sigma_2)[k] = \sigma_1[k] && 0 \leq k < |\sigma_1|, \\ &(\sigma_1 \cdot \sigma_2)[k + |\sigma_1|] = \sigma_2[k] && 0 \leq k < |\sigma_2|. \end{aligned}$$

Occurrence. We say that an element $a \in A$ *occurs* in $\sigma \in A^*$, written $a \lhd \sigma$, if there is $0 \leq k < |\sigma|$ such that $a = \sigma[k]$.

Prefixes. Given a sequence $\sigma \in A^*$, we denote by $\mathrm{last}(\sigma) = \sigma[|\sigma|]$ the last element of σ. A sequence $\sigma' \in A^*$ is a *prefix* of a sequence σ (written $\sigma' \lessdot \sigma$) if there is a sequence $\sigma'' \in A^*$ such that $\sigma' \cdot \sigma'' = \sigma$. A set $L \subseteq A^*$ of sequences is *prefix closed* if, whenever it contains a sequence, it contains also all the prefixes of that sequence. Formally, L is prefix closed if for all $\sigma \in L$ and all $\sigma' \in A^*$ with $\sigma' \lessdot \sigma$, we have $\sigma' \in L$.

Interleaving. Consider two sequences $\sigma_1, \sigma_2 \in A^*$, and let $k_1 = |\sigma_1|$ and $k_2 = |\sigma_2|$, and $k = k_1 + k_2$. The *interleaving* $\sigma_1 \bowtie \sigma_2$ of σ_1 and σ_2 is the set of all sequences σ with $|\sigma| = k_1 + k_2$, and such that there are two strictly monotonic functions $f_1 : [0..k_1 - 1] \mapsto [0..k - 1]$ and $f_2 : [0..k_2 - 1] \mapsto [0..k - 1]$ such that:

1. $\mathrm{Im}(f_1) \cap \mathrm{Im}(f_2) = \emptyset$;
2. for all $i \in [0..k_1 - 1]$, we have $\sigma_1[i] = \sigma[f_1(i)]$;
3. for all $i \in [0..k_2 - 1]$, we have $\sigma_2[i] = \sigma[f_2(i)]$.

Intuitively, each element of $\sigma_1 \bowtie \sigma_2$ corresponds to a merge of the sequences σ_1 and σ_2 that preserves the relative order of the symbols of σ_1 and σ_2. For instance, if $\sigma_1 = abcdef$ and $\sigma_2 = 12345$, then *12a3bcd4ef5* $\in \sigma_1 \bowtie \sigma_2$.