Basic Notation

Manfred Kufleitner

Automata and Formal Languages WS 2013/2014

- The composition of two mappings $\varphi : X \to Y$ and $\psi : Y \to Z$ is $\psi \circ \varphi : X \to Z$ with $(\psi \circ \varphi)(x) = \psi(\varphi(x))$ for $x \in X$.
- $\mathbb{N} = \{ 0, 1, 2, \dots \}$ natural numbers (i.e. non-negative integers)
- $\mathbb{Z} = \{ \dots, -2, -1, 0, 1, 2, \dots \}$ integers
- A *word* is a sequence of letters (aka *string*), a (formal) *language* is a set of words.
- The set of all finite words over the alphabet Σ is $\Sigma^* = \{ a_1 \cdots a_n \mid n \geq 0,\ a_i \in \Sigma \}$. It is the so-called *free monoid* over Σ. The *empty* word is denoted by ε. The *length* of a word $u = a_1 \cdots a_n$ with $a_i \in \Sigma$ is $|u| = n$, its *alphabet* is the set $\text{alph}(u) = \{ a_1, \cdots, a_n \} \subseteq \Sigma$. We have $|\varepsilon| = 0$ and $\text{alph}(\varepsilon) = \emptyset$. By writing a word $a_1 \cdots a_m$ before a word $b_1 \cdots b_n$ we obtain their *concatenation* $a_1 \cdots a_m b_1 \cdots b_n$. We have $\varepsilon u = u \varepsilon = u$ for all words $u \in \Sigma^*$.
- A set S with a binary operation $\cdot : S \times S \to S$ (written as $\cdot(u, v) = u \cdot v = uv$) forms a *semigroup* if $\cdot$ is associative, i.e., $(u \cdot v) \cdot w = u \cdot (v \cdot w)$ for all $u, v, w \in S$. In particular, the notation uvw without brackets is well-defined. When emphasizing the operation, we write $(S, \cdot)$.
- A semigroup M forms a *monoid* if there exists a *neutral element* $e \in M$, i.e., $eu = ue = u$ for all $u \in M$. The neutral element is often denoted by 1 for the operation $\cdot$ and by 0 for $+$. In the case of $\cdot$, the n-fold product of $u \in M$ with itself is written as u^n; we set $u^0 = 1$ for all $u \in M$. Both $(\mathbb{N}, +)$ and $(\mathbb{N}, \cdot)$ form monoids ($\cdot$ denotes here multiplication) ; $(\mathbb{N} \setminus \{0\}, +)$ forms a semigroup which is not a monoid. The free monoid Σ^* with concatenation forms a monoid with neutral element ε.
- A monoid G forms a *group* if for every $u \in G$ there exists an *inverse* $v \in G$ with $uv = vu = 1$. The inverse of u is often written as u^{-1} (or as $-u$ if the operation is $+$). The integers $\mathbb{Z}$ with addition form a group. Note that the inverse of an element u is unique.
- A subset X of a monoid M is a *submonoid* if $1 \in X$ and X with the operation in M forms a monoid. For example, $\mathbb{N}$ is a submonoid of $\mathbb{Z}$. Subsemigroups and subgroups are defined similarly. Let $M = \{ 1, 0 \}$ with multiplication; then both $\{1\}$ and $\{0\}$ are subsemigroups of M which form monoids, but only $\{1\}$ is a submonoid of M.
- $\Sigma \subseteq M$ *generates* a monoid M if every element in M can be written as a finite product of elements in Σ; the empty product yields the neutral element 1. In this case we call Σ a *generating set* or a set of *generators*.
- Every subset $L \subseteq M$ generates a submonoid of the monoid M, denoted by L^*.
- Examples:
  - M generates M.
  - $M \setminus \{1\}$ generates M.
  - $\{ -1, 1 \}$ generates $\mathbb{Z}$ and $\{ 1 \} \subseteq \mathbb{Z}$ generates the submonoid $\mathbb{N}$ of $\mathbb{Z}$.
  - $\{ -2, 3, 4 \}$ generates $\mathbb{Z}$ and $\{ 3 \}$ generates $3\mathbb{N}$.
  - Σ generates Σ^*.
  - $\{ aa, aaa \}$ generates the submonoid $\{a\}^* \setminus \{a\}$ of $\{a\}^*$.
- A mapping $\varphi : X \to Y$ is
  - *surjective* (aka *onto*) if the set $\varphi(X) = \{ \varphi(x) \mid x \in X \}$ equals Y, i.e., if for every $y \in Y$ there exists $x \in X$ with $\varphi(x) = y$.
  - *injective* (aka *one-to-one*) if for all $x, x' \in X$ we have $x \neq x' \;\Rightarrow\; \varphi(x) \neq \varphi(x')$; this is usually shown as $\varphi(x) = \varphi(x') \;\Rightarrow\; x = x'$.
  - *bijective* (aka *one-to-one correspondence*) if it is both surjective and injective; in this case there exists a mapping $\varphi^{-1} : Y \to X$ such that both $\varphi^{-1} \circ \varphi : X \to X$ and $\varphi \circ \varphi^{-1} : Y \to Y$ are identity mappings. A *bijection* is a bijective mapping.
- A mapping $\varphi : M \to N$ between monoids M and N is a *homomorphism* if $\varphi(1) = 1$ and $\varphi(uv) = \varphi(u)\varphi(v)$ for all $u, v \in M$; note that $\varphi(uv)$ uses the operation in M whereas $\varphi(u)\varphi(v)$ uses the operation in N. Both the length $|\,.\,| : \Sigma^* \to \mathbb{N}$ and the alphabet $\text{alph}(\,.\,) : \Sigma^* \to 2^\Sigma$ define a homormophisms (here, the operation on $\mathbb{N}$ is addition and the operation on the power set 2^Σ of Σ is union).
- If $\varphi : M \to N$ is a homomorphism, then $\varphi(M)$ is a submonoid of N (since $1 = \varphi(1) \in \varphi(M)$ and $\varphi(u)\varphi(v) = \varphi(uv) \in \varphi(M)$). Furthermore, if M is a group, then $\varphi(M)$ is a group, too (since the inverse of $\varphi(u)$ is $\varphi(u^{-1})$). Obviously, $\varphi : M \to \varphi(M)$ is surjective.
- If Σ generates M, then a homomorphism $\varphi : M \to N$ is uniquely determined by the restriction $\varphi : \Sigma \to N$ (since every element $u \in M$ can be written as $u = a_1 \cdots a_n$ with $a_i \in \Sigma$, and we have $\varphi(u) = \varphi(a_1) \cdots \varphi(a_n)$). Not every mapping $\varphi : \Sigma \to N$ induces a homomorphism $\varphi : M \to N$. For example, $\varphi(1) = 2$ and $\varphi(-1) = 3$ does not yield a homomorphism $\varphi : \mathbb{Z} \to \mathbb{N}$ since $\varphi(1 - 1) = \varphi(0) = 0$ and $\varphi(1) + \varphi(-1) = 2 + 3 = 5 \neq 0$. On the other hand, every mapping $\varphi : \Sigma \to N$ from a set Σ to a monoid N uniquely extends to a homomorphism $\varphi : \Sigma^* \to N$.
- A bijective homomorphism $\varphi : M \to N$ is an *isomorphism.* Note that in this case $\varphi^{-1} : N \to M$ is a homomorphism, too.
- Two monoids M, N are *isomorphic* if there exists an isomorphism $\varphi : M \to N$. Frequently, isomorphic monoids are considered to be identical since the elements are nothing but renamings of one another. For example, $(\{ 1, -1 \}, \cdot)$ is isomorphic to $(\{1, 0\}, +)$. On the other hand, $(\{ 1, -1 \}, \cdot)$ is not isomorphic to $(\{1, 0\}, \cdot)$ since $(\{ 1, -1 \}, \cdot)$ is a group and $(\{ 1, 0 \}, \cdot)$ is not a group.