Krohn-Rhodes Theorem

Caffeinemachine
khetan@math.tifr.res.in*

June 9, 2021

"Indeed there is no royal road through mathematics, but we do not need to break up the asphalt and destroy the signage to make travelling what roads there are a trial of one's skill." — Jordan Bell.

Contents

1 Partitions, Decompositions, and Automata

Let $A = (Q, \Sigma, f)$ be an automaton and $\mathcal{P}$ be a partition of Q. We say that $\mathcal{P}$ is **admissible** if for each $\sigma \in \Sigma$ and each $P \in \mathcal{P}$ we have $f_\sigma(P)$ is contained in some member of $\mathcal{P}$. If $\mathcal{P}$ is admissible, we naturally obtain an automaton $(\mathcal{P}, \Sigma, \bar{f})$ where $\bar{f}_\sigma(P)$ is defined as the (unique) member of $\mathcal{P}$ which contains $f_\sigma(P)$. We denote this automaton as $A/\mathcal{P}$.

A collection of subsets of a set Q is called a **decomposition** of Q if the union of all the elements of $\mathcal{D}$ is Q. Given an automaton $A = (Q, \Sigma, f)$ and a decomposition $\mathcal{D}$ of Q, we say that $\mathcal{D}$ is **admissible** if for each $D \in \mathcal{D}$ and each $\sigma \in \Sigma$ there is at least one $D' \in \mathcal{D}$ such that $f_\sigma(D)$ is contained in D'. Assuming $\mathcal{D}$ is admissible we may choose, for each $\sigma \in \Sigma$ and each $D \in \mathcal{D}$, a member D_σ of $\mathcal{D}$ such that $f_\sigma(D)$ is contained in D_σ. With this we obtain an automaton $(\mathcal{D}, \Sigma, \bar{f})$ where $\bar{f}_\sigma(D)$ is defined to be D_σ. When no confusion can occur, we denote the automaton thus obtained by $A/\mathcal{D}$, and will be referred to as a $\mathcal{D}$-**factor** of A.

Example 1.1. Let $A = (Q, \Sigma, f)$ be an automaton. Let k be an integer with $1 \leq k \leq |Q|$. Then the set of all the k-element subsets of Q forms an admissible decomposition of Q. ♢

1.1 Yoeli's Construction

Let $A = (Q, \Sigma, f)$ be an automaton and $\mathcal{D}$ be a decomposition of Q. Let $A/\mathcal{D} = (\mathcal{D}, \Sigma, \tilde{f})$ be a $\mathcal{D}$-factor of A. Define $Q_\mathcal{D} \subseteq Q \times \mathcal{D}$ as the set

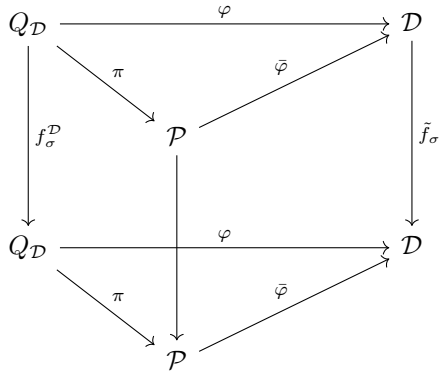
$$Q_\mathcal{D} = \{(q, D) : \ D \in \mathcal{D}, q \in D\} \tag{1.1}$$

For each $\sigma \in \Sigma$, define a map $f^\mathcal{D}_\sigma : Q_\mathcal{D} \to Q_\mathcal{D}$ which takes (q, D) to $(f_\sigma(q), \tilde{f}_\sigma(D))$. Then the triple $A_\mathcal{D} = (Q_\mathcal{D}, \Sigma, f^\mathcal{D})$ is an automaton and will be referred to as an **auxiliary semiautomaton** arising from A and $A/\mathcal{D}$. Let $\mathcal{P}$ be the partition of $Q_\mathcal{D}$ defined as $\mathcal{P} = \{D \times \{D\} : \ D \in \mathcal{D}\}$.

Lemma 1.2. *Then $A_\mathcal{D}/\mathcal{P}$ is isomorphic to $A/\mathcal{D}$.*

*For any questions, comments, suggestions, corrections, or typographical errors please write to me at this email address.

Proof. Let $\varphi : Q_{\mathcal{D}} \to \mathcal{D}$ be defined as $\varphi(q, D) = D$ for all (q, D) in $Q_{\mathcal{D}}$. Let $\pi : \mathcal{Q} \to \mathcal{P}$ be the natural map which sends an element of $Q_{\mathcal{D}}$ to the unique element of $\mathcal{P}$ that contains it. Then the following diagram commutes for all $\sigma \in \Sigma$.



where the vertical map from $\mathcal{P}$ to $\mathcal{P}$ is $\tilde{f}_\sigma^{\mathcal{D}}$ which sends $P \in \mathcal{P}$ to $f_\sigma^{\mathcal{D}}(P)$. Noticing that $\bar{\varphi}$ is bijective, we have the desired result. ■

2 Cascade Product

Let $A = (Q, \Sigma, f)$ and $A' = (Q', \Sigma', f')$ be two automata. A **connection mapping** from A to A' is a map $\omega : Q \to \mathrm{Maps}(\Sigma, \Sigma')$. The **cascade product** of A and A' with respect to a connection mapping ω is the automaton $A \circ_\omega A' = (Q \times Q', \Sigma, f^\omega)$ where f^ω is defined as

$$f_\sigma^\omega(q, q') = (f_\sigma(q), f'_{\omega_q(\sigma)}(q')) \tag{2.1}$$

A special case of this construction if the *direct product*, which is obtained as follows. Let $A = (Q, \Sigma, f)$ and $A' = (Q', \Sigma, f')$ be two automata over the same alphabet. Let $\omega : Q \to \mathrm{Maps}(\Sigma)$ be the trivial connection mapping, that is, ω_q is the identity map for each q. Then the transitions on $A \circ_\omega A'$ are given by

$$(q, q') \xrightarrow{\sigma} (f_\sigma(q), f'_\sigma(q')) \tag{2.2}$$

for each $\sigma \in \Sigma$, which justifies the name 'direct product.'

3 Coverings

Let $A = (Q, \Sigma, f)$ and $\tilde{A} = (\tilde{Q}, \tilde{\Sigma}, \tilde{f})$ be two automata. A **covering** from $\tilde{A}$ to A is a pair (φ, ξ), where $\varphi : \tilde{Q} \to Q$ is a surjective map and $\xi : \Sigma \to \tilde{\Sigma}$ such that the following diagram commutes

$$\begin{array}{ccc} \tilde{Q} & \xrightarrow{\varphi} & Q \\ \downarrow{\scriptstyle \tilde{f}_{\xi(\sigma)}} & & \downarrow{\scriptstyle f_\sigma} \\ \tilde{Q} & \xrightarrow{\varphi} & Q \end{array}$$

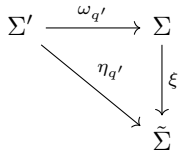
for each σ in Σ. We say that $\tilde{A}$ **covers** A if there is a covering from $\tilde{A}$ onto A. It is clear that if $\tilde{A}$ covers A and $\hat{A}$ covers $\tilde{A}$ then $\hat{A}$ covers A. In fact, if (φ, ξ) is a covering from $\tilde{A}$ onto A and (φ', ξ') is a covering from $\hat{A}$ onto $\tilde{A}$ then $(\varphi' \circ \varphi, \xi' \circ \xi)$ is a covering from $\hat{A}$ onto A.

Given an automaton $A = (Q, \Sigma, f)$, we say that a subset W of Q is **invariant** if $f_\sigma(W) \subseteq W$ for all $\sigma \in \Sigma$. By restricting the domain to f_σ to W, we obtain an automaton $(W, \Sigma, f|_W)$. A **partial covering** from $\tilde{A}$ onto A is a map (φ, ξ), where $\varphi : \tilde{W} \to Q$ is a surjective map, where $\tilde{W}$ is an invariant set in $\tilde{A}$, and ξ is a map $\xi : \Sigma \to \tilde{\Sigma}$. We say that $\tilde{A}$ **partially covers** A if there is a partial covering from $\tilde{A}$ onto A.

Lemma 3.1. *Let A, A' and $\tilde{A}$ be automata and suppose that $\tilde{A}$ covers A. Then whenever ω is a connection mapping from A' to A, there is a connection mapping η from A' to $\tilde{A}$ such that $A' \circ_\eta \tilde{A}$ covers $A' \circ_\omega A$.*

Proof. Let (φ, ξ) be a covering from $\tilde{A}$ onto A and $\omega : Q' \to \text{Maps}(\Sigma', \Sigma)$ be a connection mapping from A' to A. Define the map $\eta : Q' \to \text{Maps}(\Sigma', \tilde{\Sigma})$ as

$$\eta_{q'} = \xi \circ \omega_{q'} \tag{3.1}$$



Now define $\Phi : Q_\eta \to \mathbf{Q}_\omega$ and $\Xi : \Sigma' \to \Sigma'$ as

$$\Phi(q', \tilde{q}) = (q', \varphi(\tilde{q})) \qquad \Xi(\sigma') = \sigma' \tag{3.2}$$

for all $(q', \tilde{q}) \in Q^\eta$ and $\sigma' \in \Sigma'$[1], we see that (Φ, Ξ) is a covering from $A' \circ_\eta \tilde{A}$ onto $A' \circ_\omega A$. ■

Lemma 3.2. *Let $\mathcal{D}$ be an admissible partition of an automaton $A = (Q, \Sigma, f)$ and $A/\mathcal{D}$ be a $\mathcal{D}$-factor of A. Let $A_\mathcal{D}$ be the auxiliary automaton arising from A and $A/\mathcal{D}$. Then $A_\mathcal{D}$ covers A.*

Proof. Define $\varphi : Q_\mathcal{D} \to Q$ as $\varphi(q, D) = q$ for all (q, D) in $Q_\mathcal{D}$ and define $\xi : \Sigma \to \Sigma$ as the identity map. Then it is easy to check that (φ, ξ) is a covering map. ■

Lemma 3.3. *Let $\mathcal{P}$ be an admissible partition of an automaton $A = (Q, \Sigma, f)$ and $A/\mathcal{P}$ be the $\mathcal{P}$-factor of A. Let m be the maximum size of any element of $\mathcal{P}$. Then there is an automaton $A' = (Q', \Sigma', f')$ with $|Q'| \leq m$, and a connection mapping $\omega : \mathcal{P} \to \text{Maps}(\Sigma, \Sigma')$ such that $(A/\mathcal{P}) \circ_\omega A'$ partially covers A.*

Proof. Let $\mathcal{S}$ be a partition of Q with $|\mathcal{S}| = m$ such that the common refinement $\mathcal{P}$ and $\mathcal{S}$

$$\mathcal{P} \vee \mathcal{Q} = \{P \cap S : \ P \in \mathcal{P}, S \in \mathcal{S}\} \tag{3.3}$$

consists only of singletons, that is, $\mathcal{P} \vee \mathcal{S} = \{\{q\} : \ q \in Q\}$.[2] Fix S_0 in S arbitrarily and define the map $\pi_\mathcal{S} : Q \to \mathcal{S}$ which sends $q \in Q$ to the unique member of $\mathcal{S}$ which contains q. Also, we declare that $\pi_\mathcal{S}(\emptyset)$ is S_0.

Define $Q' = \mathcal{S}$, $\Sigma' = \mathcal{P} \times \Sigma$ and define, for each $(P, \sigma) \in \Sigma'$, the map $f'_{(P,\sigma)} : Q' \to Q'$ as

$$f'_{(P,\sigma)}(S) = \pi_\mathcal{S}(f_\sigma(P \cap S)) \tag{3.4}$$

Thus we have constructed an automaton $A' = (Q', \Sigma', f')$. For each $P \in \mathcal{P}$, define a map $\omega_P : \Sigma \to \Sigma'$ as

$$\omega_P(\sigma) = (P, \sigma) \tag{3.5}$$

Define $\omega : \mathcal{P} \to \text{Maps}(\Sigma, \Sigma')$ by declaring $\omega(P)$ to be ω_P. Thus ω is a connection mapping from $A/\mathcal{P}$ to A' and write $\tilde{A}$ to denote the corresponding cascade product. Let Q^* be a set of states in $\tilde{A}$ defined as

$$Q^* = \{(P, S) : \ P \cap S \neq \emptyset\} \tag{3.6}$$

Note that Q^* is an invariant set in $\tilde{A}$. Define a map $\varphi : Q^* \to Q$ by declaring $\varphi(P, S)$ to be the unique element of $P \cap S$, for all (P, S) in Q^*. Define $\xi : \Sigma \to \tilde{\Sigma} = \Sigma$ be the identity map. It is a routine check to verify that (φ, ξ) is a partial covering from $\tilde{A}$ onto A, finishing the proof. ■

Lemma 3.4. *Let $\mathcal{D}$ be an admissible decomposition of an automaton $A = (Q, \Sigma, f)$ and $A/\mathcal{D}$ be a $\mathcal{D}$-factor of A. Let m be the maximum size of any element of $\mathcal{D}$. Then there is an automaton $A' = (Q', \Sigma', f')$ with $|Q'| \leq m$, and a connection mapping $\omega : \mathcal{D} \to \text{Maps}(\Sigma, \Sigma')$ such that $(A/\mathcal{D}) \circ_\omega A'$ partially covers A.*

Proof. Let $A_\mathcal{D}$ be the auxiliary automaton arising from A and $A/\mathcal{D}$. By Yoeli's construction discussed in Section 1.1 we know that $A_\mathcal{D}/\mathcal{P}$ is isomorphic to $A/\mathcal{D}$, where $\mathcal{P} = \{D \times \{D\} : \ D \in \mathcal{D}\}$. By Lemma 3.3 we know that there is an automaton A' with

$$|Q'| \leq \max_{P \in \mathcal{P}} |P| = \max_{D \in \mathcal{D}} |D \times \{D\}| = \max_{D \in \mathcal{D}} |D| = m \tag{3.7}$$

such that a cascade product $(A_\mathcal{D}/\mathcal{P}) \circ_\omega A'$ partially covers $A_\mathcal{D}$. Since $A_\mathcal{D}$ covers A by Lemma 3.2, we deduce that $(A_\mathcal{D}/\mathcal{P}) \circ A'$ partially covers A. But since $A_\mathcal{D}/\mathcal{P}$ is isomorphic to $A/\mathcal{D}$, we conclude that a cascade product $(A/\mathcal{D}) \circ_\eta A'$ partially covers A and we are done. ■

[1] Thus Ξ is the identity map on Σ'.

[2] It is easy to argue that such a partition exists.

4 Permutation-Reset Automata

Let $A = (Q, \Sigma, f)$ be an automaton and $\sigma \in \Sigma$ be fixed. We say that σ is a **permutation input** if f_σ is a bijection. We say that σ is a **reset input** if the image of f_σ is a singleton. The automaton A is said to be a **permutation-reset automaton** if every σ in Σ is either a permutation input or a reset input. Similarly, A is said to be a **permutation automaton** if each input is a permutation input and a **reset automaton** if each input is a reset input.

Example 4.1. Let $A = (Q, \sigma, f)$ be an automaton and let $|Q| = n > 1$. Let $\mathcal{D}$ be the decomposition of Q consisting of all the $(n-1)$-elements subsets of Q. Then is an admissible decomposition. *We show that there is a $\mathcal{D}$-factor of A which is a permutation-reset automaton.* To see this, first note that if σ is a permutation input in A then it is also a permutation input in any $\mathcal{D}$-factor. For each such σ we set D_σ as $f_\sigma(D)$ for all $D \in \mathcal{D}$.

Now suppose σ is not a permutation input in A. Then f_σ is not a surjection, and hence we can find $D_\sigma \in \mathcal{D}$ such that $f_\sigma(D)$ is contained in D_σ for each D in $\mathcal{D}$. Now defining, for each σ in Σ, the map $\bar{f}_\sigma : \mathcal{D} \to \mathcal{D}$ which takes D to D_σ furnishes a permutation reset automaton $(\mathcal{D}, \Sigma, \bar{f})$. ♢

Theorem 4.2. *Let $A = (Q, \Sigma, f)$ be an automaton with $|Q| = n \geq 2$. Then A can be covered by a cascade product of at most $n-1$ permutation-reset automata.*

Proof. Let $\mathcal{D}$ be the decomposition of Q comprising of all the $(n-1)$-element subsets of Q. Then $\mathcal{D}$ is an admissible decomposition of Q. By Example 4.1 there is a $\mathcal{D}$-factor $A/\mathcal{D}$ which is a permutation-reset automaton. Now by Theorem 3.4, we know that there is an automaton A' with at most $n-1$ states and a connection mapping from $A/\mathcal{D}$ to A' such that $A/\mathcal{D} \circ_\omega A'$ covers A. Now we can finish inductively by making use of Lemma 3.1. ■

A Automata and Regular Languages

A **deterministic semiautomaton**, or DSA, is a triple $S = (Q, \Sigma, f)$, where Q is a finite set whose elements are called **states**, Σ is a finite set which we call the **alphabet**, and f is a map $f : \Sigma \to \text{Maps}(Q)$. We will usually write f_σ to denote the image of σ under f. Throughout this document we will write 'automaton' to mean a DSA.

Given two automata $A = (Q, \Sigma, f)$ and $A' = (Q', \Sigma, f')$ (they have the same alphabet) we say that A and A' are **isomorphic** if there is a bijective map $\varphi : Q \to Q'$ such that the following diagram commutes for each $\sigma \in \Sigma$.

$$\begin{array}{ccc} Q & \xrightarrow{\varphi} & Q' \\ \downarrow{\scriptstyle f_\sigma} & & \downarrow{\scriptstyle f'_\sigma} \\ Q & \xrightarrow{\varphi} & Q' \end{array}$$

Let $A = (Q, \sigma, f)$ be an automaton. Consider the monoid homomorphism $h : \Sigma^* \to \text{Maps}(Q)$ given by $\sigma \mapsto f_\sigma$. Let q_0 be a state in Q and w be a word in Σ^*. The **run** of the semiautomaton S on the word w starting at q_0 is defined as the state $q_0 h(w)$.

References