Metric Properties of Automata and Formal Languages

Matthew Baulch

November 5, 2010

University of Melbourne
Department of Mathematics and Statistics
Abstract

Automata theory is intimately related to the theories of directed and topological graphs, semigroup theory and recursion theory. Inspired by the calculus of relators so fruitful in group theory, we attempt a theory of strongly connected automata with a similar flavour. We investigate sufficient conditions for a “cycle structure” to completely determine the automaton. Algorithms for computing with such invariants are developed. Language-theoretic analogues of these automata-theoretic conditions are developed and studied.

Dedication

To my energetic, constructive and engaging supervisor Dr. Lawrence Reeves. For his patience, dedication and support. To all mathematicians –past and present– who haven’t shied from rethinking the foundations, who have breathed new life or shaken the dust from ideas dismissed as old hat or unfashionable.
1 Introduction

Let $G$ be a finitely generated group with generating set $X$. Over the last 50 years, a common approach to the study of $G$ is via the question:

Given $g \in G$, what words $w \in (X \cup X^{-1})^*$ satisfy $g.w = g$?

In a geometric setting where we regard $G$ as a labelled directed graph $\Gamma_G$ (or more precisely $\Gamma_{G,X}$), the question becomes:

Given a vertex $v$ in $\Gamma_G$, what are the closed directed paths based at $v$?

The answer to each of these questions gives us the cycle structure at $x$ (and $v$). Of course, since each element in $g \in G$ has a unique inverse $g^{-1} \in G$, we quickly deduce that the above questions do not depend on the choice of $g$ or $v$. It follows that for any $g_1, g_2 \in G$ and $x \in (X \cup X^{-1})^*$; $g_1.x = g_1$ if and only if $g_2.x = g_2$. Similarly, for any $v_1, v_2 \in \Gamma_G$ and path $\rho$ based at $v_1$; if $\rho$ is closed, then it is homeomorphic$^2$ to a closed path based at $v_2$. More succinctly, the stabilisers $\text{Stab}(g)$ are the same for every element $g \in G$. Equivalently, the closed paths based at each vertex $v$ in $\Gamma_G$ are the same. In this way we see that “$G$ looks the same everywhere” – algebraically and geometrically.

Consider instead a finitely generated monoid $M$. Here, we could have $u, v, w \in M$ with $uv = u$ but $wv \neq w$. What are the obvious generalisations to the above questions? One possible approach is motivated by a basic result from group theory

**Theorem. (Lagrange Coordinate Decomposition)** Let $G$ be a group (finite or infinite) and $G_1, \ldots, G_n$ a sequence of groups with $G_1 = \{1\}$, $G_n = G$ and $G_i \trianglelefteq G_{i+1}$ for each $i \in \{1, \ldots, n\}$ then we have an embedding $G \hookrightarrow (G_1/G_0) \times \cdots \times (G_n/G_{n-1})$.

**Proof.** See [1] or indeed almost any book on group theory.

Let $F$ be the monoid of order 3 with two right zeroes. That is, $F$ has an identity $1 \in F$ and $a, b \in F$ such that $ab = bb = b$ and $ba = aa = a$. In the late sixties, Krohn and Rhodes proved the following generalisation$^3$ in the case $M$ is finite. Given monoids $M$ and $N$, we say that $M$ divides $N$ if there exists a submonoid $L \leq N$ and a surjective monoid homomorphism $\phi : L \to M$.

---

$^1$The Cayley graph.

$^2$That is, a label and orientation preserving bijection.

$^3$In fact, their proof concerned the more general case where $M$ is a semigroup.
Theorem. If $M$ is a finite monoid then there exist finite simple groups $H_1, \ldots, H_n$ and $J_1, \ldots, J_m \in \{H_1, \ldots, H_n, F\}$ such that $M$ divides $J_1 \wr \ldots \wr J_m$.

The initial publications are [5] and [6]. For a proof with more detail, see [4]. A nice modern exposition is given in [1].

This decomposition is not unique for if $P$ is any monoid and $M$ divides $J_1 \wr \ldots \wr J_m$ then $M$ divides $J_1 \wr \ldots \wr J_m \wr P$. However, we can ask for a decomposition such that $m \in \mathbb{N}$ is minimal. We call $m$ the Krohn-Rhodes complexity of $M$. It is shown in [11] that the question of whether a given monoid has Krohn-Rhodes complexity equal to 1 is decidable. It is still unknown whether Krohn-Rhodes complexity is decidable in the general case.

Given monoids $J_1, \ldots, J_m$ and knowledge of their cycle structure, we effectively deduce the cycle structure of their iterated wreath product $W = J_1 \wr \ldots \wr J_m$. If $M \hookrightarrow W$ then obviously any cycle of $M$ is a cycle of $W$. Hence, the Krohn Rhodos decomposition provides a way to categorise finite monoids by their cycle structure. Work is underway to extend this theorem to the case where $M$ is (countably) infinite but is still in its infancy. See for instance [12] or [13].

While this approach has proved fruitful for numerous purposes (see [9]), it has a distinctly algebraic flavour whose geometry is difficult to comprehend. For instance, if $\Gamma_{J_1}$ and $\Gamma_{J_2}$ are Cayley graphs of the monoids $J_1$ and $J_2$ with respect to some fixed generating sets, then how can we naturally describe a Cayley graph $\Gamma_{J_1 \wr J_2}$ for $J_1 \wr J_2$ with respect to $\Gamma_{J_1}$ and $\Gamma_{J_2}$? Another issue is that for any $p \in \mathbb{N}$, there exist many monoids $M$ for which the order of the minimal decomposition $J_1 \wr \ldots \wr J_m$ is huge compared to the order of $M$. This limits the value of $J_1 \wr \ldots \wr J_m$ as an effective means of representing $M$.

In the sequel, we experiment with a new approach. Our departure point shall be the question:

How can we naturally represent a finitely generated monoid by a canonical family of generators and relators?

Let $M$ be a finitely generated monoid with generating set $X$. We have two obvious choices for our definition of relator. On the one hand, we could take the approach from group theory and define

A relator is a word $w \in X^*$ such that $r = 1_M$ in $M$.

Alternatively, we can take the semigroup-theoretic approach and define

A relator is a pair of words $(r_1, r_2) \in X^* \times X^*$ such that $r_1 = r_2$ in $M$.

The second definition has the advantage of being more general, although at the expense of weaker geometry. In particular, the first definition allows us to identify each relator with a polygon (in the Cayley graph of $M$ with respect to $X$) based at the vertex corresponding to $1_M$. Any finite family of such polygons can be glued together to obtain another relator whose boundary word over $X^*$ is a concatenation of the original relators. This provides
1 Introduction

a nice correspondence between morphisms of words and morphisms of 1-complexes (or graphs).

It is this added geometry that prompts us to adopt the first definition. For convenience, we shall use the language of automata rather than monoids. As noted in the next section, an automaton is precisely a monoid with a fixed presentation and so we lose little (if any) generality.

Fix a generating set $\Sigma$ for $M$ and consider the corresponding automaton $\mathcal{A}$ and its Cayley graph $\Gamma$. In this language, a relator is a closed path containing the identity vertex $v_1$ of $\Gamma$. The question then arises: should we allow any closed path containing $v_1$ as a relator? If we allow this, then $\mathcal{A}$ will always have infinitely many relators, even when it has finitely many states. We want a finite automaton to have a finite set of relators. Two possible definitions we could choose are

1. A relator is a closed path $\rho$ in $\Gamma$ containing $v_1$ such that $\rho$ crosses each vertex at most once.
2. A relator is a closed path $\rho$ in $\Gamma$ containing $v_1$ such that $\rho$ crosses each edge at most once.

Condition 1 is strictly less general than condition 2. One might call a paths satisfying one or two a vertex-simple or edge-simple cycle respectively. What consequences might follow from choosing condition 1? The automata in figure 1 each have just one vertex-simple cycle. Namely, a cycle corresponding to the word $a^6 = aaaaaa$. Hence, we see a basic example where vertex-simple cycles are insufficient to distinguish one automaton from another. It’s easy to see how this example can be generalised: any subset $\Gamma'$ of $\Gamma$ for which all cycles must enter and exit $\Gamma'$ from the same vertex will not have any vertex-simple cycles which intersect $\Gamma'$. Such a subset will not affect the vertex-simple cycles of $\mathcal{A}$.

Condition 2 is the definition we shall adopt. While the edge-simple cycles of an arbitrary automaton do not completely determine it, they can provide an abundance of information. For instance, if $v$ is a vertex of $\Gamma$ from which no directed path to exists to $v_1$ then the edge-simple cycle structure will not be affected by $v$. If no such vertex $v$ exists, we say $\mathcal{A}$ (or indeed $\Gamma$) is strongly connected. In the sequel, we shall study only strongly connected automata. As we’ll see later (see for inst. figure 9), the edge-simple cycle structure of an automaton does not always determine it. That our automaton be strongly connected is thus a necessary though not sufficient condition for it to be determined by its edge-simple cycle structure.

We’ll introduce two sufficient conditions for a strongly connected automaton $\mathcal{A}$ to be determined by its edge-simple cycle structure. Namely, that $\mathcal{A}$ be focal and stable. In chapter 4, we’ll provide proofs of this fact in the case that $\mathcal{A}$ is finite. It seems likely that much of chapter 4 holds in the case that $\mathcal{A}$ is infinite although this has not yet been fully investigated.

In chapter 5, we’ll investigate the case where $M$ is a group and $\mathcal{A}$ a so-called permutation automaton. The fact that $M$ is completely determined by its cycle structure shall be
1 Introduction

proven in two respects. Firstly, that the cycle set forms a complete family of group-theoretic relations with respect to the generators \( \Sigma \). Secondly, that \( \mathcal{A} \) is focal and stable and so all of chapter 4 applies in the case \( M \) (or resp. \( \mathcal{A} \)) is finite.

Before concluding, note we have implicitly assumed that our cycles (or relators) are based at the vertex \( v_1 \) although in the sequel we shall not make this assumption. A vertex of \( \Gamma \) (or equivalently, a state of \( \mathcal{A} \)) will be fixed at which the set of cycles (or relators) will be considered. Also, \( \mathcal{A} \) will be focal or stable with respect to a fixed state.
Figure 1.0.1: A pair of automata each having a single “vertex-simple” cycle/relator.
2 Basic Definitions

“If you know neither the terminology nor the concepts, you’re ignorant. If you
know the terminology, but you don’t know the concepts, you’re dangerous.”

∼ Jacob M. Appel, Arborophilia.

An alphabet $\Sigma$ is a set of symbols. In the sequel, we shall only work with finite alphabets.
We let $\Sigma^*$ denote the collection of finite sequences of symbols from $\Sigma$. By equipping $\Sigma^*$
with the binary operation of concatenation, $\Sigma^*$ becomes a free monoid over the generators
$\Sigma$. A subset $L \subseteq \Sigma^*$ is called a (formal) language over $\Sigma$. Each element of $\Sigma^*$ is called
a word. We let $\epsilon$ denote the empty word in $\Sigma^*$. We define the Kleene star of $L$ to be

$$L^* = \{ w_1 \ldots w_n \mid w_1, \ldots, w_n \in L \}$$

For each word $w \in \Sigma^*$, we define

$$\text{pref}(w) = \{ u \in \Sigma^* \mid \exists v \in \Sigma^* : uv = w \}$$

In other words, if $w = w_1 \ldots w_n = \prod_{i=1}^{n} w_i$ with $w_1, \ldots, w_n \in \Sigma$ then $\text{pref}(w) = \{ w_1 \ldots w_i \mid i \in \{1, \ldots, n\} \} = \{ \prod_{j=1}^{i} w_j \mid i \in \{1, \ldots, n\} \}$. Each element of $\text{pref}(w)$
is called a prefix of $w$. We extend the definition of prefix from $\Sigma^*$ to the powerset $P(\Sigma^*)$
in the obvious way. For each $w \in \Sigma^*$, we let $|w|$ denote the length of the corresponding
sequence of symbols. We say that $w$ has length $|w|$.

A deterministic automaton over $\Sigma$ is a triple $A = (S, S_0, \delta)$ where $S$ is a set, $S_0 \in S$
and $\delta : S \times \Sigma \rightarrow S$. We say that $A$ is finite if $S$ is finite. The set $S$ is called the collection
of states of $A$. $S_0$ is the initial state and $\delta$ is the transition function between states.
We extend $\delta$ to a map $\tilde{\delta} : S \times \Sigma^* \rightarrow S$ by letting $\tilde{\delta}(S, \epsilon) = \epsilon$ and $\tilde{\delta}(S, cw) = \tilde{\delta}(\delta(S, c), w)$
for $c \in \Sigma$ and $w \in \Sigma^*$. Without explicit mention, we will often write $\delta$ to mean $\tilde{\delta}$.
Occasionally, we may associate with $A$ a family of states $F \subseteq S$ called the accept (or final)
states of $A$. In such a case, we define the language accepted by $A$ to be the family of words $L(A) = \{ w \in \Sigma^* \mid \delta(S_0, w) \in F \}$. The transition monoid of $A$ is
the collection of state maps $\{ S \rightarrow \delta(S, w) \mid w \in \Sigma^* \}$ with function composition as the binary operation. A language $L \subseteq \Sigma^*$ is regular if there exists a finite deterministic
automaton $A$ such that $L = L(A)$. In chapter 6, we shall occasionally refer to the class of context-free
languages, a family for which the regular languages form a strict subfamily. Context-free languages shall not play a part in any of our key results and so we don’t bother to define them here. For more on formal languages, automata or for the definition
of a context-free language, see for instance [10].
2 Basic Definitions

If $M$ is a monoid with finite generating set $X$, then the Cayley graph of $M$ with respect to $X$ is the graph with vertices $M$ and for each $a \in M$, $x \in X$ a directed edge from the vertex $a$ to the vertex $ax$. With these definitions, if $M$ is a monoid then there exists an automaton $A$ such that $M$ is the transition monoid of $A$. Conversely, with each automaton $A$ we have an associated transition monoid. In this way, we see that an automaton $A$ is precisely a monoid with a fixed generating set - the alphabet of $A$.

For any graphs $\Gamma_1$ and $\Gamma_2$, we define their cartesian product $\Gamma_1 \times \Gamma_2$ and tensor product $\Gamma_1 \otimes \Gamma_2$ as follows. Both graphs have vertex sets

$$\{(\alpha_1, \alpha_2) \mid \alpha_1 \text{ is an edge of } \Gamma_1, \alpha_2 \text{ is an edge of } \Gamma_2\}$$

Their edge sets are defined as follows.

- If $\Gamma_1$ has an edge from $\alpha_1$ to $\beta_1$ or $\Gamma_2$ has an edge from $\alpha_2$ to $\beta_2$ then $\Gamma_1 \times \Gamma_2$ has an edge from $(\alpha_1, \alpha_2)$ to $(\beta_1, \beta_2)$.

- If $\Gamma_1$ has an edge from $\alpha_1$ to $\beta_1$ and $\Gamma_2$ has an edge from $\alpha_2$ to $\beta_2$ then $\Gamma_1 \otimes \Gamma_2$ has an edge from $(\alpha_1, \alpha_2)$ to $(\beta_1, \beta_2)$.

For instance, we see from the definition that $\Gamma_1 \otimes \Gamma_2$ is always a subgraph of $\Gamma_1 \times \Gamma_2$.

An automaton $A$ is called strongly connected if for all states $S$ and $T$ of $A$ there exists $u, v \in \Sigma^*$ such that $\delta(S, u) = T$ and $\delta(T, v) = S$. We shall often abbreviate and refer to $A$ as an SCDA. Let $A$ be a strongly connected deterministic automaton (or SCDA). For each state $S$ of $A$, we let path$_A(S)$ denote the collection of words $w \in \Sigma^*$ that satisfy the condition

$$\{xa, yb\} \subseteq \text{pref}(w) \land (\delta(S, x) = \delta(S, y)) \implies (a \neq b) \lor (x = y)$$

for each $a, b \in \Sigma$ and $x, y \in \Sigma^*$. Each such word is called a path. When the automaton being referred to is clear, we simply write path($S$). The same convention is adopted for other functions on states. Define cyc($S$) to be the largest subset of path($S$) for which $\delta(S, \text{cyc}(S)) = \{S\}$. Each element of cyc($S$) are called a cycle based at $S$, or an $S$-cycle.
3 Cycle Structure

“All of life is a coming home. ... All the restless hearts of the world, all trying to find a way home. ... Picture yourself walking for days in the driving snow; you don't even know you’re walking in circles. ... How small you can feel, and how far away home can be. Home. The dictionary defines it as both a place of origin and a goal or destination. ... as the poet Dante put it: In the middle of the journey ... I found myself in a dark wood, for I had lost the right path. Eventually I would find the right path, but in the most unlikely place.”

~ Patch Adams

3.1 New Cycles from Old

We now try to establish some basic properties of the set cyc($S$) for $S$ a state of a strongly connected deterministic automaton (or SCDA). Given an element $v \in$ cyc($S$), what other elements of cyc($S$) can we deduce the existence of?

**Lemma 1.** Let $u, v, w \in \Sigma^*$. If $uvw \in$ cyc($S$) and $\delta(S,u) = \delta(S,uv)$ then $uw \in$ cyc($S$) and $v \in$ cyc($\delta(S,u)$).

**Proof.** Firstly, we prove $uw \in$ cyc($S$). Take $a,b \in \Sigma$ and $x,y \in \Sigma^*$ s.t. $\{xa,yb\} \subseteq$ pref($uw$) and $\delta(S,x) = \delta(S,y)$. If $\{xa,yb\} \subseteq$ pref($u$) then $a \neq b \lor x = y$ and so we are done. Otherwise, $xa \in$ pref($uw$)\ {pref($u$)} or $yb \in$ pref($uw$)\ {u}. Consider the case $xa \in$ pref($uw$)\ {pref($u$)} and $yb \in$ pref($u$). Clearly, $x \neq y$ and so we must show $a \neq b$. Now, $\exists r \in$ pref($u$) s.t. $x = ur$ and we have $\delta(S,uru) = \delta(S,uvr) = \delta(S,u),r) = \delta(S,u),r) = \delta(S,ur) = \delta(S,x) = \delta(S,y)$. Since $\{uvra,xb\} \subseteq$ pref($uw$), either $a \neq b$ or $wv = y$. If $wv = y$ then $yb \neq$ pref($u$) which is a contradiction. Hence, $a \neq b$. Similarly, $yb \in$ pref($uw$)\ {pref($u$)} and $xa \in$ pref($u$) implies $a \neq b$. We are left with the case $\{xa,yb\} \subseteq$ pref($uw$)\ {pref($u$)}. Here, $\exists r,t \in$ pref($w$) s.t. $x = ur$ and $y = rt$. Now, $\delta(S,uvr) = \delta(S,uru) = \delta(S,x) = \delta(S,y) = \delta(S,ur) = \delta(S,wt) = \delta(S,u)$. Then $\{uxa,uyb\} \subseteq$ pref($uvw$) and $\delta(S,ux) = \delta(S,uy)$ from which we conclude $a \neq b$ or $ux = uy$. That is, $a \neq b \lor x = y$ and so $v \in$ cyc($\delta(S,u)$).

$\square$
A handy specialisation of the above is:

**Corollary 1.** If \( u \in \text{cyc}(S) \), \( v \in \text{pref}(u) \) and \( \delta(S, v) = S \) then \( v \in \text{cyc}(S) \).

**Proof.** Let \( x \in \Sigma^* \) be s.t \( x = vx \). Apply lemma 1 to the fact that \( \bar{u} = \epsilon \), \( \bar{v} = v \) and \( \bar{w} = x \) satisfy \( \delta(S, \bar{u}) = \delta(S, \bar{u}v) \) to conclude \( \bar{v} \in \text{cyc}(\delta(S, \bar{u})) = \text{cyc}(S) \).

Suppose a pair of cycle words are related by a common prefix. What can we say?

**Lemma 2.** Let \( u, v \in \Sigma^* \). If \( \{u, uv\} \subseteq \text{cyc}(S) \) then \( v \in \text{cyc}(S) \).

**Proof.** By definition we have that for every \( a, b \in \Sigma \) and \( x, y \in \Sigma^* \):

\[
\{xa, yb\} \subseteq \text{pref}(u) \land \delta(S, x) = \delta(S, y) \implies a \neq b \lor x = y \quad (3.1.1)
\]

It is straightforward that \( \delta(S, v) = S \). We must show that given such an \( a, b, x, y \):

\[
\{xa, yb\} \subseteq \text{pref}(v) \land \delta(S, x) = \delta(S, y) \implies a \neq b \lor x = y
\]

Fix \( a, b \in \Sigma \) and \( x, y \in \Sigma^* \) such that \( \{xa, yb\} \subseteq \text{pref}(v) \) and \( \delta(S, x) = \delta(S, y) \). Then \( \{uxa, uby\} \subseteq \text{pref}(uv) \). Now, \( \delta(S, uy) = \delta(\delta(S, u), y) = \delta(S, y) \) and so \( \delta(S, ux) = \)
\( \delta(S, uy) \). By (3.1.1), \( a \neq b \) or \( ux = uy \). If \( ux = uy \) then \( x = y \). Therefore \( a \neq b \) or \( x = y \).

\[\square\]

Of course, the set \( \text{cyc}(S) \) depends on the state \( S \). Given \( \text{cyc}(S) \) and another state \( T = \delta(S, u) \), what elements of \( \text{cyc}(T) \) are implied?

**Lemma 3.** Let \( u, v \in \Sigma^* \) and set \( T = \delta(S, u) \). If \( uv \in \text{cyc}(S) \) then \( vu \in \text{cyc}(T) \).

**Proof.** Suppose \( uv \in \text{cyc}(S) \). Then given any \( a, b \in \Sigma \) and \( \bar{x}, \bar{y} \in \Sigma^* \) we have

\[ \{ \bar{x}a, \bar{y}b \} \subseteq \text{pref}(uv) \land \delta(S, \bar{x}) = \delta(S, \bar{y}) \Rightarrow a \neq b \lor \bar{x} = \bar{y} \]

Consequently, for any \( a, b \in \Sigma \) and \( x, y \in \Sigma^* \) we obtain

\[ \{ uxa, uyb \} \subseteq \text{pref}(uv) \land \delta(S, ux) = \delta(S, uy) \Rightarrow a \neq b \lor ux = uy \]

by setting \( \bar{a} = a, \bar{b} = b, \bar{x} = ux \) and \( \bar{y} = uy \). From the equivalences \( x = y \iff ux = uy \), \( \{ uxa, uyb \} \subseteq \text{pref}(uv) \iff \{ xa, yb \} \subseteq \text{pref}(v) \) and \( T = \delta(S, u) \) we conclude

\[ \{ xa, yb \} \subseteq \text{pref}(v) \land \delta(T, x) = \delta(T, y) \Rightarrow a \neq b \lor x = y \]

We are left with the case \( \{ xa, yb \} \subseteq \text{pref}(vu) \setminus \text{pref}(v) \). Here we can find \( p, q \in \Sigma^* \) s.t. \( xa = vpa \) and \( yb = vqb \). Hence, \( \delta(T, x) = \delta(T, vp) = \delta(S, uvp) = \delta(S, p) \) and similarly \( \delta(T, y) = \delta(S, q) \). Assuming \( \delta(T, x) = \delta(T, y) \) it follows that \( \delta(S, p) = \delta(S, q) \). Clearly, \( \{ pa, qb \} \subseteq \text{pref}(u) \subseteq \text{pref}(uv) \) and so we can apply our hypothesis to conclude \( a \neq b \lor p = q \). In the case \( a = b \) we have \( p = q \iff vpa = vqb \iff xa = yb \iff x = y \). It is straightforward that \( \delta(S, vu) = S \).

\[\square\]

We provide here a vast generalisation of lemma 2.

**Lemma 4.** Let \( \{ u_1, \ldots, u_n \} \subseteq \text{cyc}(S) \) and \( m \leq n \) a positive integer. Then

\[ \prod_{i=1}^{n} u_i \in \text{cyc}(S) \implies \prod_{i=1}^{m} u_i \in \text{cyc}(S) \]

**Proof.** Suppose \( \{ u_1, \ldots, u_n \} \subseteq \text{cyc}(S) \) with \( \prod_{i=1}^{n} u_i \in \text{cyc}(S) \) and \( m < n \) is a positive integer. By lemma 3 with \( u = \prod_{i=m+1}^{n} u_i \) we have \( (\prod_{i=m+1}^{n} u_i)(\prod_{i=1}^{m} u_i) = u_{m+1} \ldots u_n u_1 \ldots u_m \in \text{cyc}(S) \). See figure.

By lemma 2 we have that \( u_{m+2} \ldots u_n u_1 \ldots u_m \in \text{cyc}(S) \). Continuing in this way, we conclude that \( u_1 \ldots u_m = \prod_{i=1}^{m} u_i \in \text{cyc}(S) \).

\[\square\]
So far we have investigated situations under which a cycle $z \in \text{cyc}(S)$ can be shortened or relocated between states. As we’ll see, under certain circumstances we can apply a permutation $\pi$ to $z$ to obtain another element of $\text{cyc}(S)$. We begin with a basic proposition.

**Lemma 5.** If $\{u,v,w,uw\} \subseteq \text{cyc}(S)$ then $vwu \in \text{cyc}(S)$.

**Proof.** Suppose $\{u,v,w,uw\} \subseteq \text{cyc}(S)$. Fix $a,b \in \Sigma$ and $x,y \in \Sigma^*$ such that $\{xa,yb\} \subseteq \text{pref}(vwu)$ and $\delta(S,x) = \delta(S,y)$. By lemma 4, $vw \in \text{cyc}(S)$ and so we have $vwu \in \text{cyc}(S)$ by lemma 3. Applying these lemmas again, $wu \in \text{cyc}(S)$ and so $wuv \in \text{cyc}(S)$. Therefore, $wu \in \text{cyc}(S)$ and so $vu \in \text{cyc}(S)$. We have four cases:

1. $\{xa,yb\} \subseteq \text{pref}(vu)$
2. $xa \in \text{pref}(vwu) \setminus \text{pref}(vu), yb \in \text{pref}(vu)$
3. $xa \in \text{pref}(vu), yb \in \text{pref}(vwu) \setminus \text{pref}(vu)$
4. $xa \in \text{pref}(vwu) \setminus \text{pref}(vu), yb \in \text{pref}(vwu) \setminus \text{pref}(vu)$

Case 1: Since $\{xa,yb\} \subseteq \text{pref}(vu)$ and $vu \in \text{cyc}(S)$, $a \neq b$ or $x = y$ follows.

Case 2: There are two sub-cases. Namely, $yb \in \text{pref}(vu) \setminus \text{pref}(v)$ or $yb \in \text{pref}(v)$.

For the former, there exists $p \in \Sigma^*$ s.t. $xa = vpa$ and thus $x = vp$. Firstly, if $yb \in \text{pref}(vu) \setminus \text{pref}(v)$ then $\exists q \in \Sigma^*$ such that $y = vq$. Now, $\delta(S,x) = \delta(S,vp) = \delta(S,p)$ and $\delta(S,y) = \delta(S,vq) = \delta(S,q)$. Hence, $\delta(S,p) = \delta(S,q)$. We have $pa \in \text{pref}(vw)$ and $qb \in \text{pref}(u) \subseteq \text{pref}(uvw)$ and so $\{pa,qb\} \subseteq \text{pref}(uvw)$. Since $uw \in \text{cyc}(S)$, $a \neq b$ or $p = q$. That is, $a \neq b$ or $x = y$ and we are done.

For the latter, $yb \in \text{pref}(v)$. By our assumption $\exists r \in \Sigma^*$ such that $x = vur$ where $r \in \text{pref}(w)$. Since $uv \in \text{cyc}(S)$ we have $vu \in \text{cyc}(S)$. Now, $\delta(S,x) = \delta(S,vur) = \delta(S,r) = \delta(S,vr)$ and so $\delta(S,vr) = \delta(S,y)$. Combining this with the fact $\{vra,yb\} \subseteq$
3 Cycle Structure

pref(vw) we have \( a \neq b \) or \( vr = y \). If \( vr = y \) then \( r = y \) and \( r = \epsilon \) since \( y \in \text{pref}(v) \). But \( ya \in \text{pref}(v) \) which is a contradiction. Therefore, we must have \( a \neq b \) and so the statement \( a \neq b \lor x = y \) holds.

Case 3: Same as for case 2 but with \( a \) replaced by \( b \) and \( x \) replaced by \( y \).

Case 4: There exist \( s,t \in \Sigma^* \) such that \( x = vus \) and \( y = vu \) where \( s,t \in \text{pref}(w) \). We have \( \delta(S,x) = \delta(S,vus) = \delta(S,s) \) and \( \delta(S,y) = \delta(S,vut) = \delta(S,t) \). Therefore, \( \delta(S,s) = \delta(S,t) \). Also, \( \{sa, tb\} \subseteq \text{pref}(w) \) which implies \( a \neq b \) or \( s = t \). That is, \( a \neq b \) or \( x = y \).

Lemma 5 allows us to permute subwords \( u \) and \( v \) of a cycle \( z \in \text{cyc}(S) \) provided that \( uv \in \text{pref}(z) \). We now relax this condition.

**Lemma 6.** If \( \{u,v,w,x,y,uvwxy\} \subseteq \text{cyc}(S) \) then \( uxwvy \in \text{cyc}(S) \).

**Proof.** Suppose \( \{u,v,w,x,y,uvwxy\} \subseteq \text{cyc}(S) \). By lemma 3, \( vwxyu \in \text{cyc}(S) \). Now, \( xyu \in \text{cyc}(S) \) by lemma 4 and so \( wxyu \in \text{cyc}(S) \) by lemma 5. Lemma 3 tells us \( vxyuw \in \text{cyc}(S) \) and so \( yuwxv \in \text{cyc}(S) \) by lemmas 4 and 5 respectively. Applying lemmas 3, 4, 5 and 3 tells us that \( wxvyu \), \( yuwxv \), \( xwvyu \) and \( uwxy \) respectively lie in \( \text{cyc}(S) \).

And now our most general statement concerning permutations of a word \( z \in \text{cyc}(S) \).

**Theorem 1.** Let \( \{u_1, \ldots, u_n\} \subseteq \text{cyc}(S) \) and \( \pi : \{1, \ldots, n\} \rightarrow \{1, \ldots, n\} \) a permutation. Then

\[
\prod_{i=1}^{n} u_i \in \text{cyc}(S) \implies \prod_{i=1}^{n} u_{\pi(i)} \in \text{cyc}(S)
\]

**Proof.** With repeated application of lemma 6, we can reshuffle the \( u_i \) in any order we please. The rest is notation.

If \( w \in \text{cyc}(S) \) satisfies the condition \( \text{pref}(w) \cap \text{cyc}(S) = \{\epsilon, w\} \) then we say \( w \) is an **irreducible** \( S \)-cycle. Otherwise, \( w \) is a **reducible** \( S \)-cycle. Let \( \text{irr}(S) \) denote the set of irreducible \( S \)-cycles.

**Lemma 7.** Let \( a,b \in \Sigma \). If \( \delta(S,a) = \delta(S,b) \) then \( \exists \Omega \subseteq \Sigma^* \) such that \( a\Omega = \text{irr}(S) \cap a\Sigma^* \) and \( b\Omega = \text{irr}(S) \cap b\Sigma^* \).
3 Cycle Structure

Proof. It is sufficient to show that \( \forall w \in \Sigma^* : aw \in \text{irr}(S) \implies bw \in \text{irr}(S) \). Fix such a \( w \). Then \( \text{pref}(aw) \cap \text{cyc}(S) = \{aw\} \). Take \( u \in \Sigma^* \) such that \( bu \in \text{pref}(bw) \cap \text{cyc}(S) \). Clearly, \( au \in \text{pref}(aw) \). We claim that \( au \in \text{cyc}(S) \). It then follows that \( au \in \text{irr}(S) \) from which we conclude \( u = w \) and thus \( \text{pref}(bw) \cap \text{cyc}(S) = \{bw\} \).

For the claim, fix \( c, d \in \Sigma \) and \( x, y \in \Sigma^* \) such that \( \{xc, yd\} \subseteq \text{pref}(au) \) and \( \delta(S, x) = \delta(S, y) \). If \( x = \epsilon \) then \( c = a \) and \( \delta(S, y) = \delta(S, \epsilon) = S \). Since \( y \in \text{pref}(aw) \) we can apply lemma 1 to conclude that \( y \in \text{cyc}(S) \) and so \( y \in \text{pref}(aw) \cap \text{cyc}(S) \). By our initial assumption, \( y = aw \). But this contradicts \( yd \in \text{pref}(aw) \). Hence, \( x \neq \epsilon \). By the same argument we have \( y \neq \epsilon \). In conclusion, \( \{xc, yd\} \subseteq \text{pref}(au) \) and \( \delta(S, x) = \delta(S, y) \) implies \( x \neq \epsilon \) and \( y \neq \epsilon \). When \( x \neq \epsilon \) and \( y \neq \epsilon \), \( \exists x, y \in \Sigma^* \) such that \( x = a\bar{x} \) and \( y = a\bar{y} \). Now, \( \delta(S, b\bar{x}) = \delta(S, b\bar{y}) \) and \( \{b\bar{x}, b\bar{y}\} \subseteq \text{pref}(bu) \). Since \( bu \in \text{cyc}(S) \) we have \( c \neq d \) or \( b\bar{x} = b\bar{y} \). That is, \( c \neq d \) or \( x = y \). Consequently, \( au \in \text{cyc}(S) \).

Lemma 8. If \( w \in \text{cyc}(S) \) then \( \exists w_1, \ldots, w_n \in \text{irr}(S) \) such that \( w = \prod_{i=1}^{n} w_i \).

Proof. Take \( w \in \text{cyc}(S) \). If \( w \in \text{irr}(S) \), we are done. Otherwise, \( \exists u_1 \in \text{pref}(w) \cap \text{cyc}(S) \) such that \( u_1 \notin \{\epsilon, w\} \) and so \( \exists v_1 \in \Sigma^* \) such that \( w = u_1v_1 \). Choose the shortest such \( u_1 \) that satisfies these conditions. Then \( \text{pref}(u_1) \cap \text{cyc}(S) = \{\epsilon, u_1\} \) and so \( u_1 \in \text{irr}(S) \). If \( v_1 \in \text{irr}(S) \), we are done. Otherwise, repeat the same process to find \( u_2 \in \text{pref}(v_1) \cap \text{cyc}(S) \) and \( v_2 \in \Sigma^* \) such that \( u_2 \in \text{irr}(S) \). Continuing in this way, we can find \( \{u_1, \ldots, u_m, v_m\} \subseteq \text{irr}(S) \) such that \( w = u_1 \ldots u_mv_m \).

Before concluding our discussion of cycles, we prove a few basic facts about a more specialised type of cycle. Namely, the so-called “vertex-simple” cycles described in the introduction. We now give a precise definition.

If \( w \in \text{path}(S) \) satisfies the condition
\[
\forall x, y \in \text{pref}(w) : \delta(S, x) = \delta(S, y) \implies x = y \lor \{x, y\} = \{\epsilon, w\}
\]
we say \( w \) is a rigid \( S \)-path. Let \( \text{rigPath}(S) \) denote the set of rigid \( S \)-paths. Define \( \text{rig}(S) = \text{rigPath}(S) \cap \text{cyc}(S) \) to be the collection of rigid \( S \)-cycles.

Proposition 1. \( \text{rig}(S) \subseteq \text{irr}(S) \).

Proof. Suppose \( w \in \text{rig}(S) \). Take \( u \in \text{pref}(w) \cap \text{cyc}(S) \). Then \( \delta(S, u) = S \). Since \( \delta(S, w) = S \), \( \delta(S, u) = \delta(S, w) \) and thus \( u = w \lor \{u, w\} = \{\epsilon, w\} \) by the rigidity of \( w \). That is, \( u \in \{\epsilon, w\} \) and so \( u \in \text{irr}(S) \).

Proposition 2. Let \( S \) and \( T \) be states of \( A \). Then
\[
\text{rig}(S) = \{w \in \text{cyc}(S) \mid \forall u, v \in \Sigma^* : wv = w \implies vu \in \text{irr}(\delta(S, u))\}
\]
3 Cycle Structure

Proof. Let $w \in \text{rig}(S)$ and fix $u, v \in \Sigma^*$ such that $w = uv$. Firstly, consider the case $S \neq T$. By lemma 3, $vu \in \text{cyc}(T)$. We claim that $\text{pref}(vu) \cap \text{cyc}(T) = \{\epsilon, vu\}$. Take $r \in \text{pref}(vu) \cap \text{cyc}(T) = \{\epsilon, vu\}$. In the case $r \in \text{pref}(v)$ we have $ur \in \text{pref}(w)$ and so $\delta(S, ur) = \delta(S, u)$. Since $w \in \text{rig}(S)$ we have $u = ur$ or $\{u, ur\} = \{\epsilon, vu\}$. If $u = ur$ then $r = \epsilon$. Otherwise, $u = \epsilon$ and $r = vu$. Therefore, $r \in \{\epsilon, vu\}$. In the case $r \in \text{pref}(vu) \setminus \text{pref}(v)$ there exist $p, q \in \Sigma^* \setminus \{\epsilon\}$ such that $r = vp$ and $u = pq$. Now, since $vp \in \text{cyc}(T)$ and $\delta(T, v) = S$ lemma 3 gives $pv \in \text{cyc}(S)$. We have $\{p, pq\} \subseteq \text{pref}(uv)$ with $\delta(S, p) = \delta(S, pq)$. Hence, $p = pq$ or $\{p, pq\} = \{\epsilon, uv\}$ and so $(p, q) \in \{(u, \epsilon), (\epsilon, uv)\}$. Consequently, $r \in \{v, vu\}$. If $r = v$ then $\delta(S, uv) = \delta(T, v) = T$ and so $S = \delta(S, uv) = T$. This contradicts our assumption. Therefore, $r = vu$. This proves our claim and so $vu \in \text{irr}(T)$. Finally, we consider the case $S = T$. Here, $\{u, uv\} \subseteq \text{pref}(uv)$ with $\delta(S, u) = \delta(S, uv)$. Once again, $uv \in \text{rig}(S)$ and so $u = uv$ or $\{u, uv\} = \{\epsilon, uv\}$. That is, $v = \epsilon$ or $u = \epsilon$. Both cases give $uw = vu$ and thus $vu \in \text{rig}(S) = \text{rig}(T) \supseteq \text{irr}(T)$. This establishes the inclusion $\text{rig}(S) \subseteq \{w \in \text{cyc}(S) \mid \forall u, v \in \Sigma^* : uv = w \Rightarrow vu \in \text{irr}(\delta(S, u))\}$.

For the other inclusion, let $w \in \text{cyc}(S)$ satisfy

$$\forall u, v \in \Sigma^* : uv = w \Rightarrow vu \in \text{irr}(\delta(S, u))$$

and fix $x, y \in \text{pref}(w)$ such that $\delta(S, x) = \delta(S, y)$. Set $T = \delta(S, x) = \delta(S, y)$. The conclusion then follows from the claim $x = y \lor \{x, y\} = \{\epsilon, w\}$.

For the claim, we note that $\exists \bar{x}, \bar{y} \in \Sigma^*$ such that $x\bar{x} = y\bar{y} = w$. By our hypothesis, $\{\bar{x}x, \bar{y}y\} \subseteq \text{irr}(T)$. If $x = y$, we are done. Otherwise, $x \in \text{pref}(y)$ or $y \in \text{pref}(x)$. If $x \in \text{pref}(y)$ then $\bar{y}x \in \text{pref}(\bar{y}y)$ and $\delta(T, \bar{y}x) = T$. Lemma 1 tells us that $\bar{y}x \in \text{cyc}(T)$. Since $\bar{y}y \in \text{irr}(T)$, $\text{pref}(\bar{y}y) \cap \text{cyc}(T) = \{\epsilon, \bar{y}, y\}$. Hence, $\bar{y}x \in \{\epsilon, \bar{y}y\}$ and so $(x, y) = (\epsilon, w)$ or $x = y$. Interchanging the roles of $x$ and $y$, the same argument tells us $y \in \text{pref}(x) \Longrightarrow x = y \lor (x, y) = (w, \epsilon)$. This establishes the claim.

$\square$
3 Cycle Structure

3.2 Distance and Related Invariants

Our calculus of cycles developed in section 3.1, while advancing our cause, still can’t provide us with complete knowledge of an automaton from the set cyc(S). As figures 3.2.1 and 3.2.2 demonstrate, we can construct SCDA A and A̅ having states S and S̅ for which cyc(S) = cyc(S̅). That is, the cycle set is merely an invariant of an SCDA - not a representation.

\[
\text{cyc}(S) = \{aa, ab, ba, bb\} = \text{cyc}(\overline{S})
\]

Figure 3.2.1: SCDA with equal cycle sets. Of the marked states, only one is focal.

For any states S and T of A we define

- \( \Delta(S, T) = \min\{|x| \mid x \in \Sigma^* \land \delta(S, x) = T\} \)
- \( \text{geo}(S) = \{x \in \Sigma^* \mid \Delta(S, \delta(S, x)) = |x|\} \)
- \( \text{geo}(S, T) = \{x \in \text{geo}(S) \mid \delta(S, x) = T\} \)

\( \Delta(S, T) \) is called the distance from S to T and each element \( w \in \text{geo}(S) \) is called a geodesic of S. An element \( w \in \text{cyc}(S) \) is called a flat S-cycle if \( \exists u \in \text{geo}(S) \) and \( v \in \text{geo}(\delta(S, u)) \) such that \( w = uv \). Let flat(S) denote the set flat S-cycles. It is straightforward to see that a flat cycle is necessarily irreducible. Therefore, \( \text{flat}(S) \subseteq \text{irr}(S) \).

If for all states P and Q we have \( P = Q \iff \text{geo}(P, S) = \text{geo}(Q, S) \) we say A is focal at S. We say A is stable at S if for all states T, \( a \in \Sigma \cup \{\epsilon\} \), \( u \in \text{geo}(S, T) \) and \( v \in \text{geo}(\delta(T, a), S) \) we have \( uav \in \text{cyc}(S) \). Figure 3.2.1 provides an example of an automaton that is not focal at \( T \) while figure 3.2.2 provides an example of an automaton not stable at S. We list without proof a some easy facts.

**Proposition 3.**

1. If \( w \in \text{geo}(S) \) and \( u, v \in \text{pref}(w) \) then \( \delta(S, u) = \delta(S, v) \iff u = v \).
2. \( \text{geo}(S) = \{w \in \Sigma^* \mid \delta(S, w) \notin \delta(S, \cup_{n=0}^{1} \Sigma^n)\} \)
3. If \( u, v \in \Sigma^* \) and \( uv \in \text{flat}(S) \) then \( uv \in \text{flat}(\delta(S, u)) \).
4. If A is stable at S then for all states T, \( a \in \Sigma \cup \{\epsilon\} \), \( u \in \text{geo}(S, T) \) and \( v \in \text{geo}(\delta(T, a), S) \) we have \( uav \in \text{irr}(S) \).
5. If A is stable at S then \( \text{geo}(S, T) \subseteq \text{flat}(S) \) for all states T.
However, none shall be needed in anything that follows. If the distance function $\Delta$ is symmetric, we obtain the stable condition for free.

**Lemma 9.** If for every state $T$ of $\mathcal{A}$ we have $\Delta(S,T) = \Delta(T,S)$ then $\mathcal{A}$ is stable at $S$.

**Proof.** Fix a state $T$, $u \in \text{geo}(S,T)$, $c \in \Sigma$ and $v \in \text{geo}(\delta(T,a),S)$. Take $x, y \in \Sigma^*$ and $a,b \in \Sigma$ such that $\{xa,yb\} \subseteq \text{pref}(ucv)$ and $\delta(S,x) = \delta(S,y)$. It is sufficient to show that $ucv \in \text{cyc}(S)$. In turn, this follows from $x = y \lor a \neq b$. Wlog, we may assume $x \in \text{pref}(y)$.

If $\{xa,yb\} \subseteq \text{pref}(u)$ then $x, y \in \text{pref}(u)$ and so $x = y$ from the fact $u \in \text{geo}(S)$. Similarly, if $\{xa,yb\} \subseteq \text{pref}(ucv) \setminus \text{pref}(uc)$ we must have $x = y$.

What remains is the case $xa \in \text{pref}(uc)$ and $yb \in \text{pref}(ucv) \setminus \text{pref}(uc)$. Here, we can find $z \in \Sigma^*$ such that $yb = uczb$ and thus $y = ucz$. Clearly, $z \in \text{geo}(\delta(T,c))$. If $xa = uc$ then $x = u$, $a = c$ and $\delta(T,cz) = \delta(S,ucz) = \delta(S,y) = \delta(S,x) = \delta(S,u) = T$ which implies $b \neq c$. To see this, note that $b = c$ together with the fact $zb \in \text{geo}(\delta(T,c))$ implies $|zb| = 0$ which is impossible. Hence, $xa = uc \implies a \neq b$.

The remaining case is thus $xa \in \text{pref}(u)$ and $yb \in \text{ucz}$ with $z$ as above. Here, we have $v = zbx$ and $u = xaz$ for some $z, x, z \in \Sigma^*$.

Now, $xa \in \text{pref}(u)$ and $u \in \text{geo}(S,T)$ tells us

$$\Delta(\delta(S,x),T) = \Delta(\delta(S,xa),T) + 1$$
Figure 3.2.3: The good - when ucb defines a path.

Figure 3.2.4: The bad - when ucb self intersects along an edge.
3 Cycle Structure

while \( zb \in \text{pref}(\text{geo}(\delta(T,c),S)) \) tells us

\[
\Delta(\delta(T,cz),T) = \Delta(\delta(T,czb),T) - 1
\]

Using the fact \( \delta(T,cz) = \delta(S,y) = \delta(S,x) \) the above equations yield

\[
\Delta(\delta(S,xa),T) + 1 = \Delta(\delta(T,czb),T) - 1
\]

and applying the fact \( \delta(T,cz) = \delta(S,x) \) once more gives us

\[
\Delta(\delta(S,xa),T) + 1 = \Delta(\delta(S,xb),T) - 1
\]

which can only hold if \( \delta(S,xa) \neq \delta(S,xb) \). This implies \( a \neq b \).

\[\Box\]

**Example 1.** Fix \( n \in \mathbb{N} \) and consider an automaton \( A \) over the unary alphabet \( \Sigma = \{a\} \) with states \( \{1, \ldots, n\} \) and transition function \( \delta \) given by \( \delta : (n,a) \mapsto 1 \) and \( \delta : (i,a) \mapsto i+1 \) for \( i \in \{1, \ldots, n-1\} \). Let \( S = 1 \). For each state \( i \in \{2, \ldots, n\} \) we have \( \Delta(i,S) = n-i+1 \) and \( \Delta(S,i) = i-1 \). However, \( A \) is stable at \( S \). Hence, the converse to lemma 9 is false.
4 Representation by Cycle Structure

"Science is what we understand well enough to explain to a computer. Art is everything else we do."
~ D.E. Knuth

4.1 The Transition Function

For this section, let $A$ be an SCDA with finitely many states such that $A$ is focal and stable at $S$. Let $\text{irr}(S)$, $\text{flat}(S)$ and $\text{geo}(S)$ be given. Given $u \in \text{geo}(S)$ and $a \in \Sigma$ such that $ua \notin \text{geo}(S)$ we'll show how to compute $x \in \text{geo}(S)$ such that $\delta(S, x) = \delta(S, ua)$. As hinted at in section 3.1, the sets $\text{cyc}(S)$ and $\text{irr}(S)$ have an intimate relationship. We now show that no generality is lost in representing $A$ by $\text{irr}(S)$ instead of $\text{cyc}(S)$.

**Proposition 4.** Given $\text{cyc}(S)$ we can determine $\text{irr}(S)$.

**Proof.** From the definition of $\text{irr}(S)$, it is sufficient to calculate the set $\text{pref}(w) \cap \text{cyc}(S)$ for each $w \in \text{cyc}(S)$. $\text{irr}(S)$ contains precisely the $w$ for which this set is $\{\epsilon, w\}$. Since all sets here are finite, this can be effectively determined.

If $P$ is a state of $A$ then $\text{geo}(S, P)$ is always non-empty. When $A$ is strongly connected, we always have $\text{geo}(P, S)$ non-empty. As figure 3.2.2 demonstrates such a state may not cross any cycles based at $S$ as all closed paths containing $S$ and $P$ may self-intersect. Our assumption that $A$ is stable at $S$ guarantees that for any state $P$ there exists an element of $\text{cyc}(S)$ which crosses $P$. More importantly,

**Lemma 10.** Given $\text{irr}(S)$, $u \in \text{geo}(S)$ and $a \in \Sigma \cup \{\epsilon\}$ we can determine the set $\text{geo}(\delta(S, ua), S)$.

**Proof.** Since $A$ is stable at $S$,

$$\forall v \in \text{geo}(\delta(S, ua), S) : uv \epsilon \text{irr}(S)$$ (4.1.1)

Hence, to calculate $\text{geo}(\delta(S, ua), S)$, we must decide which elements of $\text{irr}(S)$ have the above form. Let $V = \{v \in \Sigma^* \mid uv \epsilon \text{irr}(S)\}$. Since $\text{irr}(S)$ is finite, we can calculate $V$. Let $l = \min\{|v| \mid v \epsilon V\}$. Since $A$ is strongly connected, $V \neq \emptyset$ and so $l$ is defined.
Clearly, $V \cap \Sigma^l \subseteq \text{geo}(\delta(S,ua), S)$. If $v \in \text{geo}(\delta(S,ua), S)$ then $|v| = l$ and by 4.1.1 we have $uav \in \text{irr}(S)$. Hence, $v \in V \cap \Sigma^l$ and so $\text{geo}(\delta(S,ua), S) \subseteq V \cap \Sigma^l$. We conclude that $\text{geo}(\delta(S,ua), S) = V \cap \Sigma^l$ which can easily be calculated from $V$. 

\[\square\]

In using the data $\text{irr}(S)$ and $\text{geo}(S)$ to represent $\mathcal{A}$, the most obvious way to represent a state $T$ is with a word $u \in \text{geo}(S, T)$. However, if $u_1 \in \text{geo}(S, P)$ and $u_2 \in \text{geo}(S, Q)$ for some states $P$ and $Q$, we'd like to check whether $\delta(S, u_1) = \delta(S, u_2)$. In particular, whether $P = Q$. Our first step toward this goal is

**Lemma 11.** Given $\text{geo}(S)$, $\text{irr}(S)$ and a finite subset $V \subseteq \Sigma^*$, we can decide if there exists a state $T$ such that $\text{geo}(T, S) = V$. If such a $T$ exists, we can effectively compute $u \in \text{geo}(S)$ such that $\delta(S, u) = T$.

**Proof.** By lemma 10, setting $a = \epsilon$ allows us to compute $\text{geo}(\delta(S, u), S)$ for each $u \in \text{geo}(S)$. Hence, the family of geodesic sets $\{\text{geo}(\delta(S, u))S \mid u \in \text{geo}(S)\}$ can be calculated. Since this family and each of its constituent sets is finite, we can decide if $V$ is lies in the family. If it does, we have found the desired state $T = \delta(S, u)$ where $u \in \text{geo}(S)$ satisfies $V = \text{geo}(\delta(S, u), S)$. Otherwise, no such $T$ exists. 

\[\square\]

We now apply our assumption that $\mathcal{A}$ is focal at $S$.

**Lemma 12.** Given $\text{irr}(S)$, $\text{geo}(S)$ and $u, v \in \text{geo}(S)$, we can decide if $\delta(S, u) = \delta(S, v)$.

**Proof.** For each state $T$, lemma 10 allows us to determine $\text{geo}(\delta(S, u), S)$ and $\text{geo}(\delta(S, v), S)$. Since $\mathcal{A}$ is focal at $S$, $\delta(S, u) = \delta(S, v)$ precisely when these two sets are equal. Since both sets are finite, this can be decided.

\[\square\]

Our goal shall be to “reduce” a word in $\Sigma^*$ to a geodesic. In other words, given $w \in \Sigma^*$ we seek $u \in \text{geo}(S)$ such that $\delta(S, w) = \delta(S, u)$. We are now in a position to take the first elementary step.

**Lemma 13.** Given $\text{geo}(S)$, $\text{irr}(S)$, $u \in \text{geo}(S)$ and $a \in \Sigma$ we can determine $x \in \text{geo}(S)$ such that $\delta(S, ua) = \delta(S, x)$.

**Proof.** Since $\mathcal{A}$ is stable at $S$, $\forall v \in \text{geo}(\delta(S, ua), S)$ : $uav \subseteq \text{irr}(S)$. Let $Y \subseteq \Sigma^*$ be given by $ua\Sigma^* \cap \text{irr}(S) = uaY$. Let $l = \min\{|v| \mid v \in Y\}$. We then have $\text{geo}(\delta(S, ua))S = Y \cap \Sigma^l$. Apply lemma 11 with $V = \text{geo}(\delta(S, ua), S)$ to obtain $x \in \text{geo}(S)$ such that $\text{geo}(\delta(S, u), S) = V$. 

\[\square\]
We now assemble all ingredients collected thus far. Given that $\mathcal{A}$ is focal and stable at $S$, our knowledge of $\text{irr}(S)$ and $\text{geo}(S)$ allows us to construct $\mathcal{A}$, or equivalently its transition function.

**Theorem 2.** Let $\mathcal{A}$ be a finite strongly connected automaton, focal and stable at some state $S$. Given $\text{irr}(S)$, $\text{geo}(S)$ and $x, y \in \Sigma^*$ we can decide whether $\delta(S, x) = \delta(S, y)$. Moreover, $\mathcal{A}$ is completely determined by the data $\{\text{irr}(S), \text{geo}(S)\}$.

**Proof.** For each $w \in \Sigma^*$, define $\theta(w) = \min\{l \in \mathbb{N} \mid \text{pref}(w) \cap \Sigma^l \in \text{geo}(S)\}$. We claim that for any $w \in \Sigma^*$, we can determine $z \in \Sigma^*$ such that $\delta(S, z) = \delta(S, w)$ and $\theta(z) < \theta(w)$. Fix $w \in \Sigma^*$. If $w \in \text{geo}(S)$, we are done. Otherwise, $\exists u, t \in \Sigma^*$ and $a \in \Sigma$ such that $w = uat$, $u \in \text{geo}(S)$ and $ua \not\in \text{geo}(S)$. Apply lemma 13 with to obtain $r \in \text{geo}(S)$ such that $\delta(S, ua) = \delta(S, r)$. Let $z = rt$. We then have $\delta(S, w) = \delta(S, uat) = \delta(S, rt) = \delta(S, z)$ and so $\theta(z) = \theta(rt) = |r| < |uat| = \theta(w)$ as required. This verifies the claim.

Apply the claim repeatedly to $x$, obtaining $x_1, \ldots, x_i \in \Sigma^*$ where $\theta(x) < \theta(x_1) < \ldots < \theta(x_i) = |x_i|$ and $\delta(S, x) = \delta(S, x_1) = \ldots = \delta(S, x_i)$. Since $\theta(x_i) = |x_i|$, $x_i \in \text{geo}(S)$. Similarly, obtain $y_1, \ldots, y_j \in \Sigma^*$ such that $\delta(S, y) = \delta(S, y_j)$ and $y_j \in \text{geo}(S)$. By lemma 12, we can decide whether $\delta(S, x_i) = \delta(S, y_j)$. Hence, we can decide whether $\delta(S, x) = \delta(S, y)$. \hfill \Box

We provide pseudocode for algorithms that realise each of the above statements.

Note: In our algorithms, if $L_1$ and $L_2$ are lists we write $L_1 = L_2$ to mean that the elements of $L_1$ are the same as the elements of $L_2$. In particular, $L_1 = L_2$ does not necessarily imply that the elements of $L_1$ and $L_2$ appear in the same order.

**Algorithm 1** Calculation of Irreducible Cycles

**Input:** $\{\text{cyc}(S)\}$

**Output:** $\text{irr}(S)$

```
I ← ∅
for w ∈ cyc(S) do
    maybeIrr ← true
    for x ∈ cyc(S) do
        if x ∈ pref(w) and x ≠ w then
            maybeIrr ← false
        end if
    end for
    if maybeIrr then
        I ← I ∪ {w}
    end if
end for
return I
```

4 Representation by Cycle Structure
Algorithm 2 Calculation of Return Geodesics

Input: \( \{\text{irr}(S), u, a\} \) where \( u \in \text{geo}(S) \), \( a \in \Sigma \cup \{\epsilon\} \).

Output: \( \text{geo}(\delta(S,ua),S) \).

\[
\begin{align*}
\text{started} & \leftarrow \text{false} \\
\text{for } w \in \text{irr}(S) \text{ do} & \\
\text{if } ua \in \text{pref}(w) \text{ then} & \\
& v \leftarrow \{\text{word such that } w = uav\} \\
& \text{if started then} \\
& \quad \text{if } |v| = \text{dist} \text{ then} \\
& \quad \quad V \leftarrow F \cup \{v\} \\
& \quad \text{else if } |v| < \text{dist} \text{ then} \\
& \quad \quad V \leftarrow [v] \\
& \quad \quad \text{dist} \leftarrow |v| \\
& \text{end if} \\
& \text{else if not started then} \\
& \quad \text{started} \leftarrow \text{true} \\
& \quad \text{dist} \leftarrow |v| \\
& \quad V \leftarrow [v] \\
& \text{end if} \\
\text{end if} \\
\text{end for} \\
\text{return } V
\end{align*}
\]

Algorithm 3 Calculation of Flat Cycles

Input: \( \{\text{irr}(S), \text{geo}(S)\} \)

Output: \( \text{flat}(S) \)

\[
\begin{align*}
F & \leftarrow \emptyset \\
\text{for } u \in \text{geo}(S) \text{ do} & \\
& V \leftarrow \text{Alg2}(\text{irr}(S), u, \epsilon) \\
& F \leftarrow F \cup uV \\
\text{end for} \\
\text{return } F
\end{align*}
\]

Algorithm 4 Calculation of a Leading Geodesic

Input: \( \{\text{geo}(S), \text{irr}(S), V\} \) where \( V \subseteq \Sigma^* \).

Output: \( u \in \text{geo}(S) \) such that \( \text{geo}(\delta(S,u),S) = V \), assuming such a \( u \) exists.

\[
\begin{align*}
\text{for } u \in \text{geo}(S) \text{ do} & \\
& W \leftarrow \text{Alg2}(\text{irr}(S), u, \epsilon) \\
& \text{if } V = W \text{ then} \\
& \quad \text{return } u \\
& \text{end if} \\
\text{end for} \\
\text{return } '\text{fail}'
\end{align*}
\]
Algorithm 5 Comparison of Geodesics

Input: $\{\text{flat}(S), \text{geo}(S), u, v\}$ where $u, v \in \text{geo}(S)$.
Output: true if $\delta(S, u) = \delta(S, v)$, false otherwise.

$U \leftarrow \emptyset$
$V \leftarrow \emptyset$
for $z \in \text{flat}(S)$ do
  if $u \in \text{pref}(z)$ then
    $U \leftarrow U \cup \{w\}$ \{where $z = uw$\}
  else if $v \in \text{pref}(z)$ then
    $V \leftarrow V \cup \{w\}$ \{where $z = vw$\}
  end if
end for
return $U = V$

Algorithm 6 Shortening to a Geodesic

Input: $\{\text{geo}(S), \text{irr}(S), u, a\}$ where $u \in \text{geo}(S)$, $a \in \Sigma$.
Output: $x \in \text{geo}(S)$ where $\delta(S, ua) = \delta(S, x)$.

$V \leftarrow \text{Alg2}(\text{irr}(S), u, a)$
$x \leftarrow \text{Alg4}(\text{geo}(S), \text{irr}(S), V)$
return $x$

4.2 Construction of Representable Automata

Proposition 5. Let $X \subseteq \Sigma^*$ such that $\forall c \in \Sigma$, $x \in X : c^2$ is not a subword of $x$. Then $\exists$ a SCDA $\mathcal{A}$ with a state $S$ at which $\mathcal{A}$ is focal and stable such that $\text{geo}(S) = \text{pref}(X)$.

Proof. Wlog we can assume $X = \text{pref}(X)$. Let $\mathcal{A}$ be the automaton with states $X$, initial state $S = \epsilon$ and transition function $\delta : X \times \Sigma \rightarrow X$ given by

$$\delta : (x, a) \mapsto \begin{cases} xa & \text{if } xa \in X \\ y & \text{if } x = yb, b \in \Sigma \\ x & \text{otherwise} \end{cases}$$

For each state $x \in X$, $\text{geo}(x, S) = \{u \in \text{geo}(x) \mid \delta(x, u) = S\} = \{x^R\}$ where $x^R$ is the reverse of the word $x$. Hence, $\mathcal{A}$ is focal at $S$. Similarly, for each $x \in X$ we have $\text{geo}(S, x) = \{x\}$ and so $\Delta(S, x) = \Delta(x, S) = |x|$ for all $x \in X$. Applying lemma 9, we conclude that $\mathcal{A}$ is stable at $S$. Finally, any state $x \in X$ has precisely one path leading to it: the word $x$ itself. Such a path is a geodesic and so $\text{geo}(S) = X$. \qed

26
Figure 4.2.1: The automaton from prop. 5 with $\Sigma = \{a, b, c\}$ and $X = \{ab, ac, bab\}$. 
5 Permutation Automata

“... things which appear to us the same do not always behave in the same manner, and ... things which appear different to us sometimes prove in all other respects to behave the same way ... and it proceeds from this experience to ... [group] together not what appears alike but what proves to behave in the same manner in similar circumstances.”

∼ Studies on the Abuse and Decline of Reason, Hayek and Caldwell

Let \( A \) be an SCDA with states \( \Omega \), initial state \( S \) and transition function \( \delta \). Assume \( \Omega \) is finite. For each \( w \in \Sigma^* \), let \( \chi_w : \Omega \rightarrow \Omega \) denote the corresponding map in the transition monoid of \( A \). In other words, \( \chi_w : T \mapsto \delta(T, w) \). In the case \( \chi_w \) is a permutation for all \( w \in \Sigma^* \), we call \( A \) a permutation automaton. Equivalently, a permutation automaton is a finitely generated group for which a finite set of generators has been fixed.

**Proposition 6.** If \( A \) is a permutation automaton then for all states \( P \) and \( Q \) we have \( \text{cyc}(P) = \text{cyc}(Q) \), \( \text{irr}(P) = \text{irr}(Q) \), \( \text{rig}(P) = \text{rig}(Q) \), \( \text{flat}(P) = \text{flat}(Q) \) and \( \text{geo}(P) = \text{geo}(Q) \).

**Proof.** All the proofs here are similar and straightforward. They follow from the fact a path in the Cayley graph \( \Gamma_G \) of the group \( G \) corresponding to \( A \) can be translated around the graph to any vertex. The image of the path under translation is isometric to the original path. For instance, if \( w \in \text{cyc}(P) \) then there is a group element that translates the corresponding path (closed cycle) to the state (or vertex) \( Q \). The closed path based at \( Q \) will be labelled by \( w \) and hence \( w \in \text{cyc}(S) \).

\[ \Box \]

From the beginning, we’ve regarded cycle sets as defining “relators” of a SCDA. A natural question is, given a state \( S \) of \( A \), do we have a group presentation of the transition monoid \( \text{char}(A) \) given by \( \langle \Sigma \mid \text{cyc}(S) \rangle \)? It turns out the answer is yes. In fact, a slightly stronger statement is true.

**Proposition 7.** If \( A \) is a finite permutation automaton then \( \text{char}(A) \cong \langle \Sigma \mid \text{rig}(S) \rangle \) as groups.

**Proof.** \( \cup_{a \in \Sigma} \chi_a \) is a generating set for \( G = \text{char}(A) \) and so we have a group presentation \( \text{char}(A) \cong \langle \cup_{a \in \Sigma} \chi_a \mid \mathcal{R} \rangle \) for some finite \( \mathcal{R} \subseteq (\cup_{a \in \Sigma} \chi_a)^* \). With the identifications
\[ \chi_{a_1} \cdots \chi_{a_p} \leftrightarrow a_1 \cdots a_p \] we see that \( \text{char}(\mathcal{A}) \cong \langle \Sigma \mid R \rangle \) for some finite \( R \subseteq \Sigma^* \). Fix \( r \in R \).

For each \( w \in \Sigma^* \), define

\[ \Omega_w = \{ (\bar{u}, u) \in \Sigma^* \mid \bar{u} \in \text{pref}(u) \setminus \{u\}, u \in \text{pref}(w) \setminus \{r\}, \delta(S, \bar{u}) = \delta(S, u) \} \]

If \( \Omega_r = \emptyset \), then \( \forall \bar{u}, u \in \text{pref}(r) : \delta(S, \bar{u}) \neq \delta(S, u) \) which implies \( r \in \text{rig}(\mathcal{S}) \) and so we are done. Otherwise, choose \((\bar{u}, u) \in \Omega_r\). Now, \( \exists \bar{v}, v \in \Sigma^* \) such that \( u = \bar{u} \bar{v} \) and \( r = uv \). Also, \( \delta(S, \bar{u}) = \delta(S, u) \) and so \( \bar{v} = 1_G \). It follows that \( \text{char}(\mathcal{A}) \cong \langle \Sigma \mid \{r\} \rangle \cup \{uv, \bar{v}\} \) as groups. We see that \( r \) can be replaced with the relations \( \bar{u}v \) and \( \bar{v} \) where \( |\Omega_{\bar{u}v}| < |\Omega_r| \) and \( |\Omega_{\bar{v}}| = 0 \). Continuing this process, we can find a collection of relations \( \bar{R} \) such that \( \text{char}(\mathcal{A}) \cong \langle \Sigma \mid \bar{R} \rangle \) and \( \forall r \in \bar{R} : \Omega_r = \emptyset \). That is, \( \bar{R} \subseteq \text{rig}(\mathcal{S}) \).

The requirement that our automata be focal and stable was important in chapter 4.

What can we say about the focality and stability of a permutation automaton?

**Proposition 8.** Let \( \mathcal{A} \) be a permutation automaton. Then \( \mathcal{A} \) is focal and stable at every state.

**Proof.** The collection of state maps \( G = \{ \rho_w \mid w \in \Sigma^* \} \) given by \( \rho_w : T \mapsto \delta(T, w) \) forms a group under composition. That is, if \( \rho_u, \rho_v \in G \) then \( \rho_u \rho_v : T \mapsto \delta(\delta(T, u), v) = \delta(T, uv) \).

In this setting if we fix a state \( S \) of \( \mathcal{A} \) and let \( d_G : G \times G \to \mathbb{N} \) denote the word metric on \( G \) then \( \Delta(\delta(S, u), \delta(S, v)) = d_G(\rho_u, \rho_v) \) for all \( \rho_u, \rho_v \in G \). Hence, \( \Delta \) is a metric when \( \mathcal{A} \) is a permutation automaton. We can apply lemma 9 to conclude that \( \mathcal{A} \) is stable at any such \( S \) and so is stable at every state.

Fix \( u, v \in \Sigma^* \) such that \( \rho_u \neq \rho_v \). That is, choose some arbitrary distinct elements of \( G \). Fix \( \rho_w \in G \). Then if \( \rho_x \in G \) is the element such that \( \rho_u \rho_x = \rho_w \) we have \( \rho_v \rho_x \neq \rho_w \) in view of the existence of \( (\rho_u)^{-1} \in G \). Hence, if \( \delta(S, ux) = \delta(S, w) \) then \( \delta(S, ux) \neq \delta(S, vx) \) and so in the case of geodesics we have

\[ \text{geo}(\delta(S, u), \delta(S, x)) \cap \text{geo}(\delta(S, v), \delta(S, x)) = \emptyset \]

Thus, for all states \( T_1, T_2 \) and \( T_3 \) of \( \mathcal{A} \) we have \( \text{geo}(T_1, T_2) \cap \text{geo}(T_2, T_3) = \emptyset \). Since both sets are always non-empty, we have \( T_1 = T_2 \iff \text{geo}(T_1, T_3) = \text{geo}(T_2, T_3) \) and so \( \mathcal{A} \) is focal at any such state \( T_3 \). Hence, \( \mathcal{A} \) is focal at every state.
6 Strongly Connected Languages

“wherever you go, you must be able to get back. If you go from A to B, you need to be able to get back from B to A. You don’t need to do the same ‘move’, but just get back.”

∼ David Belle, founder and practitioner of l’art du déplacement.

So far we have focussed exclusively on automata. As noted in chapter 2, there is a family of languages $L_A$ associate with each automaton $A$. Namely, a language is associated to each choice of states. We shall investigate $L_A$ in the case where $A$ is an SCDA.

Let $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$. With each language $L \subseteq \Sigma^*$, we associate the Myhill-Nerode equivalence relation $\sim_L$ on $\Sigma^*$ given by

$$u \sim_L v \text{ if } \forall w \in \Sigma^* : uw \in L \iff vw \in L.$$ 

The relation $\sim_L$ gives rise to an automaton which accepts $L$. Let $\mathcal{M}(L)$ be the automaton with states the equivalence classes $\Sigma^*/\sim_L$, initial state $[\epsilon]$, accept states $\{[w] \mid w \in L\}$ and transition function $\delta : (\Sigma^*/\sim_L) \times \Sigma \to (\Sigma^*/\sim_L)$ given by $([w], c) \mapsto [wc]$.

A language $L \subseteq \Sigma^*$ is called complete if for all $u \in \Sigma^*$ there exists $v \in \Sigma^*$ such that $uv \in L$. When $L$ satisfies the condition

$$\forall u \in \Sigma^* \exists v \in \Sigma^* : uv\Sigma^* \cap L = uvL$$

we say $L$ is strongly connected. Note that the definitions of complete and strongly connected depend on a choice of alphabet $\Sigma$. If $L$ is complete (or strongly connected) with respect to an alphabet $\Sigma_1$, $L$ need not be complete (or strongly connected) w.r.t another alphabet $\Sigma_2$.

**Example 2.** The language $L_1 = \{a^p \mid p \in \mathbb{N}, p \text{ is prime}\}$ over $\Sigma = \{a\}$ is complete but not strongly connected.
6 Strongly Connected Languages

6.1 Basic language properties

As we’ll soon see, the classes of complete and strongly connected languages are deeply related.

Proposition 9. Let $L \subseteq \Sigma^*$. The following are equivalent

1. $L$ is complete
2. $\text{pref}(L) = \Sigma^*$
3. $\forall w \in \Sigma^*: w\Sigma^* \cap L \neq \emptyset$

Proof. Assume (1). Take $u \in \Sigma^*$. Then $\exists v \in \Sigma^*$ such that $uv \in L$ and so $u \in \text{pref}(L)$. Hence, $\text{pref}(L) \supseteq \Sigma^*$ and so the other inclusion is obvious and so $\text{pref}(L) = \Sigma^*$. Assume (2). Take $w \in \Sigma^*$. Then $w \in \text{pref}(L)$ and so $\exists u \in \Sigma^*: uw \in L$. That is, $w \Sigma^* \cap L \neq \emptyset$. Assume (3). Take $u \in \Sigma^*$. Then $u \Sigma^* \cap L \neq \emptyset$ and so $\exists w \in u \Sigma^* \cap L$. Namely, $w = uv$ for some $v \in \Sigma^*$. Since $w \in u \Sigma^* \cap L \subseteq L$, we have $uv \in L$.

The automata and language theoretic definitions for “strongly connected” coincide as well as could be hoped for.

Proposition 10. Let $L \subseteq \Sigma^*$. Then $L$ is strongly connected if and only if $\mathcal{M}(L)$ is strongly connected.

Proof. Fix a state $[u]$ of $\mathcal{M}(L)$ where $u \in \Sigma^*$. When $L$ is strongly connected, $\exists v \in \Sigma^*$ such that $uv \Sigma^* \cap L = uvL$. That is, $\forall w \in \Sigma^*: uw \in L \iff w \in L$ and so $uv \sim_L \epsilon$. Hence, $\delta(T, v) = \delta([u], v) = [uv] = [\epsilon]$. Since $\mathcal{M}(L)$ is initially connected, this shows it is strongly connected. Conversely, suppose $\mathcal{M}(L)$ is strongly connected. Then for all states $[u]$ of $\mathcal{M}(L)$ there exists $v \in \Sigma^*$ such that $\delta([u], v) = [\epsilon]$. That is, $[uv] = [\epsilon]$ and so $uv \sim_L \epsilon$. For any $w \in \Sigma^*$ we then have $uvw \in L \iff w \in L$. In other words, $uv \Sigma^* \cap L = uvL$. Since such a $v$ exists for any $u \in \Sigma^*$, $L$ is strongly connected.

If we disregard the empty language, then there is a strict containment of these language classes.

Proposition 11. If $L \subseteq \Sigma^*$ is strongly connected and $L \neq \emptyset$ then $L$ is complete.

Proof. Take $u \in \Sigma^*$. By assumption, $\exists \bar{v} \in \Sigma^*$ such that $u \bar{v} \Sigma^* \cap L = u \bar{v}L$. Since $L \neq \emptyset$, $\exists w \in L$. Then $u \bar{v}w \in u \bar{v}L = u \bar{v} \Sigma^* \cap L \subseteq L$. Setting $v = \bar{v}w$ gives us $uv \in L$.

With any complete language, we can naturally associate a strongly connected language.
Proposition 12. If \( L \subseteq \Sigma^* \) is complete then \( L^* \) is strongly connected.

Proof. Take \( u \in \Sigma^* \). By assumption, \( \exists v \in \Sigma^* \) such that \( uv \in L \). Hence, \( uvL^* \subseteq LL^* \subseteq L^* \). Clearly, \( uvL^* \subseteq w\Sigma^* \) also and so \( uvL^* \subseteq w\Sigma^* \cap L^* \). On the other hand, if \( x \in w\Sigma^* \cap L^* \) then \( \exists w \in \Sigma^* \) such that \( x = uwv \). Since \( uww \in L^* \) and \( uv \in L \) we have \( w \in L^* \). Hence, \( x = uww \in uvL^* \) which implies \( w\Sigma^* \cap L^* \subseteq uvL^* \). Together, these containments imply \( w\Sigma^* \cap L^* = uvL^* \) and so \( L^* \) is strongly connected.

Example 3. Consider the languages \( L_3 = \{ a^{2n} \mid n \in \mathbb{N} \} \) and \( L_4 = \{ a^{2n+1} \mid n \in \mathbb{N} \} \) over \( \Sigma = \{ a \} \). \( L_3 \) and \( L_4 \) are both complete but \( L_3 \cap L_4 = \emptyset \) is not. Hence, the class of complete languages is not closed under intersection.

However, we see that complete languages are closed under the familiar operations of union, Kleene star and concatenation.

Proposition 13. If \( P, Q \subseteq \Sigma^* \) are complete then \( P \cup Q, P^* \) and \( PQ \) are complete.

Proof. Take \( u \in \Sigma^* \). Since \( P \) is complete, \( \exists v \in \Sigma^* \) such that \( uv \in P \subseteq P \cup Q \). Additionally, since \( P \subseteq P^* \) we have \( uv \in P^* \). Now, \( uv \in \Sigma^* \) and since \( Q \) is complete \( \exists w \in \Sigma^* \) such that \( uww \in Q \). Hence, given \( u \in \Sigma^* \) we find \( x = vw \in \Sigma^* \) for which \( ux \in PQ \). This shows that each language is complete.

Note if \( L \subseteq \Sigma^* \) is complete then the complement \( \Sigma^* \setminus L \) need not be complete. For instance, if \( F \subseteq \Sigma^* \) is finite and \( L = \Sigma^* \setminus F \) then \( \Sigma^* \setminus L = F \) is not complete.

The closure properties of strongly connected languages are more involved. To settle them, we turn to a deep result in graph theory.

Theorem 3. (see [2], [7])

Let \( \Gamma_1 \) and \( \Gamma_2 \) be (finite or infinite) strongly connected directed graphs. Then every connected component in the tensor (or Kronecker) product \( \Gamma_1 \otimes \Gamma_2 \) is strongly connected.

Theorem 4. Let \( R, T \subseteq \Sigma^* \) be strongly connected. Then \( R \cup T, R \cap T, \Sigma^* \setminus R, \) and \( RT \) are strongly connected. If \( \epsilon \in R \) then \( R^* \) is also strongly connected.

Proof. Let \( \mathcal{A}_1 \) be a DFA for \( R \) and \( \mathcal{A}_2 \) a DFA for \( T \). Let \( \Omega_1, S_1, F_1 \) and \( \delta_1 \) be the states, initial state, accept states and transition functions (resp.) of \( \mathcal{A}_i \) for \( i \in \{ 1, 2 \} \). Construct an automaton \( \mathcal{A} \) with states \( \Omega_1 \times \Omega_2 \), initial state \( (S_1, S_2) \), accept states \( F \subseteq F_1 \times F_2 \) and transition function \( \delta : (\Omega_1 \times \Omega_2) \times \Sigma \rightarrow \Omega_1 \times \Omega_2 \) given by

\[
\delta : ((P, Q), a) \mapsto (\delta_1(P, a), \delta_2(Q, a))
\]
Since $R$ and $T$ are strongly connected, the transition graphs for $\mathcal{A}_1$ and $\mathcal{A}_2$ are strongly connected. The transition graph of $\tilde{\mathcal{A}}$ is precisely the tensor product of the transition graphs of $\mathcal{A}_1$ and $\mathcal{A}_2$. By theorem 3, the component of $\tilde{\mathcal{A}}$ containing $(S_1, S_2)$ is strongly connected. Let $\mathcal{A}$ be the minimal DFA obtained from $\tilde{\mathcal{A}}$. It can easily be shown that $\mathcal{A}$ is strongly connected. If we set $\mathcal{F} = \mathcal{F}_1 \times \Omega_2 \cup \Omega_1 \times \mathcal{F}_2$ then $\mathcal{L}(\mathcal{A}) = R \cup T$. Otherwise, if we set $\mathcal{F} = \mathcal{F}_1 \times \mathcal{F}_2$ then $\mathcal{L}(\mathcal{A}) = R \cap T$. Hence we have that both $R \cup T$ and $R \cap T$ are strongly connected.

To see that $R^*$ is strongly connected, note that $R$ is complete by proposition 11. By proposition 13, $R^*$ is complete and so by proposition 12 we have that $R^*$ is strongly connected.
6.2 Metric Properties

There is an obvious way of regarding $\Sigma^*$ as a metric space. For each $u, v \in \Sigma^*$, let $M_{u,v}$ be the length of the longest common prefix of $u$ and $v$. In other words, $M_{u,v}$ is the number

$$\max \{ |w| \mid w \in \text{pref}(u) \cap \text{pref}(v) \}$$

Define a map $d : \Sigma^* \times \Sigma^* \to \mathbb{N}$ by $(u, v) \mapsto |u| + |v| - 2M_{u,v}$.

**Proposition 14.** $d$ is a metric on $\Sigma^*$.

*Proof.* Take $u, v, w \in \Sigma^*$. We have $d(u, u) = |u| + |u| - 2M_{u,u} = 2|u| - 2M_{u,u}$. Since $M_{u,u} = |u|$ we have $d(u, u) = 0$. The fact $d(u, v) = d(v, u)$ is clear from the definition of $d$. We have $M_{u,v} \leq \min\{|u|, |v|\}$ and so $d(u, v) \geq |u| + |v| - 2 \min\{|u|, |v|\}$. Since $|u| + |v| \geq 2 \min\{|u|, |v|\}$ we conclude $d(u, v) \geq 0$.

For the triangle inequality, let $x \in \Sigma^*$ be the longest word in pref$(u) \cap$ pref$(v) \cap$ pref$(w)$. Then $\exists \bar{u}, \bar{v}, \bar{w} \in \Sigma^*$ such that $u = x\bar{u}$, $v = x\bar{v}$ and $w = x\bar{w}$. It’s clear that $d(u, v) = d(\bar{u}, \bar{v})$, $d(u, w) = d(\bar{u}, \bar{w})$ and $d(v, w) = d(\bar{v}, \bar{w})$. Hence, wlog we’ll assume pref$(u) \cap$ pref$(v) \cap$ pref$(w) = \emptyset$. Also, since the $u, v, w$ were chosen symmetrically and $d$ is symmetric in its arguments, it suffices to consider the case pref$(u) \cap$ pref$(v) = \text{pref}(v) \cap$ pref$(w) = \emptyset$. Let $y \in \Sigma^*$ be such that $u = yu'$, $v = yv'$ and $|y| = M_{u,v}$. We have that $e$ lies on the unique geodesic(s) from $u$ to $w$ and $v$ to $w$. Hence, $d(u, w) = d(u, e) + d(e, w) = |u| + |w|$ and $d(v, w) = |v| + |w|$ similarly. Now,

$$d(u, v) + d(v, w) = (|u| + |v| - 2M_{u,v}) + |v| + |w| = (|u| + |w|) + 2(|v| - M_{u,v})$$

Clearly, $|v| \geq M_{u,v}$ and thus $2|v| - 2M_{u,v} \geq 0$ from which we conclude that $d(u, w) \leq d(u, v) + d(v, w)$.

\[\square\]

A language $L \subseteq \Sigma^*$ is called **cobounded** if there exists $k \geq 0$ such that

$$\forall u \in \Sigma^* \exists v \in L : d(u, v) \leq k$$

Note that this agrees with our notion of a cobounded subset of a general metric space. If we restrict ourselves to regular languages, completeness has a very satisfying characterisation.

**Proposition 15.** Let $R \subseteq \Sigma^*$ be regular. Then $R$ is complete if and only if it is cobounded.

*Proof.* Suppose $R$ is regular and complete. Let $k$ be the constant given by lemma 24. Fix $u \in \Sigma^*$. We claim that $d(u, R) \leq k$. Since $R$ is complete, $\exists v \in \Sigma^*$ such that $uv \in R$. [34]
If \(|v| \leq k\), we are done. Otherwise, we can write \(uv = xyz\) with \(x, y, z \in \Sigma^*, |y| \geq 1, |yz| \leq k\) and \(\forall i \in N : xy^iz \in R\). Hence, \(xz \in R\). Now, \(|yz| \leq k\) and \(|v| > k\) together imply \(yz \in \text{suff}(v)\). Hence, \(\exists w \in \Sigma^*\) such that \(v = wyz\) and \(x = uw\). Since \(xz \in R\) we have \(uwz \in R\) where \(|wz| < |wyz| = |u|\) as \(|y| > 1\). We conclude that \(d(u, R) \leq |v| - 1\). This shows that if \(uv \in R\) and \(|v| > k\), we can always find a shorter word \(\bar{v}\) with \(|\bar{v}| < |v|\) such that \(\bar{v} \in R\). It follows that \(d(u, R) \leq k\) and hence \(R\) is cobounded.

Conversely, suppose \(R\) is cobounded. Let \(k\) be the associated constant. Fix \(u \in \Sigma^*\). If \(u \Sigma^* \cap R = \emptyset\) then we can find \(w \in \Sigma^*\) so that \(d(w, R)\) is arbitrarily large. This would contradict \(R\) cobounded. Hence, \(u \Sigma^* \cap R\) is non-empty. Say, \(x \in u \Sigma^* \cap R\) for which we can find \(v \in \Sigma^*\) such that \(x = uv\). We conclude \(uv \in u \Sigma^* \cap R \subseteq R\) and so \(R\) is complete.

\[\square\]

**Example 4.** The language \(L_1\) defined earlier is complete but not cobounded. Hence, it is not regular.

**Example 5.** The language \(L_2\) = \(\{w \in \{a, b\}^* \mid |w|_a = |w|_b\}\) is complete (in fact, strongly connected!) but not cobounded. Hence, it is not regular. This also demonstrates theorem 15 is false for context-free languages.

Our goal shall be to develop a theory of so-called “ends” for \((\Sigma^*, d)\). Instead of the usual definition of and end in a metric space (for instance, see [8]), we adopt another definition better tailored to working with \((\Sigma^*, d)\). Our definition will correspond to the classical one in the context of \((\Sigma^*, d)\). Roughly speaking, we’ll show that a language is complete if and only if its ends occupy all of \((\Sigma^*, d)\). We’ll give a similar statement regarding strongly connected languages, although sadly it must be left as a conjecture.

Let \((X, d)\) be a metric space. If \(k \in \mathbb{N}\) then \((X, d)\) is called \textbf{k-steppable} if for all \(x, \bar{x} \in X\) there exists \(x_1, \ldots, x_p \in X\) such that \(x = x_1, \bar{x} = x_p\) and

\[
\forall i \in \{1, \ldots, p - 1\} : d(x_i, x_{i+1}) \leq k
\]

We start with a sequence of technical lemmas.

**Lemma 14.** If \(L \subseteq \Sigma^*\) is complete, \(k\)-steppable for some \(k \in \mathbb{N}\) and \(|\Sigma| \geq 2\) then \(B_k(\epsilon) \cap L \neq \emptyset\).

**Proof.** Consider the ball \(B_k(\epsilon) \subseteq L\). Now, \(\exists x,y \in B_k(\epsilon)\) such that \(d(x,y) = 2k\). For instance, take \(a^k\) and \(b^k\) where \(a, b \in \Sigma\) with \(a \neq b\). Since \(L\) is complete, \(\exists x, y \in \Sigma^*\) such that \(x\bar{x}, y\bar{y} \in L\). Since \(L\) is \(k\)-steppable, \(\exists w_1, \ldots, w_n \in L\) such that \(w_1 = x\bar{x}, w_n = y\bar{y}\) and

\[
\forall i \in \{1, \ldots, n - 1\} : d(w_i, w_{i+1}) \leq k
\]

The empty word \(\epsilon \in \Sigma^*\) lies on the (unique) geodesic from \(w_1\) to \(w_n\). It follows that some \(i \in \{1, \ldots, n\}\) must satisfy \(d(w_i, \epsilon) \leq k\).\(^1\) We thus have \(w_i \in B_k(\epsilon)\).

\[\square\]

\(^1\)In fact, \(d(w_i, \epsilon) \leq \frac{k}{2}\) holds but we won’t need this.
Lemma 15. If \( L \subseteq \Sigma^* \) is complete and \( k \)-steppable for some \( k \in \mathbb{N} \) with \( |\Sigma| \geq 2 \) then \( \exists K \in \mathbb{N} \) such that \( \forall u \in \Sigma^* \exists v \in \Sigma^* : uv \in L \wedge |v| \leq K \).

Proof. Apply lemma 14 to obtain \( w \in L \) such that \( d(\epsilon, u) \leq k \). Fix \( u \in \Sigma^* \). Since \( L \) is complete, \( \exists u \in \Sigma^* \) such that \( uv \in L \). As \( L \) is \( k \)-steppable, \( \exists w_1, \ldots, w_n \in L \) such that \( w_1 = w \) and \( w_n = uvu \) such that

\[
\forall i \in \{1, \ldots, n-1\} : d(w_i, w_{i+1}) \leq k
\]

Now, \( u \) lies on the (unique) geodesic from \( w_1 \) to \( w_n \) and so \( \exists i \in \{1, \ldots, n\} \) such that \( u \in \text{pref}(w_i) \) and \( d(u, w_i) \leq k \). We have \( w_i = uv \) for some \( v \in \Sigma^* \). Such a \( v \) satisfies \( uv \in L \) and \( |v| \leq K \).

As the next examples show, the property of a language being \( k \)-steppable for some \( k \) is independent of the property of being complete.

Example 6. The language \( L_5 \) over \( \Sigma = \{a\} \) given by \( L_5 = \{a^{n^2} \mid n \in \mathbb{N}\} \) is complete. However, for all \( k \in \mathbb{N} \), \( L \) is not \( k \)-steppable.

Example 7. Any finite language \( L \) over some alphabet \( \Sigma \) is \( k \)-steppable but not complete.

For any metric space \((X, d)\), let \( k^X \) be the minimal \( k \) for which \((X, d)\) is \( k \)-steppable. For each \( k \in \mathbb{N} \), \( \#_k(X) \) is the number of \( k \)-steppable components of \( X \). For \((X, d)\) \( k \)-steppable, \( Y \subseteq X \) is called an end set of \( X \) if

\[
\forall y \in Y \exists N \in \mathbb{N} \forall n \geq N : \#_k(Y \setminus B_n(y)) = 1
\]

Let \( E_X \) denote the collection of end sets of \( X \). Define an equivalence relation \( \sim \) on \( E_X \) by setting \( X_1 \sim X_2 \) if \( \exists m \in \mathbb{N} : X_1 \subseteq B_m(X_2) \). Each element of \( E_X \) is called an end of \( X \). Consider a subset \( Y \subseteq X \). For any end \( \mathcal{E} \in E_X \), we write \( Y \subseteq \mathcal{E} \) if there exists an end set \( X \) of \( \mathcal{E} \) such that \( Y \subseteq X \). Similarly, we let \( Y \cap \mathcal{E} \) denote the union of all \( Y \cap X \) where \( X \) is an end set of \( \mathcal{E} \).

For each map \( f : \mathbb{N} \to \Sigma \) let \( \mathcal{E}_f \) be the end containing the end set

\[
S_f = \bigcup_{m \in \mathbb{N}} \prod_{l=1}^m f(l) = \bigcup_{m \in \mathbb{N}} f(1) \cdots f(m) = \{e, f(1), f(1)f(2), \ldots\}
\]

If \( X \) is an endset, we let \([X]\) denote the end containing \( X \). For instance, we have \( \mathcal{E}_f = [S_f] \) for each \( f : \mathbb{N} \to \Sigma \).

Lemma 16. For each end set \( Y \) of \((\Sigma^*, d)\) there exists a unique \( f : \mathbb{N} \to \Sigma \) such that \( S_f \cap Y \) is infinite. Further, there is a constant \( p \in \mathbb{N} \) such that for all \( g : \mathbb{N} \to \Sigma \) we have \( f = g \) or \( S_g \cap Y \subseteq B_p(\epsilon) \).
Proof. Firstly, suppose that for all \( f : \mathbb{N} \to \Sigma \), \( S_f \cap Y \) is finite. For each \( f \) we have \( S_f \cap Y \subseteq B_p(\epsilon) \) for some \( p \in \mathbb{N} \). From the tree structure of \((\Sigma^*, d)\), it follows that each \( S_f \cap Y \) is \( k^Y \)-steppable. If there is no uniform bound on the \( p \) as \( f \) varies then \( Y \) has at \( k^Y \)-steppable components lying an arbitrarily large distance apart. Hence, \( Y \) is not \( k \)-steppable for any \( k \). A contradiction and thus at least one such \( f \) must exist.

Instead, suppose there exist \( f : \mathbb{N} \to \Sigma \) and \( g : \mathbb{N} \to \Sigma \) with \( f \neq g \) such that \( S_f \cap Y \) and \( S_g \cap Y \) are both infinite. Like above, we note that \( S_f \cap Y \) and \( S_g \cap Y \) are \( k^Y \)-steppable. Choose \( i \in \mathbb{N} \) such that \( d(f(i), g(i)) > k \). Let \( y = f(i) \) and \( N = d(f(i), g(i)) \). Since \( Y \) is an end set, \( \exists m \geq N \) such that

\[
\#_{k^Y}(Y \setminus B_m(y)) = 1 \tag{6.2.1}
\]

But then \((Y \setminus B_m(y)) \cap S_f \) and \((Y \setminus B_m(y)) \cap S_g \) are infinite \( k^Y \)-steppable components of distance at least \( m \) apart where \( m \geq d(f(i), g(i)) > k \). This contradicts 6.2.1. Hence, at most one such map \( f \) can have \( S_f \cap Y \) infinite.

And now for the first punchline: the end sets \( \{S_f\} \) form a complete set of representatives for the ends of \((\Sigma^*, d)\).

**Lemma 17.** For each end \( E \) of \((\Sigma^*, d)\) there exists \( f : \mathbb{N} \to \Sigma \) such that \( E = E_f \).

**Proof.** Let \( E \) be an end of \((\Sigma^*, d)\). Fix an end set \( Y \) of \( E \). By lemma 16, \( \exists p \in \mathbb{N} \) and \( f : \mathbb{N} \to \Sigma \) such that for all maps \( g : \mathbb{N} \to \Sigma \) we have either \( f = g \) or \( S_g \cap Y \subseteq B_p(\epsilon) \). Obviously,

\[
Y = \bigcup_{g : \mathbb{N} \to \Sigma} S_g \cap Y \\
= \left( \bigcup_{\substack{g : \mathbb{N} \to \Sigma \ \mid \ g \neq f}} S_g \cap Y \right) \cup S_f \\
\subseteq B_p(\epsilon) \cup S_f
\]

But \( B_p(\epsilon) \cup S_f \sim S_f \) and \( Y \sim B_p(S_f) \). Hence, \( Y \sim S_f \) and hence \( E = E_f \).

**Lemma 18.** Let \( Z \) be an end set of a metric space \((X, d)\) and \( Y \subseteq Z \). If we set \( k = k^Y \) then for each \( y \in Y \) there exists \( n \in \mathbb{N} \) such that

\[
\#_k(Y \setminus B_n(y)) \in \{0, 1\}
\]

Moreover, for such an \( n \) and \( m \geq n \) we have

\[
\#_k(Y \setminus B_m(y)) = \#_k(Y \setminus B_n(y))
\]
6 Strongly Connected Languages

Proof. Apply lemma 17 to obtain \( f : \mathbb{N} \to \Sigma \) such that \( Z = \mathcal{E}_f \). Now, \( \exists p \in \mathbb{N} \) such that \( Z \subseteq B_p(\mathcal{S}_f) \) and so \( \exists n \in \mathbb{N} \) such that \( d(f(1) \ldots f(n), y) \leq p \). We have that \( d(y, \epsilon) \leq p + n \) and

\[
\#_k(Y \setminus B_{p+n}(y)) = \begin{cases} 
1 & \text{if } Y \text{ infinite,} \\
0 & \text{if } Y \text{ finite.} 
\end{cases}
\]

\( \square \)

Lemma 19. If \( \mathcal{E} \) is an end and \( Y \subseteq \mathcal{E} \) a subset then for all \( k \in \mathbb{N} \) we have \( B_k(Y) \subseteq \mathcal{E} \).

Proof. Let \( \mathcal{E} \) be an end of \( (\Sigma^*, d) \) and \( Y \subseteq \mathcal{E} \). Let \( k = k^Y \). If \( Y \) is an end set of \( \mathcal{E} \) then trivially \( B_k(Y) \sim Y \) and thus \( B_k(Y) \) is an end set of \( \mathcal{E} \). Hence, \( B_k(Y) \subseteq \mathcal{E} \).

Otherwise, \( Y \) is not an end set of \( \mathcal{E} \) and so

\[ \exists y \in Y \forall N \in \mathbb{N} \exists n \geq N : \#_k(Y \setminus B_n(y)) \neq 1 \]

By lemma 18, the fact that \( \#_k(Y \setminus B_n(y)) \neq 1 \) for arbitrarily large \( n \) implies that \( \#_k(Y \setminus B_m(y)) \neq 0 \) for some \( m \in \mathbb{N} \). Hence, \( \exists y \in Y \) and \( m \in \mathbb{N} \) such that \( \#_k(Y \setminus B_m(y)) = 0 \) and thus \( Y \setminus B_m(Y) = \emptyset \). We conclude that \( Y \subseteq B_m(y) \subseteq B_m(Y) \subseteq \mathcal{E} \).

\( \square \)

Theorem 5. Let \( L \subseteq \Sigma^* \) be \( k \)-steppable for some \( k \in \mathbb{N} \). Then \( L \) is complete if and only if for all ends \( \mathcal{E} \) of \( (\Sigma^*, d) \), \( L \cap \mathcal{E} \) is an end of \( (\Sigma^*, d) \). Moreover, we have \( L \cap \mathcal{E} = \mathcal{E} \) in this case.

Proof. Suppose \( L \subseteq \Sigma^* \) is complete and \( k \)-steppable for some \( k \in \mathbb{N} \). Fix an end \( \mathcal{E} \) of \( (\Sigma^*, d) \). By lemma 17, \( \exists f : \mathbb{N} \to \Sigma \) such that \( \mathcal{E} = \mathcal{E}_f \). We claim that \( L \cap \mathcal{E}_f \) is an end of \( (\Sigma^*, d) \). If \( |\Sigma| = 1 \) then \( (\Sigma^*, d) \) has precisely one end and the result is clear. Hence, we can assume \( |\Sigma| \geq 2 \). Fix \( K \in \mathbb{N} \) as described in lemma 15. For each \( m \in \mathbb{N} \), let \( u_m = \prod_{i=1}^m f(l) \) and fix \( v_m \in \Sigma^* \) such that \( u_m v_m \in L \) and \( |v_m| \leq K \). Now, \( \cup_{m \in \mathbb{N}} B_k(u_m) \subseteq \mathcal{E} \) by lemma 19 and \( \cup_{m \in \mathbb{N}} u_m v_m \subseteq L \) from our choice of the \( v_m \). Since \( \cup_{m \in \mathbb{N}} u_m v_m \subseteq \cup B_k(u_m) \subseteq \mathcal{E} \cap L \) we conclude \( \cup_{m \in \mathbb{N}} u_m v_m \subseteq \mathcal{E} \cap L \). Since \( |v_m| \leq K \) for each \( m \in \mathbb{N} \), we have \( \cup_{m \in \mathbb{N}} u_m v_m \subseteq \mathcal{E} \cap L \) and thus \( \mathcal{E} \cap L = \mathcal{E} \).

Conversely, suppose that \( L \subseteq \Sigma^* \) is \( k \)-steppable and for all ends \( \mathcal{E} \) of \( (\Sigma^*, d) \), \( L \cap \mathcal{E} \) is an end of \( (\Sigma^*, d) \). Then for all \( f : \mathbb{N} \to \Sigma \) there exists \( g : \mathbb{N} \to \Sigma \) such that \( L \cap \mathcal{E}_f = \mathcal{E}_g \).

Take \( u \in \Sigma^* \). Say, \( u = u_1 \ldots u_n \) where \( u_1, \ldots, u_n \in \Sigma \). Define \( f : \mathbb{N} \to \Sigma \) by

\[
i \mapsto \begin{cases} 
u_i & i \in \{1, \ldots, n\} \\
u_n & i > n \end{cases}
\]

Apply the above to obtain \( g : \mathbb{N} \to \Sigma \) such that \( L \cap \mathcal{E}_f = \mathcal{E}_g \). Let \( X \) be an end set of \( \mathcal{E}_g \) where \( X \) is \( k \)-steppable. Then \( \exists v \in \Sigma^* : |v| \leq k \) such that \( uv \in X \). Since \( X \subseteq L \) we conclude \( uv \in L \). Hence, \( L \) is complete.

\( \square \)
Before concluding, we note a question that warrants further study.

Declare a map \( f : \Sigma^* \to \Sigma^* \) to be suffix preserving if for all \( w \in \Sigma^* \), \( w \in \text{suff}(f(w)) \).
The author has confidence in the following statement, although he failed to complete a timely proof.

**Conjecture 1.** A language \( L \subseteq \Sigma^* \) is strongly connected if and only if for all ends \([Y]\) of \( L \) there is a suffix preserving isometric embedding \( L \hookrightarrow [Y] \).
6.3 Linear Sub-Languages

In formal language theory, it is common to study an invariant called Parikh image of a language. For a discussion, see [10]. In this section, we prove a result that decomposes a strongly connected language into sublanguages having “nice” Parikh images.

A subset \( f \subseteq \mathbb{N}^n \) is **linear** if there exists \( f_0, f_1, \ldots, f_m \in \mathbb{N}^n \) such that
\[
f = f_0 + \text{span}_\mathbb{N}\{f_1, \ldots, f_m\} = \{f_0 + k_1 f_1 + \ldots + k_m f_m \mid k_1, \ldots, k_m \in \mathbb{N}\}.
\]

A set is **semilinear** if it is a finite union of linear sets. The function \( \psi : \Sigma^* \to \mathbb{N}^n \) given by \( w \mapsto (|w|_{\sigma_1}, \ldots, |w|_{\sigma_n}) \) is called the **Parikh map**. A standard result of formal language theory states that if \( L \) is regular then \( \psi(L) \) is semilinear. For any \( h \subseteq \mathbb{N}^n \) we define \( L^h = \{w \in L \mid \psi(w) \in h\} \).

**Lemma 20.** Let \( R \subseteq \Sigma^* \) be regular and \( h \subseteq \mathbb{N}^n \) linear. Then \( R^h \) is regular.

**Proof.** By assumption, \( \exists a, b_1, \ldots, b_m \in \mathbb{N}^n \) such that \( h = a + \text{span}_\mathbb{N}\{b_1, \ldots, b_m\} \). For each \( i \in \{1, \ldots, m\} \), define a language \( P_i \subseteq \Sigma^* \) by
\[
P_i = \{w \in \Sigma^* \mid \psi(w) \in \text{span}_\mathbb{N}\{b_i\}\}.
\]

Let \( \{e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)\} \) be the standard basis for \( \mathbb{N}^n \). Each \( P_i \) is regular and is accepted by a DFA \( A_i \) with states \( \{c \in \mathbb{N}^n \mid c \leq b_i\} \), initial state \( (0, \ldots, 0) \), accept state(s) \( \{(0, \ldots, 0)\} \) and transition function \( \delta_{A_i} \) given by
\[
\delta_{A_i}(c, \sigma_j) = \begin{cases} 
  c + e_j & \text{if } c + \sigma_j \leq b_i \\
  c - c_j e_j & \text{otherwise}
\end{cases}
\]

where \( c = (c_1, \ldots, c_m) \). Define a language \( P \subseteq \Sigma^* \) by
\[
P = \left( \prod_{j=1}^k P_{\alpha_k} \mid \alpha_1, \ldots, \alpha_k \in \{1, \ldots, m\} \text{ with } \alpha_s = \alpha_t \implies s = t \right)
\]

Since \( P \) is a finite union of products of the \( P_i \), it is regular. Finally, we let \( Q = \{w \in \Sigma^* \mid \psi(w) = a\} \). Since \( Q \) is finite, it is regular. Now we have \( QP = \{w \in \Sigma^* \mid \psi(w) \in h\} \).

Hence, \( R^h = R \cap QP \).

\[ \square \]

**Corollary 2.** Let \( R \subseteq \Sigma^* \) be regular and \( h \subseteq \mathbb{N}^n \) semilinear. Then \( R^h \) is regular.

**Lemma 21.** Let \( R \subseteq \Sigma^* \) be regular. Then there exist disjoint regular \( R_1, \ldots, R_p \subseteq \Sigma^* \) such that \( R = R_1 \cup \ldots \cup R_p \) with each \( \psi(R_i) \) linear.
6 Strongly Connected Languages

Proof. Since $\psi(R)$ is semilinear, there exist $h_1, \ldots, h_p \subseteq \mathbb{N}^n$ such that $\psi(R) = h_1 \cup \ldots \cup h_p$. By the main result in [3], we can choose the $h_1, \ldots, h_p$ to be disjoint. For each $i \in \{1, \ldots, p\}$, let $R_i = R^{h_i}$. By lemma 20, each $R_i$ is regular. If $w \in R_i \cap R_j$ then $\psi(w) \in h_i \cap h_j$. But the $h_1, \ldots, h_p$ are disjoint and hence $i = j$. Hence, the $R_1, \ldots, R_p$ are disjoint. If $w \in R$ then $\exists i$ such that $\psi(w) \in h_i$. From the definition we have $w \in R^{h_i}$ and so $R \subseteq R^{h_1} \cup \ldots \cup R^{h_p}$. The reverse inclusion is clear.

Lemma 22. Let $R \subseteq \Sigma^*$ be strongly connected and regular. If $h \subseteq \mathbb{N}^n$ is linear and infinite, then $R^h$ is strongly connected.

Proof. Firstly, we observe that $L = (\Sigma^*)^h$ is strongly connected in the case $h$ infinite. Since $R^h = R \cap L$ we have from theorem 4 that $R^h$ is strongly connected.

Theorem 6. Let $R$ be strongly connected and regular. Then $\exists R_1, \ldots, R_p \subseteq \Sigma^*$ with each $R_i$ is strongly connected and each $\psi(R_i)$ linear such that $R = R_1 \cup \ldots \cup R_p$.

Proof. By lemmas 21 and 22, there exist disjoint $R_1, \ldots, R_p, F_1, \ldots, F_q \subseteq \Sigma^*$ with each $R_i$ strongly connected, each $\psi(R_i)$ linear and each $F_j$ finite such that $R = R_1 \cup \ldots \cup R_p \cup F_1 \cup \ldots \cup F_q$. Hence, for all $u \in \Sigma^*$ there exists $v \in \Sigma^*$ such that

$uv\Sigma^* \cap R = uvR$

$\iff uv\Sigma^* \cap (R_1 \cup \ldots \cup R_p \cup F_1 \cup \ldots \cup F_q) = uv(R_1 \cup \ldots \cup R_p \cup F_1 \cup \ldots \cup F_q)$

$\iff (uv\Sigma^* \cap (R_1 \cup \ldots \cup R_p \cup F_1 \cup \ldots \cup F_q)) \cup (uv\Sigma^* \cap (F_1 \cup \ldots \cup F_q))$

$= uv(R_1 \cup \ldots \cup R_p) \cup uv(F_1 \cup \ldots \cup F_q)$

where $\bar{R} = R_1 \amalg \ldots \amalg R_p$ is strongly connected. Hence,

$\forall u \in \Sigma^* \exists v \in \Sigma^* : uv\Sigma^* \cap (F_1 \cup \ldots \cup F_q) = uv(F_1 \cup \ldots \cup F_q)$

and so the finite language $F_1 \cup \ldots \cup F_q$ is strongly connected. This implies $F_1 \cup \ldots \cup F_q = \emptyset$. Therefore, we conclude $R = R_1 \cup \ldots \cup R_p$.

\[\square\]
6.4 Closure Properties

A map $f : \Sigma^* \rightarrow \Sigma^*$ is a homomorphism if for all $a_1, \ldots, a_n \in \Sigma$ we have $f(a_1 \ldots a_n) = f(a_1) \ldots f(a_n)$. A class of languages $\mathcal{C}$ is said to be closed under a union, intersection, Kleene star, concatenation, complementation or homomorphism if for all languages $L_1$ and $L_2$ in $\mathcal{C}$ we have $L_1 \cup L_2$, $L_1 \cap L_2$, $L_1^*$, $\Sigma^* \setminus L_1$ or $f(L)$ (respectively) as languages in $\mathcal{C}$.

Example 8. Let $\Sigma = \{a, b\}$ define $f$ to be the homomorphism satisfying $a \mapsto ab$, $b \mapsto \epsilon$. The language $L = \Sigma^*$ is complete however the language $f(L) = \{ab\}^*$ is not complete with respect to $\Sigma$, or indeed with respect to any alphabet $\Sigma' \subseteq \Sigma$.

We summarise here some closure properties of the classes of complete, strongly connected, regular and context-free languages.

<table>
<thead>
<tr>
<th></th>
<th>$L \cup M$</th>
<th>$L \cap M$</th>
<th>$L^*$</th>
<th>$LM$</th>
<th>$\Sigma^* \setminus L$</th>
<th>$f(L)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete</td>
<td>√</td>
<td>×</td>
<td>√</td>
<td>√</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Strongly Connected</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>×</td>
<td>√</td>
<td>×</td>
</tr>
<tr>
<td>Regular</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Context Free</td>
<td>√</td>
<td>×</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>

The counter examples for complete and strongly connected languages are contained earlier in the text. The proofs and counter-examples for regular and context-free languages, can be found in [10].
7 Appendix

The usual pumping lemma for regular languages is as follows.

**Lemma 23.** Let \( R \subseteq \Sigma^* \) be regular. Then there exists \( k \in \mathbb{N} \) such that every \( w \in \Sigma^* \) with \(|w| \geq k\) can be written as \( w = xyz \) for some \( x, y, z \in \Sigma^* \) satisfying

1. \(|y| \geq 1\)
2. \(|xy| \leq k\)
3. \(\forall i \in \mathbb{N} : xy^iz \in R\)

We provide here a slight variation.

**Lemma 24.** Let \( R \subseteq \Sigma^* \) be regular. Then there exists \( k \in \mathbb{N} \) such that every \( w \in \Sigma^* \) with \(|w| \geq k\) can be written as \( w = xyz \) for some \( x, y, z \in \Sigma^* \) satisfying

1. \(|y| \geq 1\)
2. \(|yz| \leq k\)
3. \(\forall i \in \mathbb{N} : xy^iz \in R\)

**Proof.** Let \( \hat{k} \) be the cardinality of the set \( \Sigma^*/\sim_R \). Fix \( w \in \Sigma^* \). Let \( z \in \Sigma^* \) be the longest suffix of \( w \) such that \(|\delta([\epsilon],\text{pref}(z))] = |z|\) and \( \bar{w} \in \Sigma^* \) the word satisfying \( w = \bar{w}z \). Our choice of \( z \) ensures that \(|z| < \hat{k}\). Also, \( \exists x, y \in \Sigma^* \) such that \( \bar{w} = xy \) and \( x \sim_R xy \). By choosing \( x \) to be sufficiently long, we can assume that \(|y| \geq 1\) and \( \bar{y} \in \text{pref}(y) \wedge xy \sim_R x\bar{y} \). This implies that \(|y| \leq \hat{k}\). Hence, \( k = 2\hat{k} \) satisfies \(|yz| \leq k\). Finally, see from \( x \sim_R xy \) and \( w = xyz \in R \) that \( \forall i \in \mathbb{N} : xy^iz \in R \).

\(\Box\)
Glossary

\( E_X \)  The collection of end sets of the metric space \( X \).

\( \Sigma^* \)  The family of all words over the alphabet \( \Sigma \).

\( |w| \)  The length of the word \( w \).

\( \sim \)  An equivalence relation on the end sets of a metric space.

\( \sim_L \)  The Myhill-Nerode equivalence relation associated with the language \( L \).

\( \mathcal{A} \)  A deterministic automaton.

\( \Delta(S,T) \)  The distance from the state \( S \) to \( T \).

\( \delta \)  The transition function of an automaton.

\( \mathcal{L}(\mathcal{A}) \)  The language accepted by the automaton \( \mathcal{A} \).

\( k^X \)  The smallest \( k \in \mathbb{N} \) for which the metric space \( X \) is \( k \)-steppable.

\( \text{cyc}(S) \)  The collection of words defining cycles based at the state \( S \).

\( d \)  A metric defined on the space of words \( \Sigma^* \).

\( \text{flat}(S) \)  The collection of words defining flat cycles based at the state \( S \).

\( \text{geo}(S) \)  The collection of words defining geodesics based at the state \( S \).

\( \text{geo}(S,T) \)  The collection of words defining geodesics from the state \( S \) to \( T \).

\( \text{irr}(S) \)  The collection of words defining irreducible cycles based at the state \( S \).

\( \text{path}(S) \)  The collection of words defining paths based at the state \( S \).

\( \text{pref}(w) \)  The collection of prefixes of the word \( w \).

\( \text{rig}(S) \)  The collection of words defining rigid cycles based at the state \( S \).

\( \text{rigPath}(S) \)  The collection of words defining rigid paths based at the state \( S \).
Bibliography


# Index

**A**
- alphabet, 9
- automaton
  - accept states of, 9
  - initial state of, 9
  - permutation, 28
  - states of, 9
  - strongly connected, 10

**C**
- Cayley graph, 10
- cycle, 10
  - flat, 18
  - irreducible, 15
  - reducible, 15
  - rigid, 16

**D**
- deterministic automaton, 9
- distance, 18

**E**
- end, 36
- end set, 36

**G**
- geodesic, 18

**K**
- Kleene star
  - of a language, 9
- Krohn-Rhodes complexity, 5
- k-steppable, 35

**L**
- language, 9
  - accepted by an automaton, 9
  - cobounded, 34
  - complete, 30
  - strongly connected, 30

**M**
- monoid
  - divides, 4
- Myhill-Nerode, equivalence relation, 30

**P**
- Parikh map, 40
- path, 10
  - rigid, 16
- prefix
  - of a word, 9
- pumping lemma
  - for regular languages, 43

**S**
- set
  - linear, 40
  - semilinear, 40
- state
  - focality at, 18
  - stability at, 18
- suffix preserving map, 39

**T**
- transition function, 9
- transition monoid, 9

**W**
- word, 9