A tutorial on sequential functions

Jean-Éric Pin

LIAFA, CNRS and University Paris 7

30 January 2006, CWI, Amsterdam
(1) Sequential functions
(2) A characterization of sequential transducers
(3) Minimal sequential transducers
(4) Minimization of sequential transducers
(5) Composition of sequential transducers
(6) An algebraic approach
(7) The wreath product principle
Part I

Sequential functions
Informal definitions

A transducer (or state machine) is an automaton equipped with an output function. A transducer computes a relation on $A^* \times B^*$.

A sequential transducer is a transducer whose underlying automaton is deterministic (but not necessarily complete). A sequential transducer computes a partial function from $A^*$ into $B^*$.

A pure sequential transducer computes a partial function $\varphi$ preserving prefixes: if $u$ is a prefix of $v$, then $\varphi(u)$ is a prefix of $\varphi(v)$. 
An example of a pure sequential transducer

On the input $abaa$, the output is $01001$. 
A pure sequential transducer is a 6-tuple

\[ A = (Q, A, B, i, \cdot, *) \]

where the input function \((q, a) \rightarrow q \cdot a \in Q\) and the output function \((q, a) \rightarrow q * a \in B^*\) are defined on the same domain \(D \subseteq Q \times A\).
The transition function is extended to $Q \times A^* \rightarrow Q$. Set $q \cdot \varepsilon = q$ and, if $q \cdot u$ and $(q \cdot u) \cdot a$ are defined, $q \cdot (ua) = (q \cdot u) \cdot a$.

The output function is extended to $Q \times A^* \rightarrow B^*$. Set $q \ast \varepsilon = \varepsilon$ and, if $q \ast u$ and $(q \ast u) \ast a$ are defined, $q \ast (ua) = (q \ast u)((q \ast u) \ast a)$.

![Diagram of automaton states and transitions]

- $q$ transitions to $q \cdot u$ on input $u$.
- From $q \cdot u$, it transitions to $q \cdot ua$ on input $a$.
- The output function at $q \cdot u$ is $(q \ast u)((q \ast u) \ast a)$.
Pure sequential functions

The function $\varphi: A^* \rightarrow B^*$ defined by

$$\varphi(u) = i \ast u$$

is called the function realized by $A$.

A function is **pure sequential** if it can be realized by some pure sequential transducer.
Examples of pure sequential functions

Replacing consecutive white spaces by a single one:

![Diagram 1]

Converting upper case to lower case letters:

![Diagram 2]
Coding and decoding

Consider the coding

\[
a \rightarrow 0 \quad b \rightarrow 1010 \quad c \rightarrow 100 \quad d \rightarrow 1011 \quad r \rightarrow 11
\]

Decoding function
Decoding

\[ a \rightarrow 0 \quad b \rightarrow 1010 \quad c \rightarrow 100 \quad d \rightarrow 1011 \quad r \rightarrow 11 \]

\[
\begin{array}{c}
\begin{array}{c}
0|a \\
1|\epsilon \\
1|r \\
0|\epsilon \\
1|\epsilon \\
0|\epsilon \\
1|\epsilon \\
\end{array} \\
\begin{array}{c}
0|b \\
1|d \\
0|c \\
\end{array}
\end{array}
\]

\[010101101000101101010110 \rightarrow abracadabra\]
A sequential transducer is a transducer whose underlying automaton is deterministic (but not necessarily complete). There is an initial prefix and a terminal function.

On the input $abaa$, the output is $110100100$. 
A sequential transducer is a 8-tuple

\[ A = (Q, A, B, i, \cdot, *, m, \rho) \]

where \((Q, A, B, i, \cdot, *)\) is a pure sequential transducer, \(m \in B^*\) is the initial prefix and \(\rho: Q \rightarrow B^*\) is a partial function, called the terminal function.
Sequential functions

The function $\varphi: A^* \rightarrow B^*$ defined by

$$\varphi(u) = m(i \ast u)\rho(i \cdot u)$$

is called the function realized by $A$.

A function is **sequential** if it can be realized by some sequential transducer.
Some examples of sequential functions

The function $x \rightarrow x + 1$ (in reverse binary)

The map $\varphi : A^* \rightarrow A^*$ defined by $\varphi(x) = uxv$. 

LIAFA, CNRS and University Paris VII
In inverse binary notation, \(22 = 2 + 4 + 16 \rightarrow 01101\) and \(13 = 1 + 4 + 8 \rightarrow 10110\). Taking as input \((0, 1)(1, 0)(1, 1)(0, 1)(1, 0)\), the output is \(110001\), the inverse binary representation of \(35 = 1 + 2 + 32\).
Hardware applications (Wikipedia)

The circuit diagram for a 4 bit TTL counter
Other examples

Multiplication by 4

Replacing each occurrence of 011 by 100.
Multiplication by 10
Part II

A characterization
The geodesic metric

The distance between $ababab$ and $abaabba$ is 7.
The geodesic metric (2)

Denote by $u \wedge v$ the longest common prefix of the words $u$ and $v$. Then

$$d(u, v) = |u| + |v| - 2|u \wedge v|$$

Example: $d(ababab, abaabba) = 6 + 7 - 2 \times 3 = 7$.

One can show that $d$ is a metric.

1. $d(u, v) = 0$ iff $u = v$,
2. $d(u, v) = d(v, u)$,
3. $d(u, v) \leq d(u, w) + d(w, v)$. 
A characterization of sequential functions

A function $\varphi : A^* \rightarrow B^*$ is Lipschitz if there exists some $K > 0$ such that, for all $u, v \in A^*$,

$$d(\varphi(u), \varphi(v)) \leq K d(u, v)$$

**Theorem (Choffrut 1979)**

Let $\varphi : A^* \rightarrow B^*$ be a function whose domain is closed under taking prefixes. TFCAE:

(1) $\varphi$ is sequential,
(2) $\varphi$ is Lipschitz, and $\varphi^{-1}$ preserves regular sets.
Theorem (Ginsburg-Rose 1966)

Let $\varphi : A^* \to B^*$ be a function whose domain is closed under taking prefixes. TFCAE:

(1) $\varphi$ is a pure sequential function,

(2) $\varphi$ is Lipschitz and preserves prefixes, and $\varphi^{-1}$ preserves regular sets.
Part III

Minimal sequential transducers
Residuals of a language

Let $L$ be a language over $A^*$. Let $u \in A^*$. The (left) residual of $L$ by $u$ is the set

$$u^{-1}L = \{x \in A^* \mid ux \in L\}.$$

It is easy to see that $v^{-1}(u^{-1}L) = (uv)^{-1}L$.

Let $A = \{a, b\}$ and $L = A^*abaA^*$. Then

$$1^{-1}L = L \quad a^{-1}L = A^*abaA^* \cup baA^*$$

$$b^{-1}L = L \quad (ab)^{-1}L = A^*abaA^* \cup aA^*,$$ etc.
The minimal automaton of a language \( L \) is equal to

\[
A(L) = (Q, A, \cdot, i, F)
\]

where \( Q = \{ u^{-1}L \neq \emptyset \mid u \in A^* \} \), \( i = L \) and \( F = \{ u^{-1}L \mid u \in L \} \). The transition function is given by

\[
(u^{-1}L) \cdot a = a^{-1}(u^{-1}L) = (ua)^{-1}L.
\]
Example of a minimal automaton

Let $A = \{a, b\}$ and $L = A^*abaA^*$. Then

$$a^{-1}L = A^*abaA^* \cup baA^* = L_1$$
$$b^{-1}L_1 = A^*abaA^* \cup aA^* = L_2$$
$$a^{-1}L_2 = A^* = L_3$$
$$a^{-1}L_3 = b^{-1}L_3 = L_3$$

$$b^{-1}L = L$$
$$a^{-1}L_1 = L_1$$
$$b^{-1}L_2 = L$$

$L$ \[ \xrightarrow{a} L_1 \xrightarrow{b} L_2 \xrightarrow{a} L_3 \]
Residuals of a sequential function

Let $\varphi : A^* \to B^*$ be a function and let $u \in A^*$. The residual of $\varphi$ by $u$ is the function $u^{-1}\varphi : A^* \to B^*$ defined by

$$(u^{-1}\varphi)(x) = (\varphi * u)^{-1}\varphi(ux)$$

where $(\varphi * u)$ is the longest common prefix of the words $\varphi(ux)$, for $ux \in \text{Dom}(\varphi)$.

In other words, $u^{-1}\varphi$ can be obtained from the function $x \mapsto \varphi(ux)$ by deleting the prefix $\varphi * u$ of $\varphi(ux)$. 
The function $n \rightarrow 6n$

<table>
<thead>
<tr>
<th>$n$</th>
<th>$x$</th>
<th>$\varphi(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\varepsilon$</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>011</td>
</tr>
<tr>
<td>2</td>
<td>01</td>
<td>0011</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>01001</td>
</tr>
<tr>
<td>4</td>
<td>001</td>
<td>00011</td>
</tr>
<tr>
<td>5</td>
<td>101</td>
<td>01111</td>
</tr>
<tr>
<td>6</td>
<td>011</td>
<td>001001</td>
</tr>
<tr>
<td>7</td>
<td>111</td>
<td>010101</td>
</tr>
<tr>
<td>8</td>
<td>0001</td>
<td>000011</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$n$</th>
<th>$x$</th>
<th>$\varphi(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>1001</td>
<td>011011</td>
</tr>
<tr>
<td>10</td>
<td>0101</td>
<td>001111</td>
</tr>
<tr>
<td>11</td>
<td>1101</td>
<td>0100001</td>
</tr>
<tr>
<td>12</td>
<td>0011</td>
<td>0001001</td>
</tr>
<tr>
<td>13</td>
<td>1011</td>
<td>0111001</td>
</tr>
<tr>
<td>14</td>
<td>0111</td>
<td>0010101</td>
</tr>
<tr>
<td>15</td>
<td>1111</td>
<td>0101101</td>
</tr>
<tr>
<td>16</td>
<td>00001</td>
<td>0000011</td>
</tr>
<tr>
<td>17</td>
<td>10001</td>
<td>0110011</td>
</tr>
</tbody>
</table>
Let $\varepsilon^{-1}\varphi = \varphi_0$. Then $\varphi_0$ represents $n \rightarrow 3n$

<table>
<thead>
<tr>
<th>$n$</th>
<th>$x$</th>
<th>$\varphi(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\varepsilon$</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>011</td>
</tr>
<tr>
<td>2</td>
<td>01</td>
<td>0011</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>01001</td>
</tr>
<tr>
<td>4</td>
<td>001</td>
<td>00011</td>
</tr>
<tr>
<td>5</td>
<td>101</td>
<td>01111</td>
</tr>
<tr>
<td>6</td>
<td>011</td>
<td>001001</td>
</tr>
<tr>
<td>7</td>
<td>111</td>
<td>010101</td>
</tr>
<tr>
<td>8</td>
<td>0001</td>
<td>000011</td>
</tr>
<tr>
<td>9</td>
<td>1001</td>
<td>011011</td>
</tr>
<tr>
<td>10</td>
<td>0101</td>
<td>001111</td>
</tr>
<tr>
<td>11</td>
<td>1101</td>
<td>0100001</td>
</tr>
<tr>
<td>12</td>
<td>0011</td>
<td>0001001</td>
</tr>
<tr>
<td>13</td>
<td>1011</td>
<td>0111001</td>
</tr>
<tr>
<td>14</td>
<td>0111</td>
<td>0010101</td>
</tr>
<tr>
<td>15</td>
<td>1111</td>
<td>0101101</td>
</tr>
<tr>
<td>16</td>
<td>00001</td>
<td>0000011</td>
</tr>
<tr>
<td>17</td>
<td>10001</td>
<td>0110011</td>
</tr>
</tbody>
</table>
The function $\varphi_0$, representing $n \rightarrow 3n$

<table>
<thead>
<tr>
<th>$n$</th>
<th>$x$</th>
<th>$\varphi_0(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\varepsilon$</td>
<td>$\varepsilon$</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>01</td>
<td>011</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>1001</td>
</tr>
<tr>
<td>4</td>
<td>001</td>
<td>0011</td>
</tr>
<tr>
<td>5</td>
<td>101</td>
<td>1111</td>
</tr>
<tr>
<td>6</td>
<td>011</td>
<td>01001</td>
</tr>
<tr>
<td>7</td>
<td>111</td>
<td>10101</td>
</tr>
<tr>
<td>8</td>
<td>0001</td>
<td>00011</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$n$</th>
<th>$x$</th>
<th>$\varphi_0(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>1001</td>
<td>11011</td>
</tr>
<tr>
<td>10</td>
<td>0101</td>
<td>01111</td>
</tr>
<tr>
<td>11</td>
<td>1101</td>
<td>100001</td>
</tr>
<tr>
<td>12</td>
<td>0011</td>
<td>001001</td>
</tr>
<tr>
<td>13</td>
<td>1011</td>
<td>111001</td>
</tr>
<tr>
<td>14</td>
<td>0111</td>
<td>010101</td>
</tr>
<tr>
<td>15</td>
<td>1111</td>
<td>101101</td>
</tr>
<tr>
<td>16</td>
<td>00001</td>
<td>000011</td>
</tr>
<tr>
<td>17</td>
<td>10001</td>
<td>110011</td>
</tr>
</tbody>
</table>
Residuals of $\varphi_0$

Let $\varphi_0$, $\varphi_1$ and $\varphi_2$ be the functions representing $n \to 3n$, $n \to 3n + 1$ and $n \to 3n + 2$, respectively.

$\varphi_0 \ast 0 = 0$

$(0^{-1} \varphi_0)(x) = 0^{-1} \varphi_0(0x) = \varphi_0(x)$

$\varphi_0 \ast 1 = 1$

$(1^{-1} \varphi_0)(x) = 1^{-1} \varphi_0(1x) = \varphi_1(x)$

Indeed, if $x$ represents $n$, $1x$ represents $2n + 1$, $\varphi_0(1x)$ represents $3(2n + 1) = 6n + 3$ and $1^{-1} \varphi_0(1x)$ represents $((6n + 3) - 1)/2 = 3n + 1$. 
The function $\varphi_1$, representing $n \rightarrow 3n + 1$

<table>
<thead>
<tr>
<th>$n$</th>
<th>$x$</th>
<th>$\varphi_1(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\varepsilon$</td>
<td>$\varepsilon$</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>001</td>
</tr>
<tr>
<td>2</td>
<td>01</td>
<td>111</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>0101</td>
</tr>
<tr>
<td>4</td>
<td>001</td>
<td>1011</td>
</tr>
<tr>
<td>5</td>
<td>101</td>
<td>00001</td>
</tr>
<tr>
<td>6</td>
<td>011</td>
<td>11001</td>
</tr>
<tr>
<td>7</td>
<td>111</td>
<td>01101</td>
</tr>
<tr>
<td>8</td>
<td>0001</td>
<td>10011</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$n$</th>
<th>$x$</th>
<th>$\varphi_1(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>1001</td>
<td>00111</td>
</tr>
<tr>
<td>10</td>
<td>0101</td>
<td>100001</td>
</tr>
<tr>
<td>11</td>
<td>1101</td>
<td>010001</td>
</tr>
<tr>
<td>12</td>
<td>0011</td>
<td>101001</td>
</tr>
<tr>
<td>13</td>
<td>1011</td>
<td>000101</td>
</tr>
<tr>
<td>14</td>
<td>0111</td>
<td>110101</td>
</tr>
<tr>
<td>15</td>
<td>1111</td>
<td>011101</td>
</tr>
<tr>
<td>16</td>
<td>00001</td>
<td>100011</td>
</tr>
<tr>
<td>17</td>
<td>10001</td>
<td>001011</td>
</tr>
</tbody>
</table>
Residuals of $\varphi_1$

\[
\varphi_1 \ast 0 = 1 \\
(0^{-1} \varphi_1)(x) = 1^{-1} \varphi_1(0x) = \varphi_0(x)
\]

Indeed, if $x$ represents $n$, $0x$ represents $2n$, $\varphi_1(0x)$ represents $3(2n) + 1 = 6n + 1$ and $1^{-1} \varphi_1(0x)$ represents $((6n + 1) - 1)/2 = 3n$.

\[
\varphi_1 \ast 1 = 0 \\
(1^{-1} \varphi_1)(x) = 0^{-1} \varphi_1(1x) = \varphi_2(x)
\]

Indeed, if $x$ represents $n$, $1x$ represents $2n + 1$, $\varphi_1(1x)$ represents $3(2n + 1) + 1 = 6n + 4$ and $0^{-1} \varphi_1(1x)$ represents $(6n + 4)/2 = 3n + 2$.
The function $\varphi_2$, representing $n \rightarrow 3n + 2$

<table>
<thead>
<tr>
<th>$n$</th>
<th>$x$</th>
<th>$\varphi_2(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\varepsilon$</td>
<td>$\varepsilon$</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>101</td>
</tr>
<tr>
<td>2</td>
<td>01</td>
<td>0001</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>1101</td>
</tr>
<tr>
<td>4</td>
<td>001</td>
<td>0111</td>
</tr>
<tr>
<td>5</td>
<td>101</td>
<td>10001</td>
</tr>
<tr>
<td>6</td>
<td>011</td>
<td>00101</td>
</tr>
<tr>
<td>7</td>
<td>111</td>
<td>11101</td>
</tr>
<tr>
<td>8</td>
<td>0001</td>
<td>01011</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$n$</th>
<th>$x$</th>
<th>$\varphi_2(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>1001</td>
<td>10111</td>
</tr>
<tr>
<td>10</td>
<td>0101</td>
<td>000001</td>
</tr>
<tr>
<td>11</td>
<td>1101</td>
<td>110001</td>
</tr>
<tr>
<td>12</td>
<td>0011</td>
<td>011001</td>
</tr>
<tr>
<td>13</td>
<td>1011</td>
<td>100101</td>
</tr>
<tr>
<td>14</td>
<td>0111</td>
<td>001101</td>
</tr>
<tr>
<td>15</td>
<td>1111</td>
<td>111101</td>
</tr>
<tr>
<td>16</td>
<td>00001</td>
<td>010011</td>
</tr>
<tr>
<td>17</td>
<td>10001</td>
<td>101011</td>
</tr>
</tbody>
</table>
Residuals of $\varphi_2$

$$\varphi_2 \ast 0 = 0$$

$$(0^{-1} \varphi_2)(x) = 0^{-1} \varphi_2(0x) = \varphi_1(x)$$

Indeed, if $x$ represents $n$, $0x$ represents $2n$, $\varphi_2(0x)$ represents $3(2n) + 2 = 6n + 2$ and $0^{-1} \varphi_2(0x)$ represents $(6n + 2)/2 = 3n + 1$.

$$\varphi_2 \ast 1 = 1$$

$$(1^{-1} \varphi_2)(x) = 1^{-1} \varphi_2(1x) = \varphi_2(x)$$

Indeed, if $x$ represents $n$, $1x$ represents $2n + 1$, $\varphi_2(1x)$ represents $3(2n + 1) + 2 = 6n + 5$ and $1^{-1} \varphi_2(1x)$ represents $((6n + 5) - 1)/2 = 3n + 2$. 
Minimal sequential transducer of a function $\varphi$

It is the sequential transducer whose states are the residuals of $\varphi$ and transitions are of the form $a\mid\psi\ast a \rightarrow a^{-1}\psi$

Recall that $\psi\ast a$ is the longest common prefix of the words $\psi(ax)$, for $ax \in \text{Dom}(\varphi)$. The initial state is $\varepsilon^{-1}\varphi$ and the initial prefix is $\varphi\ast\varepsilon$. 
More formally...

It is the sequential transducer $A_\varphi = (Q, A, B, i, \cdot, *, m, \rho)$ defined by

$Q = \{ u^{-1} \varphi | u \in A^* \text{ and } \text{Dom}(\varphi \cdot u) \neq \emptyset \}$

$i = \varepsilon^{-1} \varphi$, $m = \varphi \star \varepsilon$ and, for $q \in Q$, $\rho(q) = q(\varepsilon)$

A typical transition of $A_\varphi$:

$$u^{-1} \varphi \xrightarrow{a | (u^{-1} \varphi) \star a} (ua)^{-1} \varphi$$

$(u^{-1} \varphi)(\varepsilon)$ $(((ua)^{-1} \varphi)(\varepsilon)$
The minimal sequential function of $n \rightarrow 6n$

$185 = 1 + 8 + 16 + 32 + 128$ and $6 \times 185 = 1110 = 2 + 4 + 16 + 64 + 1024$.

Thus $\varphi(10011101) = 01101010001$
Part IV

Minimizing sequential transducers
The three steps of the algorithm

How to minimize a sequential transducer?

1. Obtain a trim transducer (easy)
2. Normalise the transducer (tricky)
3. Merge equivalent states (standard)
Obtaining a trim transducer

Let \( A = (Q, A, B, i, \cdot, *, m, \rho) \) be a sequential transducer and let \( F = \text{Dom}(\rho) \). The transducer \( A \) is trim if the automaton \((Q, A, \cdot, q_0, F)\) is trim: all states are accessible from the initial state and one can reach a final state from any state.

**Algorithm**: it suffices to remove the useless states.
Equivalent transducers

These four sequential transducers realize exactly the same function \( \varphi : \{a, b\}^* \rightarrow \{a, b\}^* \), with domain \((aa)^*b\), defined, for all \(n \geq 0\), by \(\varphi(a^{2n}b) = (ab)^n a\).
Normalized transducer

Let $A = (Q, A, B, i, \cdot, *, m, \rho)$ be a sequential transducer. For each state $q$, denote by $m_q$ the greatest common prefix of the words $(q \cdot u)\rho(q \cdot u)$, where $u$ ranges over the domain of the sequential function.

Equivalently, $m_q = \varphi_q \epsilon$, where $\varphi_q$ is the sequential function realized by the transducer derived from $A$ by taking $q$ as initial state and the empty word as initial prefix.

A sequential transducer is normalized if, for all states $q$, $m_q$ is the empty word.
\[ m_q = (q \ast u) \rho (q \cdot u) \]

\begin{align*}
(1) & \quad m_1 = \varepsilon & m_2 = \varepsilon & m_3 = \varepsilon \\
(2) & \quad m_1 = \varepsilon & m_2 = a & m_3 = \varepsilon \\
(3) & \quad m_1 = \varepsilon & m_2 = a & m_3 = \varepsilon \\
(4) & \quad m_1 = a & m_2 = a & m_3 = \varepsilon 
\end{align*}
Normalising a transducer

Let $A = (Q, A, B, i, \cdot, \ast, m, \rho)$ be a trim sequential transducer. One obtains a normalised transducer by changing the initial prefix, the output function and the terminal function as follows:

$q' a = m_q^{-1}(q \ast a)m_{q \cdot a}$

$m' = mm_i$

$\rho'(q) = m_q^{-1}\rho(q)$
Normalisation on an example

One has $m_1 = a$, $m_2 = a$, $m_3 = \varepsilon$. Thus

$$m' = mm_1 = \varepsilon a = a$$

$$1*'a = m_1^{-1}(1*a)m_2 = a^{-1}(ab)a = ba$$

$$2*'a = m_2^{-1}(1*a)m_1 = a^{-1}(\varepsilon)a = \varepsilon$$

$$1*'b = m_1^{-1}(1*b)m_3 = a^{-1}(a)\varepsilon = \varepsilon$$

$$\rho'(3) = m_3^{-1}\rho(3) = \varepsilon^{-1}\varepsilon = \varepsilon$$
Computing the $m_q$ is not so easy...

\[
X_1 = abX_1 + abaX_2 + abX_3 \\
X_2 = X_1 + bX_4 \\
X_3 = X_1 + abX_4 \\
X_4 = abX_2 + abab
\]
Solving the system

\[ X_1 = abX_1 + abaX_2 + abX_3 \]
\[ X_2 = X_1 + bX_4 \]
\[ X_3 = X_1 + abX_4 \]
\[ X_4 = abX_2 + abab \]

We work on \( k = A^* \cup \{0\} \). Addition is the least common prefix operator (\( u + 0 = 0 + u = u \) by convention). Observe that \( u + u = u \) and \( u(v_1 + v_2) = uv_1 + uv_2 \) (but \( (v_1 + v_2)u = v_1u + v_2u \) does not hold in general). Thus \( k \) is a left semiring.
The prefix order is a partial order $\leq$ on $k$ (with $u \leq 0$ by convention). One can extend this order to $k^n$ componentwise.

**Proposition**

For all $u, v \in k^n$, the function $f(x) = ux + v$ is increasing. The sequence $f^n(0)$ is decreasing and converges to the greatest fixpoint of $f$.

The greatest solution of our system is exactly $(m_1, m_2, m_3, m_4)$. 
Example of Choffrut’s algorithm

\[ X_1 = abX_1 + abaX_2 + abX_3 \]
\[ X_2 = X_1 + bX_4 \]
\[ X_3 = X_1 + abX_4 \]
\[ X_4 = abX_2 + abab \]

The sequence \( f^n(0) \) is \((0, 0, 0, 0), (0, 0, 0, abab), (0, babab, ababab, abab), (abababab, babab, ababab, ab), (abab, \varepsilon, ababab, ab), (aba, \varepsilon, abab, ab), (aba, \varepsilon, aba, ab), (aba, \varepsilon, aba, ab)\).

Thus \( m_1 = aba, m_2 = \varepsilon, m_3 = aba, m_4 = ab \).
Merging states

Two states are equivalent if they are equivalent in the input automaton \((Q, A, i, F, \cdot)\), have the same output functions and the same terminal functions:

\[
p \sim q \iff \begin{cases} 
p \cdot a \sim q \cdot a \\
p \ast a = q \ast a \\
\rho(p) = \rho(q)
\end{cases}
\]
Part V

Composition of sequential functions
Composition of two pure sequential transducers

**Theorem**

*Pure sequential functions are closed under composition.*

Let \( \sigma \) and \( \tau \) be two pure sequential functions realized by the transducers

\[
A = (Q, A, B, q_0, \cdot, *) \quad \text{and} \quad B = (P, B, C, p_0, \cdot, *)
\]

The **wreath product** of \( B \) by \( A \) is obtained by taking as input for \( B \) the output of \( A \). It realizes \( \tau \circ \sigma \).
Wreath product of two pure sequential transducers

The wreath product is defined by

\[ \mathcal{B} \circ \mathcal{A} = (P \times Q, A, C, (p_0, q_0), \cdot, \ast) \]

\[(p, q) \cdot a = (p \cdot (q \ast a), q \cdot a)\]

\[(p, q) \ast a = p \ast (q \ast a)\]

\[a \mid p \ast (q \ast a)\]
Composition of two sequential transducers

**Theorem**

*Sequential functions are closed under composition.*

Let $\varphi$ and $\psi$ be two sequential functions realized by the transducers $A$ (equipped with the initial word $n$ and the terminal function $\rho$) and $B$ (equipped with the initial word $m$ and the terminal function $\sigma$).

The **wreath product** of $B$ by $A$ is obtained by taking $m(p_0 \ast n)$ as initial word and, as terminal function,

$$\omega(p, q) = (p \ast \rho(q))\sigma(p \cdot \rho(q)).$$
Iterating sequential functions can lead to difficult problems.

Let \( f(n) = \begin{cases} 
3n + 1 & \text{if } n \text{ is odd} \\
n/2 & \text{if } n \text{ is even} 
\end{cases} \)

It is conjectured that for each positive integer \( n \), there exists \( k \) such that \( f^k(n) = 1 \). The problem is still open.
Minimal transducer of the $3n + 1$ function

Let $f(n) = \begin{cases} 
3n + 1 & \text{if } n \text{ is odd} \\
n/2 & \text{if } n \text{ is even} 
\end{cases}$
Iterating the $3n + 1$ function...

A useful result

Let $\varphi : A^* \to B^*$ be a pure sequential function realized by $A = (Q, A, B, q_0, \cdot, \ast)$. Let $L$ be the regular language over $B^*$ recognized by the DFA $B = (P, B, \cdot, p_0, F)$. The wreath product of $B$ by $A$ is the DFA $B \circ A = (P \times Q, A, (p_0, q_0), \cdot)$ defined by $(p, q) \cdot a = (p \cdot (q \ast a), q \cdot a)$.

Theorem

The language $\varphi^{-1}(L)$ is recognized by $B \circ A$. 
Example 1

Let $\varphi(u) = a^n$, where $n$ is the number of occurrences of $aba$ in $u$. This function is pure sequential:

Then $\varphi^{-1}(a)$ is the set of words containing exactly one occurrence of $aba$. 
Wreath product of the two automata
The operation $L \rightarrow LaA^*$

Let $A = (Q, A, B, q_0, F, \cdot)$ be a DFA. Let $B = Q \times A$ and let $\sigma : A^* \rightarrow B^*$ be the pure sequential function defined by

$$\sigma(a_1 \cdots a_n) = (q_0, a_1)(q_0 \cdot a_1, a_2) \cdots (q_0 a_1 \cdots a_{n-1}, a_n)$$

Let $a \in A$ and let $C = F \times \{a\} \subseteq B$. Then $\sigma^{-1}(B^*CB^*) = LaA^*$. [Proof on blackboard!]
Example 2

Therefore $B \circ A$ recognizes $LaA^*$, where $B$ is the minimal automaton of $B^*CB^*$.

Note that if $\varphi$ is a formula of linear temporal logic, then $L(F(p_a \land X\varphi)) = A^*aL(\varphi)$
Part VI

The algebraic approach

Idea: replace automata by monoids.
Transformation monoid of an automaton

Relations:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>a</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>b</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>c</td>
<td>-</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
Transformations monoid of an automaton

Relations:
\[ aa = a \]

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>(a)</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>(b)</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>(c)</td>
<td>-</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
Transformation monoid of an automaton

Relations:
\[ aa = a \]
Transformation monoid of an automaton

Relations:

\[
\begin{align*}
  aa &= a \\
  ac &= a
\end{align*}
\]
Transformation monoid of an automaton

Relations:

\[
\begin{align*}
    aa &= a \\
    ac &= a \\
    ba &= a
\end{align*}
\]

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>b</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>c</td>
<td>-</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>ab</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
Transformation monoid of an automaton

![Diagram of an automaton with states 1, 2, and 3 connected by transitions labeled a, b, and c.]

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>b</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>c</td>
<td>-</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>ab</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Relations:

- $aa = a$
- $ac = a$
- $ba = a$
- $bb = b$
Transformation monoid of an automaton

Relations:
- $aa = a$
- $ac = a$
- $ba = a$
- $bb = b$
Transformation monoid of an automaton

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>a</strong></td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td><strong>b</strong></td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td><strong>c</strong></td>
<td>-</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td><strong>ab</strong></td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td><strong>bc</strong></td>
<td>-</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td><strong>ca</strong></td>
<td>-</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Relations:
- \( aa = a \)
- \( ac = a \)
- \( ba = a \)
- \( bb = b \)
Transformation monoid of an automaton

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>b</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>c</td>
<td>-</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>ab</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>bc</td>
<td>-</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>ca</td>
<td>-</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Relations:

- $aa = a$
- $ac = a$
- $ba = a$
- $bb = b$
- $cb = bc$
Transformation monoid of an automaton

Relations:

- $aa = a$
- $ac = a$
- $ba = a$
- $bb = b$
- $cb = bc$
- $cc = c$
Transformation monoid of an automaton

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>b</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>c</td>
<td>-</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>ab</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>bc</td>
<td>-</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>ca</td>
<td>-</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Relations:

\[
\begin{align*}
aa &= a \\
ac &= a \\
ba &= a \\
bb &= b \\
bc &= bc \\
cc &= c \\
abc &= ab
\end{align*}
\]
Transformation monoid of an automaton

![Diagram of an automaton with states 1, 2, and 3, and transitions labeled with symbols a, b, and c.]

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>b</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>c</td>
<td>-</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>ab</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>bc</td>
<td>-</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>ca</td>
<td>-</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Relations:

- $aa = a$
- $ac = a$
- $ba = a$
- $bb = b$
- $cb = bc$
- $cc = c$
- $abc = ab$
- $bca = ca$
Transformation monoid of an automaton

Relations:

<table>
<thead>
<tr>
<th>Relation</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$aa$</td>
<td>$a$</td>
</tr>
<tr>
<td>$ac$</td>
<td>$a$</td>
</tr>
<tr>
<td>$ba$</td>
<td>$a$</td>
</tr>
<tr>
<td>$bb$</td>
<td>$b$</td>
</tr>
<tr>
<td>$cb$</td>
<td>$bc$</td>
</tr>
<tr>
<td>$cc$</td>
<td>$c$</td>
</tr>
</tbody>
</table>

Table:

<table>
<thead>
<tr>
<th>State</th>
<th>State 1</th>
<th>State 2</th>
<th>State 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$b$</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>$c$</td>
<td>-2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>$ab$</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>$bc$</td>
<td>-3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>$ca$</td>
<td>-2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
Transformation monoid of an automaton

Relations:

\begin{align*}
    aa &= a \\
    ac &= a \\
    ba &= a \\
    bb &= b \\
    cb &= bc \\
    cc &= c \\
    abc &= ab \\
    bca &= ca \\
    cab &= bc \\
\end{align*}

The end!
Recognizing by a morphism

**Definition**

Let $M$ be a monoid and let $L$ be a language of $A^*$. Then $M$ recognizes $L$ if there exists a monoid morphism $\varphi : A^* \to M$ and a subset $P$ of $M$ such that $L = \varphi^{-1}(P)$.

**Proposition**

A language is recognized by a finite monoid iff it is recognized by a finite deterministic automaton.
Syntactic monoid

**Definition (algorithmic)**
The **syntactic monoid** of a language is the transition monoid of its **minimal** automaton.

**Definition (algebraic)**
The **syntactic monoid** of a language $L \subset A^*$ is the quotient monoid of $A^*$ by the syntactic congruence of $L$: $u \sim_L v$ iff, for each $x, y \in A^*$, $xvy \in L \iff xuy \in L$.
The wreath product principle

The wreath product $N \circ K$ of two monoids $N$ and $K$ is defined on the set $N^K \times K$ by the following product:

$$(f_1, k_1)(f_2, k_2) = (f, k_1k_2) \text{ with } f(k) = f_1(k)f_2(kk_1)$$

Straubing’s wreath product principle provides a description of the languages recognized by the wreath product of two automata (or monoids).
Proposition

Let $M$ and $N$ be monoids. Every language of $A^*$ recognized by $M \circ N$ is a finite union of languages of the form $U \cap \sigma_\varphi^{-1}(V)$, where $\varphi : A^* \to N$ is a monoid morphism, $U$ is a language of $A^*$ recognized by $\varphi$ and $V$ is a language of $B_N^*$ recognized by $M$. 
Theorem

Let $L \subseteq A^*$ be a language recognized by an wreath product of the form $(P, Q \times A) \circ (Q, A)$. Then $L$ is a finite union of languages of the form $W \cap \sigma^{-1}(V)$, where $W \subseteq A^*$ is recognized by $(Q, A)$, $\sigma$ is a $C$-sequential function associated with the action $(Q, A)$ and $V \subseteq (Q \times A)^*$ is recognized by $(P, Q \times A)$. 
