Extending the Lyndon-Schützenberger Theorem

SOGMSC 2016

Taylor J. Smith

Joint work with Jeffrey Shallit

David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, Canada

June 14, 2016

Table of Contents

SOGMSC 2016

Table of Contents

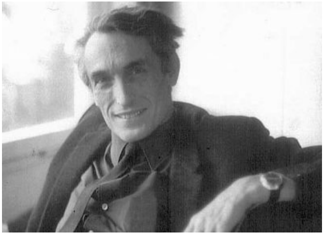
Background

- Combinatorics on words is the branch of mathematics that focuses on combinations, sequences, and patterns of symbols.
- By investigating properties of words, we get many useful applications (e.g. pattern matching).
- Most of the time, we only consider words in one dimension.
- What happens to some of these properties if we introduce a second dimension?

Background

- The **Lyndon-Schützenberger theorem** defines a set of conditions for when the concatenation of two words x and y commutes; that is, when $xy = yx$.
- This theorem is one of the most well-known results in the field of combinatorics on words. (For a proof, see the paper by Lyndon and Schützenberger.)

R. Lyndon



M.-P. Schützenberger

Table of Contents

1D Preliminaries

- A **symbol** is a primitive, atomic unit, such as a letter. A nonempty set of symbols is called an **alphabet**.
- A **word** (or string) is a combination of symbols.
- A **language** is a set of words.
- Given a word w, we can take the n-th **power** of w, written w^n, by repeating w a total of n times.

1D Preliminaries

- A **symbol** is a primitive, atomic unit, such as a letter. A nonempty set of symbols is called an **alphabet**.
- A **word** (or string) is a combination of symbols.
- A **language** is a set of words.
- Given a word w, we can take the n-th **power** of w, written w^n, by repeating w a total of n times.

Example

Given the alphabet $\Sigma = \{\mathtt{a}, \mathtt{c}, \mathtt{t}\}$, we can form the word $w = \mathtt{cat}$ and the language $L = \{\mathtt{at},\ \mathtt{act},\ \mathtt{cat},\ \mathtt{tac}\}$.

1D Lyndon-Schützenberger Theorem

Theorem (1D Lyndon-Schützenberger Theorem)

Let $x, y \in \Sigma^+$. Then the following three conditions are equivalent:

1. $xy = yx$;
2. *There exist $z \in \Sigma^+$ and integers $k, l > 0$ such that $x = z^k$ and $y = z^l$;*
3. *There exist integers $i, j > 0$ such that $x^i = y^j$.*

1D Lyndon-Schützenberger Theorem

SOGMSC 2016

Theorem (1D Lyndon-Schützenberger Theorem)

Let $x, y \in \Sigma^+$. Then the following ***five*** *conditions are equivalent:*

1. $xy = yx$;
2. *There exist $z \in \Sigma^+$ and integers $k, l > 0$ such that $x = z^k$ and $y = z^l$;*
3. *There exist integers $i, j > 0$ such that $x^i = y^j$;*
4. ***There exist integers $r, s > 0$ such that $x^r y^s = y^s x^r$;***
5. $\boldsymbol{x\{x, y\}^* \cap y\{x, y\}^* \neq \emptyset}$.

3. There exist integers $i, j > 0$ such that $x^i = y^j$.

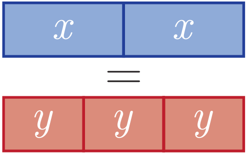
$\Downarrow$

4. There exist integers $r, s > 0$ such that $x^r y^s = y^s x^r$.

Proof.

If $x^i = y^j$, then comparing prefixes and suffixes reveals that $x^i y^j = y^j x^i$.

Take $r = i$ and $s = j$ to get $x^r y^s = y^s x^r$. $\square$



3. There exist integers $i, j > 0$ such that $x^i = y^j$.

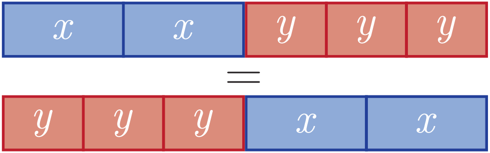
$\Downarrow$

4. There exist integers $r, s > 0$ such that $x^r y^s = y^s x^r$.

Proof.

If $x^i = y^j$, then comparing prefixes and suffixes reveals that $x^i y^j = y^j x^i$.

Take $r = i$ and $s = j$ to get $x^r y^s = y^s x^r$. □



1D Lyndon-Schützenberger Theorem

4. There exist integers $r, s > 0$ such that $x^r y^s = y^s x^r$.

$\Downarrow$

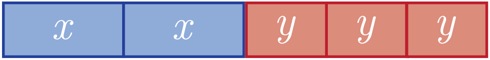
5. $x\{x, y\}^* \cap y\{x, y\}^* \neq \emptyset$.

Proof.

Let $z = x^r y^s$. Then $z \in x\{x, y\}^*$.

By condition 4, we know that $z = y^s x^r$, so $z \in y\{x, y\}^*$.

Therefore, $x\{x, y\}^* \cap y\{x, y\}^* \neq \emptyset$. $\square$

$z =$ 

1D Lyndon-Schützenberger Theorem

4. There exist integers $r, s > 0$ such that $x^r y^s = y^s x^r$.

$\Downarrow$

5. $x\{x, y\}^* \cap y\{x, y\}^* \neq \emptyset$.

Proof.

Let $z = x^r y^s$. Then $z \in x\{x, y\}^*$.

By condition 4, we know that $z = y^s x^r$, so $z \in y\{x, y\}^*$.

Therefore, $x\{x, y\}^* \cap y\{x, y\}^* \neq \emptyset$. $\square$

1D Lyndon-Schützenberger Theorem

4. There exist integers $r, s > 0$ such that $x^r y^s = y^s x^r$.

$\Downarrow$

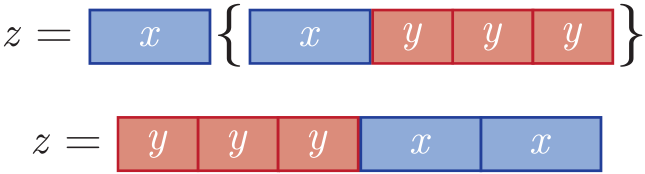
5. $x\{x, y\}^* \cap y\{x, y\}^* \neq \emptyset$.

Proof.

Let $z = x^r y^s$. Then $z \in x\{x, y\}^*$.

By condition 4, we know that $z = y^s x^r$, so $z \in y\{x, y\}^*$.

Therefore, $x\{x, y\}^* \cap y\{x, y\}^* \neq \emptyset$. $\square$



1D Lyndon-Schützenberger Theorem

SOGMSC 2016

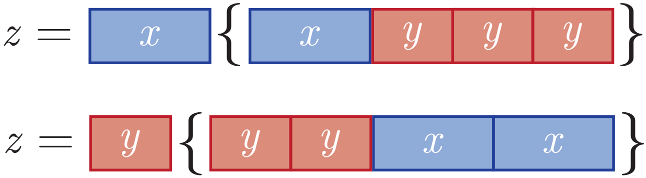
4. There exist integers $r, s > 0$ such that $x^r y^s = y^s x^r$.

$\Downarrow$

5. $x\{x, y\}^* \cap y\{x, y\}^* \neq \emptyset$.

Proof.

Let $z = x^r y^s$. Then $z \in x\{x, y\}^*$.
By condition 4, we know that $z = y^s x^r$, so $z \in y\{x, y\}^*$.
Therefore, $x\{x, y\}^* \cap y\{x, y\}^* \neq \emptyset$. $\square$



5. $x\{x, y\}^* \cap y\{x, y\}^* \neq \emptyset$.

$\Downarrow$

1. $xy = yx$.

Proof.

By induction on $|xy|$.

- Both the base case ($|xy| = 2$) and the case where $|x| = |y|$ are trivial.

1D Lyndon-Schützenberger Theorem

5. $x\{x,y\}^* \cap y\{x,y\}^* \neq \emptyset$.

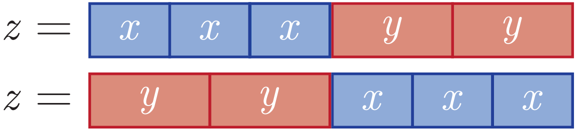
$\Downarrow$

1. $xy = yx$.

Proof.

By induction on $|xy|$.

- Without loss of generality, assume $|x| < |y|$.
  Let z be as before. Since $z \in x\{x,y\}^*$ and $z \in y\{x,y\}^*$ by condition 5, we know x is a proper prefix of y.



1D Lyndon-Schützenberger Theorem

SOGMSC 2016

5. $x\{x, y\}^* \cap y\{x, y\}^* \neq \emptyset$.

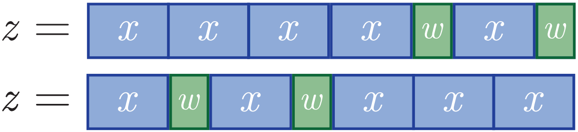
$\Downarrow$

1. $xy = yx$.

Proof.

By induction on $|xy|$.

- Let $y = xw$. Then z has the prefixes xx and xw, so $x^{-1}z \in x\{x, w\}^*$ and $x^{-1}z \in w\{x, w\}^*$. Thus, $x\{x, w\}^* \cap w\{x, w\}^* \neq \emptyset$.
  By induction, condition 1 holds for x and w, so $xw = wx$ and therefore $yx = (xw)x = x(wx) = xy$. □



1D Lyndon-Schützenberger Theorem

SOGMSC 2016

5. $x\{x,y\}^* \cap y\{x,y\}^* \neq \emptyset$.

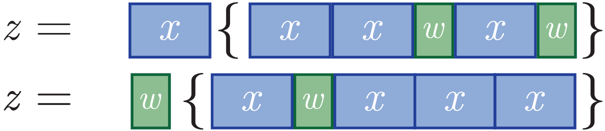
$\Downarrow$

1. $xy = yx$.

Proof.

By induction on $|xy|$.

- Let $y = xw$. Then z has the prefixes xx and xw, so $x^{-1}z \in x\{x,w\}^*$ and $x^{-1}z \in w\{x,w\}^*$. Thus, $x\{x,w\}^* \cap w\{x,w\}^* \neq \emptyset$.
  By induction, condition 1 holds for x and w, so $xw = wx$ and therefore $yx = (xw)x = x(wx) = xy$. □



1D Lyndon-Schützenberger Theorem

5. $x\{x,y\}^* \cap y\{x,y\}^* \neq \emptyset$.

$\Downarrow$

1. $xy = yx$.

Proof.

By induction on $|xy|$.

- Let $y = xw$. Then z has the prefixes xx and xw, so $x^{-1}z \in x\{x,w\}^*$ and $x^{-1}z \in w\{x,w\}^*$. Thus, $x\{x,w\}^* \cap w\{x,w\}^* \neq \emptyset$.
  By induction, condition 1 holds for x and w, so $xw = wx$ and therefore $yx = (xw)x = x(wx) = xy$. □

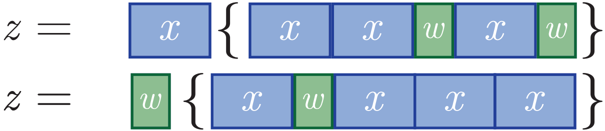


Table of Contents

2D Preliminaries

- We consider a **two-dimensional word** to be an array of symbols from some alphabet Σ.
- $\Sigma^{m \times n}$ is the set of all $m \times n$ rectangular arrays M of elements chosen from Σ.
- If $M \in \Sigma^{m \times n}$, then $M^{p \times q}$ is the $pm \times qn$ rectangular array constructed by repeating M in p rows and q columns.

- We consider a **two-dimensional word** to be an array of symbols from some alphabet Σ.
- $\Sigma^{m\times n}$ is the set of all $m \times n$ rectangular arrays M of elements chosen from Σ.
- If $M \in \Sigma^{m\times n}$, then $M^{p\times q}$ is the $pm \times qn$ rectangular array constructed by repeating M in p rows and q columns.

Example

If $M = \begin{bmatrix} \mathtt{a} & \mathtt{b} \\ \mathtt{c} & \mathtt{d} \end{bmatrix}$, then $M^{2\times 3} = \begin{bmatrix} \mathtt{a} & \mathtt{b} & \mathtt{a} & \mathtt{b} & \mathtt{a} & \mathtt{b} \\ \mathtt{c} & \mathtt{d} & \mathtt{c} & \mathtt{d} & \mathtt{c} & \mathtt{d} \\ \mathtt{a} & \mathtt{b} & \mathtt{a} & \mathtt{b} & \mathtt{a} & \mathtt{b} \\ \mathtt{c} & \mathtt{d} & \mathtt{c} & \mathtt{d} & \mathtt{c} & \mathtt{d} \end{bmatrix}$.

2D Preliminaries

- We can **concatenate** two arrays A and B, but we must insist on a matching of dimension.
- If A is $m \times n_1$ and B is $m \times n_2$, then $A \varobar B$ is the $m \times (n_1 + n_2)$ array obtained by placing B to the right of A.
- If A is $m_1 \times n$ and B is $m_2 \times n$, then $A \ominus B$ is the $(m_1 + m_2) \times n$ array obtained by placing B beneath A.

2D Preliminaries

- We can **concatenate** two arrays A and B, but we must insist on a matching of dimension.
- If A is $m \times n_1$ and B is $m \times n_2$, then $A \oplus B$ is the $m \times (n_1 + n_2)$ array obtained by placing B to the right of A.
- If A is $m_1 \times n$ and B is $m_2 \times n$, then $A \ominus B$ is the $(m_1 + m_2) \times n$ array obtained by placing B beneath A.

Example

If $A_1 = \begin{bmatrix} \mathtt{a} & \mathtt{b} \end{bmatrix}$ and $B_1 = \begin{bmatrix} \mathtt{c} & \mathtt{d} \end{bmatrix}$, then $A_1 \ominus B_1 = \begin{bmatrix} \mathtt{a} & \mathtt{b} \\ \mathtt{c} & \mathtt{d} \end{bmatrix}$.

Example

If $A_2 = \begin{bmatrix} \mathtt{a} & \mathtt{b} \\ \mathtt{d} & \mathtt{e} \end{bmatrix}$ and $B_2 = \begin{bmatrix} \mathtt{c} \\ \mathtt{f} \end{bmatrix}$, then $A_2 \oplus B_2 = \begin{bmatrix} \mathtt{a} & \mathtt{b} & \mathtt{c} \\ \mathtt{d} & \mathtt{e} & \mathtt{f} \end{bmatrix}$.

2D Lyndon-Schützenberger Theorem

Theorem (2D Lyndon-Schützenberger Theorem)

Let A and B be nonempty arrays. Then the following three conditions are equivalent:

1. *There exist positive integers p_1, p_2, q_1, q_2 such that* $A^{p_1 \times q_1} = B^{p_2 \times q_2}$*;*
2. *There exist a nonempty array C and positive integers r_1, r_2, s_1, s_2 such that* $A = C^{r_1 \times s_1}$ *and* $B = C^{r_2 \times s_2}$*;*
3. *There exist positive integers t_1, t_2, u_1, u_2 such that* $A^{t_1 \times t_2} \circ B^{u_1 \times u_2} = B^{u_1 \times u_2} \circ A^{t_1 \times t_2}$ *where $\circ$ can be $\varobar$ or $\ominus$.*

Remark

- Conditions 1, 2, and 3 in the 2D version correspond to conditions 3, 2, and 4, respectively, in the 1D version.
- Here, we prove $2 \Rightarrow 1$ and $2 \Rightarrow 3$. (Other directions omitted.)

2. There exist a nonempty array C and positive integers r_1, r_2, s_1, s_2 such that $A = C^{r_1 \times s_1}$ and $B = C^{r_2 \times s_2}$.

$\Downarrow$

1. There exist positive integers p_1, p_2, q_1, q_2 such that $A^{p_1 \times q_1} = B^{p_2 \times q_2}$.

Proof.

Let $p_1 = r_2$, $p_2 = r_1$, $q_1 = s_2$, and $q_2 = s_1$. Then

$$\begin{aligned} A^{p_1 \times q_1} &= (C^{r_1 \times s_1})^{p_1 \times q_1} \\ &= C^{p_1 r_1 \times q_1 s_1} \\ &= C^{r_2 p_2 \times s_2 q_2} \\ &= (C^{r_2 \times s_2})^{p_2 \times q_2} \\ &= B^{p_2 \times q_2}. \end{aligned}$$

□

2. There exist a nonempty array C and positive integers r_1, r_2, s_1, s_2 such that $A = C^{r_1 \times s_1}$ and $B = C^{r_2 \times s_2}$.

$\Downarrow$

3. There exist positive integers t_1, t_2, u_1, u_2 such that $A^{t_1 \times t_2} \circ B^{u_1 \times u_2} = B^{u_1 \times u_2} \circ A^{t_1 \times t_2}$ where $\circ$ can be $\varobar$ or $\ominus$.

Proof.

Assume the operation is $\varobar$. (The proof is similar for $\ominus$.) Let $t_1 = r_2$, $t_2 = r_1$, $u_1 = s_2$, and $u_2 = s_1$. Then

$$\begin{aligned} A^{t_1 \times u_1} \varobar B^{t_2 \times u_2} &= (C^{r_1 \times s_1})^{t_1 \times u_1} \varobar (C^{r_2 \times s_2})^{t_2 \times u_2} \\ &= C^{r_1 t_1 \times s_1 u_1} \varobar C^{r_2 t_2 \times s_2 u_2} \\ &\vdots \\ &= C^{r_2 t_2 \times s_2 u_2} \varobar C^{r_1 t_1 \times s_1 u_1} \\ &= (C^{r_2 \times s_2})^{t_2 \times u_2} \varobar (C^{r_1 \times s_1})^{t_1 \times u_1} \\ &= B^{t_2 \times u_2} \varobar A^{t_1 \times u_1}. \end{aligned}$$

□

2D Lyndon-Schützenberger Theorem

- What does this theorem give us?
  - Conditions to check for and to match patterns in large arrays.
  - An algorithm to determine the primitivity or periodicity of a given array.
  - An algorithm to find the "primitive root" of a given array.
- For details, see our paper!

$A^{m \times n} =$

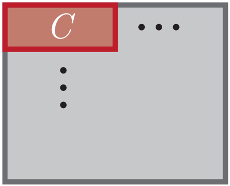


Table of Contents

SOGMSC 2016

Conclusions

- The one-dimensional version of the Lyndon-Schützenberger theorem admits two new equivalent conditions.
- There exists an analogous two-dimensional version of the Lyndon-Schützenberger theorem that is remarkably similar to the one-dimensional case.
- This two-dimensional version of the theorem allows us to investigate many useful properties of two-dimensional words.

Future Work

- Is there a two-dimensional analogue to conditions 1 and 5 of the one-dimensional Lyndon-Schützenberger theorem?
- Do higher-dimensional analogues (e.g. 3D) of this theorem exist? What information can we gain from these analogues?

References

[1] R. C. Lyndon and M.-P. Schützenberger. The equation $a^M = b^N c^P$ in a free group. *Mich. Math. J.*, 9(4):289–298, 1962.

[2] J. Shallit and T. J. Smith. Periodicity in rectangular arrays. arXiv:1602.06915.