# Alternative Versions of the Lyndon-Schützenberger Theorems

In what follows, $\Sigma$ is always a finite alphabet.

## 1 Second theorem of Lyndon-Schützenberger

A more general version of the second Lyndon-Schützenberger theorem can be stated as follows:

**Theorem 1.** *Let $x, y \in \Sigma^+$. Then the following five conditions are equivalent:*

*(1) $xy = yx$;*

*(2) There exist $z \in \Sigma^+$ and integers $k, \ell > 0$ such that $x = z^k$ and $y = z^\ell$;*

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

*(6) $x\{x, y\}^\omega \cap y\{x, y\}^\omega \neq \emptyset$.*

*Proof.* Let us prove (2) $\implies$ (3) $\implies$ (1) $\implies$ (4) $\implies$ (5) $\implies$ (6) $\implies$ (2).

(2) $\implies$ (3): Take $i = \ell$ and $j = k$. Then $x^i = (z^k)^i = (z^i)^k = (z^\ell)^k = y^k = y^j$.

(3) $\implies$ (1): Without loss of generality, assume $|x| \leq |y|$. Then there exists $w$ such that $y = xw$. Hence $x^i = y^j = (xw)^j = x(wx)^{j-1}w$. Cancelling $x$ on the left of both sides of the equation gives $x^{i-1} = (wx)^{j-1}w$; then multiplying on the right by $x$ gives $x^i = (wx)^j$. Hence $(xw)^j = (wx)^j$, and hence $xw = wx$. So $y = xw = wx$ and $yx = (xw)x = x(wx) = xy$.

(1) $\implies$ (4): Take $r = s = 1$.

(4) $\implies$ (5): Let $z = x^r y^s$. Then by (4) we have $z = y^s x^r$. So $z = x(x^{r-1}y^s)$ and $z = y(y^{s-1}x^r)$. So $z \in x\{x, y\}^* \cap y\{x, y\}^*$.

(5) $\implies$ (6): Since $x\{x, y\}^* \cap y\{x, y\}^* \neq \emptyset$, that means there is a $z$ in the intersection that can be written both as $xz_1$ and $yz_2$, where $z_1, z_2 \in \{x, y\}^*$. Hence $z^\omega \in x\{x, y\}^\omega \cap y\{x, y\}^\omega$.

(6) $\implies$ (2): By induction on the length of $|xy|$. The base case is $|xy| = 2$. More generally, if $|x| = |y|$ then clearly (6) implies $x = y$ and so (2) holds with $z = x = y$ and $k = \ell = 1$. Otherwise without loss of generality $|x| < |y|$. Suppose $\mathbf{t} \in x\{x, y\}^\omega$ and $\mathbf{t} \in y\{x, y\}^\omega$. Then $x$ is a proper prefix of $y$, so write $y = xw$ for a nonempty word $w$. Then $\mathbf{t}$ has prefix $xx$ and also prefix $xw$. Thus $x^{-1}\mathbf{t} \in x\{x, w\}^\omega$ and $x^{-1}\mathbf{t} \in w\{x, w\}^\omega$, where by $x^{-1}\mathbf{t}$ we mean remove the prefix $x$ from $\mathbf{t}$. So $x\{x, w\}^\omega \cap w\{x, w\}^\omega \neq \emptyset$. Now $|xw| = |y| < |xy|$, so the induction hypothesis applies to $x$ and $w$. Thus there exist a word $z$ and integers $k, \ell > 0$ such that $x = z^k$ and $w = z^\ell$. So $y = xw = z^{k+\ell}$. □

# 2 First theorem of Lyndon-Schützenberger

A variant of the first theorem of Lyndon-Schützenberger is the following:

**Theorem 2.** *Let $z \in \Sigma^+$. Then the following are equivalent:*

*(1) There exists $p \in \Sigma^+$ such that $p$ is both a proper prefix and suffix of $z$;*

*(2) There exist $u \in \Sigma^+, v \in \Sigma^*$ and an integer $e \geq 1$ such that $z = (uv)^e u$;*

*(3) There exist $s \in \Sigma^+, t \in \Sigma^*$ such that $z = sts$;*

*(4) There exist $q \in \Sigma^+, r \in \Sigma^*$ such that $qr$ is a proper prefix of $z$, and $qrz = zrq$;*

*(5) There exist $e \in \Sigma^+, f \in \Sigma^*$ such that $fe$ is a proper suffix of $z$, and $efz = zfe$;*

*(6) There exist $w \in \Sigma^+$ that is a proper prefix of $z$ and $x \in \Sigma^*$ and an integer $i \geq 2$ such that $zx = w^i$;*

*(7) There exist $g \in \Sigma^+$ that is a proper suffix of $z$ and $h \in \Sigma^*$ and an integer $j \geq 2$ such that $hz = g^j$.*

*Proof.* We will prove (1) $\implies$ (2) $\implies$ (3) $\implies$ (4) $\implies$ (6) $\implies$ (1). The implications (3) $\implies$ (5) $\implies$ (7) $\implies$ (1) are symmetric to these and are left to the reader.

(1) $\Rightarrow$ (2): Suppose $p$ is a proper prefix and suffix of $z$. Then there exist $\alpha, \beta \in \Sigma^+$ such that $z = p\alpha = \beta p$. We prove, by induction on $|p|$, that the equality $p\alpha = \beta p$ implies that there exist $u \in \Sigma^+, v \in \Sigma^*$ such that $p = (uv)^{e-1}u$ for some $e \geq 1$, and $\alpha = vu$, and $\beta = uv$.

The base case is $|p| = 1$. Then $z = p\gamma p$ for some $\gamma \in \Sigma^*$. Take $e = 1$, $u = p$, and $v = \gamma$ to get $p = u$, $\alpha = vu$, $\beta = uv$, and $z = (uv)^e u$.

Now suppose $|p| > 1$. Write $z = p\alpha = \beta p$. There are two cases:

- If $|\alpha| \geq |p|$ then there exists $\delta \in \Sigma^*$ such that $\beta = p\delta$ and $\alpha = \delta p$. Once again, take $e = 1$, $u = p$, and $v = \delta$ to get $p = u$, $\alpha = vu$, $\beta = uv$, and $z = (uv)^e u$.

- If $|\alpha| < |p|$, then there exists $\delta \in \Sigma^+$ such that $p = \delta\alpha = \beta\delta$. Now $0 < |\delta| = |p| - |\beta| < |p|$, so we can apply induction to the equality $\delta\alpha = \beta\delta$. This gives us $u \in \Sigma^+$, $v \in \Sigma^*$, and an integer $e \geq 1$ such that $\alpha = vu$, $\beta = uv$, and $p = (uv)^e u$. Hence $z = p\alpha = (uv)^e vu = (uv)^{e+1}vu$.

(2) $\Rightarrow$ (3): We know that $z = (uv)^e u = uv(uv)^{e-1}u$ for some $e \geq 1$. Take $s = u$ and $t = v(uv)^{e-1}$. Since $u$ is nonempty, then $s$ is nonempty, and $z = sts$.

(3) $\Rightarrow$ (4): We know that $z = sts$. Take $q = s$ and $r = t$. Then $qrz = ststs = zrq$. Since $q$ is nonempty, $qr$ is a proper prefix of $z$.

(4) $\Rightarrow$ (6): Multiply the equality $qrz = zrq$ on the right by $r$ to get $(qr)(zr) = (zr)(qr)$. By the second Lyndon-Schützenberger theorem, we get that there exists $\zeta \in \Sigma^*$ and integers $k, \ell > 0$ such that $qr = \zeta^k$ and $zr = \zeta^\ell$. Now take $w = \zeta$ and $x = r$ and $i = \ell$. We have $|w| = |\zeta| \leq |qr| < |z|$, so $w$ is a prefix of $q$ and hence a proper prefix of $z$. Then $zx = zr = \zeta^\ell = w^i$. Since $qr = \zeta^k$ is a proper prefix of $z$, it is also a proper prefix of $zr = \zeta^\ell$. So $k < \ell$. Since $k \geq 1$, we have $i = \ell \geq 2$.

(6) $\Rightarrow$ (1): Choose $m < i$ such that $m|w| < |z| \leq (m+1)|z|$. Since $w$ is a proper prefix of $z$, we know that $m \geq 1$. Write $z = w^m p$; since $z$ is a prefix of $w^i$, it follows that $p$ is a prefix of $w$ and hence a prefix of $z$. Furthermore, $p$ is nonempty since $|z| > m|w|$. So $p$ is both a proper prefix and suffix of $z$. $\square$