Commuting and conjugate words

Definition. We say that nonempty words x and y are conjugate, if there are words u and v such that $x = uv$ and $y = vu$.

Theorem. Let $u, v \in \Sigma^+$. The following conditions are equivalent:

(a) $uv = vu$,
(b) $u^i = v^j$ for some $i, j \in \mathbb{N}$,
(c) $u = t^k$ and $v = t^\ell$ for some $t \in \Sigma^+$ and some $k, \ell \in \mathbb{N}$.

Proof. (a) $\Longrightarrow$ (c) If $|u| = |v|$, then $t = u = v$ and $k = \ell = 1$. Proceed by induction on $|uv|$. If $|uv| = 2$, then $|u| = |v| = 1$ and we are done. Assume WLOG, that $|u| < |v|$, and let $w = u^{-1}v$. Then $uuw = uwu$, thus $uw = wu$. By the induction assumption, we have $u = t^k$ and $w = t^{\ell'}$ for some t and some $k, \ell' \in \mathbb{N}$. Then $v = uw = t^{k+\ell}$.

(c) $\Longrightarrow$ (b) It is enough to take $i = \ell$ and $j = k$.

(b) $\Longrightarrow$ (a) If $|u| = |v|$, then also $u = v$ and $uv = vu$. Assume, again WLOG, that $|u| < |v|$ and $v = uw$. Then $v^j = (uw)^j = u^i = u^{-1}u^i u = (wu)^j$, and thus $uw = wu$. Then also $vu = uwu = uuw = uv$. □

Corollary. Every nonempty word is a power of a unique primitive word t.

The word t from the previous claim is called the *primitive root* of w. The theorem can be significantly generalized by the following lemma.

Lemma. Let $uv \neq vu$. Denote $z = uv \wedge vu$. Then $z = uw_1 \wedge vw_2$ for any words $w_1, w_2 \in \langle u, v \rangle$ such that $|uw_1| \geq |z|$ and $|vw_2| \geq |z|$.

Proof. Let $za \leq uv$ and $zb \leq vu$, where a, b are letters. It is enough to show, that $za \leq u^i v$ and $zb \leq v^i u$ for each $i \in \mathbb{N}$. This is obvious for $i = 1$. Proceed by induction. By induction assumption, the word $u^{i+1}v$ has a prefix uz, which is also a prefix of uvu. Thus all three words have a common prefix of length $|z|+1$, namely za as one can see using uvu. Similarly we can show $zb \leq v^i u$. □

Example. *Let $u = aaba$ and $v = aab$. Then $z = uv \wedge vu = aabaa$. Note that z can be longer than both u and v.*

Corollary. If words u and v satisfy a nontrivial relation, then they commute.

For three words, there is no upper bound on the length of the common prefix of differently formed words. Consider, for instance, the words $x = ab$, $y = aba$ a $z = baa$. Then $xy^\omega = yz^\omega$. Observe, moreover, that x, y, z form a code. Therefore, words with no finite relation can satisfy an infinite relation. For three words, however, such a relation is known to be at most one.

We can also observe that conjugate words x, y satisfy a "both sides infinite" relation: $x^{\mathbb{Z}}$ a $y^{\mathbb{Z}}$ are the same sequences up to a shift.

For words $x = aba$, $y = b$ we have still another situation. The sequence $(xy)^{\mathbb{Z}}$ is equal to itself by a nontrivial shift by two letters.

Theorem. Let the words x and y be conjugate.

(a) The word x is primitive iff y is primitive.
(b) The primitive roots of x and y are conjugate.
(c) There is a unique pair of words $(t_1, t_2) \in \Sigma^+ \times \Sigma^*$ such that $t_1 t_2$ is the primitive root of x and $t_2 t_1$ is the primitive word of y.

Proof. Let $x = uv = t^i$, where t is the primitive root of uv and $y = vu$. Then there is a nonempty prefix t_1 of t and an exponent $0 \le j < i$ such that $u = t^j t_1$ and $v = t_2 t^{i-j-1}$, where $t_2 = t_1^{-1}u$. Then $y = (t_2t_1)^i$. Similarly, we obtain $x = (s_2s_1)^{i'}$, where $s = s_1s_2$ is a primitive root of y and $y = s^{i'}$. The theorem about commutation implies $i = i'$ and $s = t_2t_1$, which proves (a) and (b).

Let now $t = t_1't_2'$ and $s = t_2't_1'$. Assume WLOG that $|t_1| \le |t_1'|$. Then $t_1' = t_1r$ and $t_2 = rt_2'$ for some r. We get $rs = rt_2't_1' = t_2t_1' = t_2t_1r = sr$. Since r is shorter than the primitive root of s and $sr = rs$, we conclude that r is empty, proving (c). □

The following theorem is an equivalent characterization of conjugacy.

Theorem. The words x, y, z satisfy $zx = yz$ iff x and y are conjugate and $z \in t_2(t_1t_2)^*$, where $(t_1, t_2) \in \Sigma^+ \times \Sigma^*$ is a pair such that t_1t_2 is the primitive root of x and t_2t_1 is the primitive root of y.

Proof. We prove the “only if” by induction on the length of z. Suppose, first, that $0 \le |z| < |y|$. Then $y = zz'$, with $z = t_2(t_1t_2)^j$ and $z' = (t_1t_2)^{j'}t_1$ for some $0 \le j$ and some nonempty suffix t_1 of the primitive root $t = t_2t_1$ of y. Then $zx = zz'z = yz$ and $x = z'z = (t_1t_2)^{j+j'+1}$. The previous theorem implies that t_1t_2 is the primitive root of x.

If $|z| > |y|$, then $z = yz' = z'x$ for $z' = y^{-1}z$. The induction assumption implies $z' \in t_2(t_1t_2)^*$ with $x \in (t_1t_2)^*$, and hence also $z = z'x \in t_2(t_1t_2)^*$.

The “if” part can be easily verified. □