

WORDS AND EQUATIONS

Let $\Theta = \{x_0, x_1, \dots, x_{n-1}\}$ be an alphabet of letters called *unknowns*, and let Σ be a *target* alphabet.

A pair $(L, R) \in \Theta^* \times \Theta^*$ is an *equation* or *relation*, which is *nontrivial* if $L \neq R$. A monoid morphism $\varphi : \Theta^* \rightarrow \Sigma^*$ is a *solution* of (L, R) if $\varphi(L) = \varphi(R)$. We then also say that the words $u_0, u_1, \dots, u_n$, with $u_i := \varphi(x_i)$, *satisfy the relation* (L, R) . We typically speak about an equation when we look for a solution of a given pair (L, R) , and about a relation, when the words u_i are given and we look for pairs (L, R) of which the morphism φ , defined as above, is a solution.

A solution is *non-erasing* if $\varphi(x) \neq \varepsilon$ for each $x \in \Theta$, and it is periodic if there is a word t such that $\varphi(x)$ is a power of t for each $x \in \Theta$.

A word u is *primitive* if $u = t^i$ implies $i = 1$. That is, a word is primitive iff it is not a power of any shorter word. Note also that the empty word is not primitive.

COMMUTING AND CONJUGATE WORDS

Theorem 1. Words $u, v \in \Sigma^*$ satisfy $uv = vu$ iff there is a word $t \in \Sigma^+$, and integers $i, j \in \mathbb{N}$ such that $u = t^i$ and $v = t^j$.

The claim is obvious if at least one of the words is empty. For nonempty words, we prove the following stronger claim.

Theorem 2. Let $u, v \in \Sigma^+$. The following conditions are equivalent:

- (a) $uv = vu$,
- (b) $u^i = v^j$ for some $i, j > 0$,
- (c) $u = t^k$ and $v = t^\ell$ for some $t \in \Sigma^+$ and some $k, \ell \in \mathbb{N}$.

Proof. (a) $\implies$ (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 $u w u = u w u$, thus $u w = w u$. By the induction assumption, we have $u = t^k$ and $w = t^{\ell'}$ for some t and some $k, \ell' \in \mathbb{N}$. Then $v = u w = t^{k+\ell'}$.

(c) $\implies$ (b) Since both u and v are nonempty, we have $\ell, k > 0$, and it is enough to take $i = \ell$ and $j = k$.

(b) $\implies$ (a) If $|u| = |v|$, then also $u = v$ and $uv = vu$. Assume, again WLOG, that $|u| < |v|$ and $v = u w$. Then $v^j = (u w)^j = u^j = u^{-1} u^j u = (u w)^j$, and thus $u w = w u$. Then also $v u = u w u = u w u = u v$. $\square$

Corollary 3. Every nonempty word is a power of a unique primitive word t .

Proof. Every nonempty word is a power of a primitive word by induction on length. If $u = s^i = r^j$ where s and r are primitive, then both s and r are powers of some t , which yields $r = s = t$. $\square$

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 $z = u w_1 \wedge v w_2$ for any words $w_1, w_2 \in \langle u, v \rangle$ such that $|u w_1| \geq |z|$ and $|v w_2| \geq |z|$.

Proof. Let $z a \leq uv$ and $z b \leq vu$, where a, b are letters. It is enough to show, that $z a \leq u^i v$ and $z b \leq v^i u$ 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 $u z$, 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 $zb \leq v^i u$. $\square$

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 4. 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 5. Let $uwv = wv$. Then u , v and w commute. In particular, if w is primitive, then either u or v is empty.

Proof. Since $u \leq_p w$, $v \leq_s w$, and $|uv| = |w|$, we have $w = uv$. From $uwv = wv$, we obtain $uv = vu$. The claim follows considering the common primitive root of the three words. $\square$

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 6. 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 $0 \leq j < i$ such that $u = t^j t_1$ and $v = t_2 t_1^{-j-1}$, where $t_2 = t_1^{-1} u$. Then $y = (t_2 t_1)^i$. Similarly, we obtain $x = (s_2 s_1)^j$, where $s = s_1 s_2$ is the primitive root of y and $y = s^j$. Since the primitive root is unique, s is the primitive root of $t_2 t_1$ and $i \leq j$. Similarly, t is the primitive root of $s_2 s_1$ and $j \leq i$. Therefore $i = j$ and $s = t_2 t_1$, which proves (a) and (b).

Let now $t = t'_1 t'_2$ and $s = t'_2 t'_1$. Assume WLOG that $|t_1| \leq |t'_1|$. Then $t'_1 = t_1 r$ and $t_2 = r t'_2$ for some r . We get $rs = r t'_2 t'_1 = t_2 t'_1 = t_2 t_1 r = sr$. Since r is shorter than the primitive root of s and $sr = rs$, we conclude that r is empty, proving (c). $\square$

The following theorem is an equivalent characterization of conjugacy.

Theorem 7. Let $x, y, z \in \Sigma^*$. Then $xz = zy$ holds if and only if either $x = y = \varepsilon$ or there are words $u, v \in \Sigma^*$ and $i \in \mathbb{N}$ such that $x = uv$, $y = vu$, and $z = (uv)^i u$.

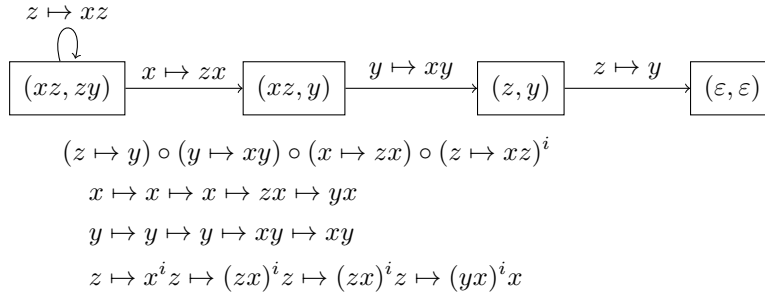
Proof. 1. Assume $xz = zy$.

a) Let $|z| \leq |x|$, and let v be such that $x = zv$. Then $vz = y$, and the claim holds with $i = 0$ and $u = z$.

b) Let $|x| < |z|$, and let $z = xz'$. Then $xz' = z'y$. If $x = \varepsilon$, then also $y = \varepsilon$, and we are done. Otherwise $|z'| < |z|$, and, by induction on $|z|$, there are words u and v and $j \in \mathbb{N}$ such that $x = uv$, $y = vu$, and $z' = (uv)^j u$. Then $z = (uv)^{j+1} u$.

2. The opposite implication is obvious. $\square$

The previous proof can be captured through the following graph of transformations of the equation. If x and y are leading unknowns of left- and right-hand sides of the equation, then there are three possibilities: either $x = yx'$ or $y = xy'$ or $y = x$. We have therefore three transformations to consider. Moreover, with the fresh x' or y' , the apostroph can be omitted, since the old unknown is fully replaced.



Note that if the equation is *quadratic*, which means that it contains at most two occurrences of each unknown, then the length of the equation never increases by the transformation, and the corresponding graph is finite. This means, in particular, that solvability of quadratic equations is decidable. In fact, solvability of word equations is decidable in general, a celebrated result of Makanin (1977), which was subsequently reproved by W. Plandowski (1999), and later by A. Jeř (2012). Due to Plandowski and Jeř, the problem is in PSPACE. It is also NP-hard, and it is an open problem whether it is in NP.

Theorem 8. The words x, y, z satisfy $zx = yz$ iff $x = y = \varepsilon$, or x and y are conjugate and $z \in t_2(t_1 t_2)^*$, where $(t_1, t_2) \in \Sigma^+ \times \Sigma^*$ is a pair such that $t_1 t_2$ is the primitive root of x and $t_2 t_1$ is the primitive root of y .

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

If $|z| > |y|$, then $z = yz' = z'x$ for $z' = y^{-1}z$. The induction assumption implies $z' \in t_2(t_1 t_2)^*$ with $x \in (t_1 t_2)^*$, and hence also $z = z'x \in t_2(t_1 t_2)^*$.

The “if” part can be easily verified. $\square$