Principal solution

If T is a system o equations, let $\mathrm{alph}(T)$ denote the set of unknowns occurring in T. A solution g of T is a mapping $g : \mathrm{alph}(T)^* \to \Sigma^*$. We say that g is *erasing*, if $g(x) = \varepsilon$ for at least one x in the domain. Otherwise g is *nonerasing*. We denote $\mathrm{alph}(g)$ the set of letters that occur in $g(x)$ for at least one x. Even if not stated explicitly, if we speak about a solution g of a system T, then we assume $g : \mathrm{alph}(T)^* \to \mathrm{alph}(g)^*$.

Let $g : \mathrm{alph}(T)^* \to \mathrm{alph}(g)^*$ a $h : \mathrm{alph}(T)^* \to \mathrm{alph}(h)^*$ be two solutions of a system T. We say that h *divides* g, if there is a morphism $\vartheta : \mathrm{alph}(h)^+ \to \mathrm{alph}(g)^+$ such that $g = \vartheta \circ h$.

A solution g of T is called *principal*, if it is minimal in the just defined order of divisibility. In other words, if $g = \vartheta \circ h$, where $\vartheta : \mathrm{alph}(h)^+ \to \mathrm{alph}(g)^+$, and h is a solution of T, then ϑ is a renaming of letters and $h = \vartheta^{-1} \circ g$. We then say that g and h are *associated*, and may be identified. In particular, any renaming of letters is associated with identity.

Note that we can obtain a non-principal solution $h = \vartheta \circ g$ from a principal solution g if ϑ does not preserve length, but also if it does, but it is not injective (gluing some letters).

We consider two types of *elementary transformations* of a system of equations. The *regular* elementary transformation φ_{xy}, is defined by

$$\varphi_{xy}(z) = \begin{cases} xy, & \text{if } z = y \\ z, & \text{if } z \neq y\,, \end{cases}$$

and the *singular* elementary transformation π_x erases the letter x, that is

$$\pi_x(z) = \begin{cases} \varepsilon, & \text{if } z = x \\ z, & \text{if } z \neq y\,. \end{cases}$$

We say that an elementary transformation φ is *associated* to a system of equations T if either

- $\varphi = \pi_x$, with $x \in \alpha(T)$; or
- $\varphi = \varphi_{xy}$, where $x, y \in \mathrm{alph}(T)$, and $(rxu, ryv) \in T$ or $(ryu, rxv) \in T$ for some words r, u, v.

The mapping $L(g) : x \mapsto |g(x)|$ is called the *length type* of g. If the domain alphabet Θ of g is finite, then $L(g)$ is usually seen as a tuple in $\mathbb{N}^{|\Theta|}$ (which implies that some order on Θ is given).

The principal solution of a given length type can be obtained by successive application of elementary transformations. If $T = \{(u_i, v_i) \mid i \in I\}$, then $\varphi(T)$ denotes the system $\{(\varphi(u_i), \varphi(v_i)) \mid i \in I\}$. The basic idea is formulated in the following lemma.

Lemma. Let $h = h' \circ \varphi : \mathrm{alph}(T)^* \to \mathrm{alph}(h)^*$ be a solution of a system T, where φ is an elementary transformation associated to T. Then h' is a principal solution of $T' = \varphi(T)$ if and only if h is a principal solution of T.

Proof. Assume that h is principal. If $h' = \vartheta \circ g'$, where ϑ is nonerasing and g' is a solution of T', then $h = \vartheta \circ g' \circ \varphi$, where $g = g' \circ \varphi$ is a solution of T. Therefore ϑ is a renaming of letters. We have shown that h' is principal.

To show the direct implication, assume now that h' is principal. Let $h = \vartheta \circ g$, where ϑ is nonerasing and g is a solution of T. The key step of the proof is to show that $g = g' \circ \varphi$ for some g'. For $\varphi = \pi_x$ this obviously holds for g' identity on $\pi_x(T)$. If $\varphi = \varphi_{xy}$ is associated with T, then $h(x) = h'(x) \leq_p h'(xy) = h(y)$. Since g is a solution of T, we have that $g(x)$ and $g(y)$ are prefix comparable, and $h = \vartheta \circ g$ implies $g(x) \leq_p g(y)$. Then g', defined by $g' : y \mapsto g(x)^{-1}g(y)$, satisfies $g = g' \circ \varphi_{xy}$.

Now $h = \vartheta \circ g' \circ \varphi = h' \circ \varphi$, where g' is a solution of T'. For both singular and regular φ this implies $h' = \vartheta \circ g'$. (For $\varphi = \varphi_{xy}$ this follows since φ is invertible in the free group, namely $\varphi^{-1} : y \mapsto x^{-1}y$.) Therefore ϑ is renaming, and we are done. □

Theorem. Let $h : \mathrm{alph}(T)^* \to \Sigma^*$ be a solution of a system T. Then there is a unique (up to association) principal solution g of T and a unique morphism $\vartheta : \mathrm{alph}(g)^+ \to \mathrm{alph}(h)^+$ such that $h = \vartheta \circ g$ and $|\mathrm{alph}(g)| \leq |\mathrm{alph}(T)|$.

Moreover,

- $|\mathrm{alph}(g)| < |\mathrm{alph}(T)|$ if T is nontrivial; and
- g and $L(\vartheta)$ depend on $L(h)$ only (and on T).

Proof. We proceed by induction on

$$|\mathrm{alph}(T)| + \sum_{x \in \mathrm{alph}(T)} |h(x)| \ .$$

First suppose that $h(x) = \varepsilon$ for some x. Then $h = h' \circ \pi_x$, and h' is a solution of $T' = \pi_x(T)$. By induction, and by the the previous lemma, there is a unique principal solution g dividing h, given by $h = \vartheta \circ g = \vartheta \circ g' \circ \pi_h$. Since g' and $L(\vartheta)$ is given by $L(h')$, also g is given by $L(h)$. (Note, in particular, that $h(x) = \varepsilon$ is equivalent to $|h(x)| = 0$.) Moreover, $|\mathrm{alph}(g)| = |\mathrm{alph}(g')| \leq |\mathrm{alph}(T')| < |\mathrm{alph}(T)|$.

Let now h be nonerasing. If T is trivial, then the only principal solution is identity, $|\mathrm{alph}(\mathrm{id})| = |\mathrm{alph}(T)|$, $\vartheta = h$, and $L(\vartheta) = L(h)$.

Let T be nontrivial, and let $(rxu, ryv) \in T$ for some $x, y \in \mathrm{alph}(T)$, $x \neq y$. If $|h(x)| \leq |h(y)|$, then $h(x)$ is a prefix of $h(y)$, and $h = h' \circ \varphi_{xy}$, where h' is defined by $h' : y \mapsto h(x)^{-1}h(y)$. Again, by induction and by the previous lemma, h has a unique principal solution dividing it, namely $h = \vartheta \circ g = \vartheta \circ g' \circ \varphi_{xy}$, where g' is the unique principal solution of $T' = \varphi_{xy}(T)$ dividing h'. Also, g and $L(\vartheta)$ is given by $L(h)$ since $L(h')$ is given by $L(h)$. Note that T' is nontrivial, since φ_{xy} is invertible. Therefore $|\mathrm{alph}(g)| = |\mathrm{alph}(g')| < |\mathrm{alph}(T')| = |\mathrm{alph}(T)|$. □

The proof of the previous theorem actually yields a simple algorithm that computes the principal solution dividing any solution with the given length type. Such a solution is obtained as a composition of elementary transformations, since after a finite number of rounds, we reach a trivial system.