Collect. Math. **46**, 1–2 (1995), 77–81

A precedence theorem for semigroups

Pierre Antoine Grillet

Tulane University, New Orleans, LA 70118, U.S.A.

Dedicated to the memory of P. Dubreil

Abstract

In a finite semigroup, the least element under a precedence order is an idempotent in the kernel.

The reader is referred to [4] for general semigroup concepts.

Precedence orders are defined as follows. When S is a set and $<$ is a total order relation on S, semigroup operations on S can be ordered lexicographically: if $m', m'' : S \times S \longrightarrow S$, then $m' < m''$ in case there exists $a, b \in S$ such that $m'(x,y) = m''(x,y)$ whenever $x < a$, $m'(a,y) = m''(a,y)$ whenever $y < b$, and $m'(a,b) < m''(a,b)$.

If m is a semigroup operation and σ is a permutation of S, the permuted operation and permuted dual operation $m_\sigma, m^*_\sigma : S \times S \longrightarrow S$ are defined by

$$m_\sigma(x,y) = \sigma^{-1}\, m\,(\sigma x, \sigma y), m^*_\sigma(x,y) = \sigma^{-1}\, m\,(\sigma y, \sigma x)$$

for all $x, y \in S$. Thus σ is an isomorphism of $S = (S,m)$ onto $S_\sigma = (S, m_\sigma)$ and an antiisomorphism of S onto $S^*_\sigma = (S, m^*_\sigma)$. Note that $(m_\sigma)_\tau = m_{\sigma\tau}$ and $(m^*_\sigma)_\tau = m^*_{\sigma\tau}$.

A *precedence order* on $S = (S,m)$ is a total order $<$ on S such that $m_\sigma \geq m$ and $m^*_\sigma \geq m$ for every permutation σ of S. (It is not assumed that m and $<$ are compatible.)

Precedence occurs naturally in computer lists of distinct finite semigroups, such as [3], where the elements of S are in a fixed order $<$ and multiplication tables are generated in lexicographic order. A semigroup (S, m) added to the list should not be isomorphic or antiisomorphic to any of the previous semigroups. This means no permutation σ such that $m_\sigma < m$ or $m^*_\sigma < m$; equivalently, the fixed order $<$ on S is a precedence order. This provides abundant finite examples of precedence orders.

Conversely, precedence considerations can be used to greatly reduce computation time in the enumeration of finite semigroups [1].

In general, a precedence order exists on every semigroup $S = (S, m)$ or on the dual (opposite) semigroup S^*; in particular, every commutative semigroup has a precedence order. To see this, let $<$ be any well order on S. Operations on S are then well ordered lexicographically. Hence the set of all m_σ and m^*_σ has a least element. If m_σ is the least element, then $<$ is a precedence order on $S_\sigma \cong S$; ordering S by $\sigma x < \sigma y$ yields a precedence order on S. If m^*_σ is least, there is a similar precedence order on the dual semigroup $S^* \cong S^*_\sigma$.

From this argument we also see that precedence orders exist on both S and S^* if and only if there is an antiautomorphism $S \cong S^*$. Also the number of precedence orders on S (if one exists) equals the number of automorphisms of S.

Our precedence theorem is:

Theorem

In a finite semigroup, the least element e under a precedence order $<$ is an idempotent in the kernel.

The easy part of the Theorem is that e is idempotent. Otherwise $S = (S, m)$ contains an idempotent $f \neq e$. Since $e^2 \neq e$, the transposition $\tau = (e\ f)$ satisfies

$$\tau^{-1}\, m\,(\tau e, \tau e) \;=\; \tau^{-1}(ff) = e < m\,(e, e).$$

Since e is the least element of S, this shows $m_\tau < m$, which cannot happen if $<$ is a precedence order.

The rest of the proof consists of two Lemmas.

Lemma 1

Under a precedence order, $ex \leq x$ for all $x \in S$, and $x \leq y$ implies $ex \leq ey$.

Proof. Assume $ex > x$ for some $x \in S$. Let $a \in S$ be the least such element, so that $ea > a$ and $ex \leq x$ for all $x < a$; in particular, $e < a$. Let $\tau = (a\ ea)$. When $x < a$,

$$\tau^{-1}\, m\,(\tau e, \tau x) \;=\; \tau^{-1}(ex) = ex = m\,(e, x).$$

But

$$\tau^{-1}\, m\,(\tau e, \tau a) \;=\; \tau^{-1}(ea) = a < m\,(e, a).$$

This is the required contradiction.

Similarly, assume that $a < b$ satisfy $ea > eb$. Again $e < a$. Let $\tau = (a\ b)$. If $x < a$, then $ex \leq x < a$ and

$$\tau^{-1}\, m\,(\tau e, \tau x) \;=\; \tau^{-1}(ex) = ex = m\,(e, x).$$

But $eb < ea \leq a$ and

$$\tau^{-1}\, m\,(\tau e, \tau a) \;=\; \tau^{-1}(eb) = eb < m\,(e, a). \;\square$$

Lemma 2

Let $f \neq e$ be idempotent. If $fe = f$ then $ef = e$.

Proof. Assume $f^2 = f \neq e$, $fe = f$, and $ef \neq e$ (so that $e < f$, $e < ef$ under the precedence order). We contradict the finiteness of S by constructing for every $r \geq 1$ a set $A \subseteq S$ with r elements and the following properties, in which c denotes the greatest element of A:

(1) $e \in A$ and $c < f$;
(2) $ea = a < fa$ for all $a \in A$;
(3) let $x \leq c$; if $fx = fa$ for some $a \in A$, then $ex = a$; if $fx \notin fA$ then $ex = fx$.

If $r = 1$, then $A = \{\, e \,\}$ suffices.

Now let $r \geq 1$; assume that $A \subseteq S$ has r elements, greatest element c, and properties (1), (2), and (3). It follows from (2) that A and $fA \subseteq fS$ are disjoint and from (3) that $a \longmapsto fa$ is a bijection of A onto fA (since $fb = fa$ implies $b = eb = a$). Let σ be the product of disjoint transpositions

$$\sigma \;=\; \textstyle\prod_{a \in A}\, (a\ fa)\ .$$

Let $x \leq c$. If $x = a \in A$, then $ex = a$, $\sigma x = fa$, and

$$\sigma^{-1}\, m\,(\sigma e, \sigma x) \;=\; \sigma^{-1}(fa) = a = m\,(e, x).$$

If $x = fa \in fA$ (with $a \in A$), then $ex = a$ by (3) and

$$\sigma^{-1} m(\sigma e, \sigma x) \;=\; \sigma^{-1}(fa) = a = m(e, x).$$

If $x \notin A$, $x \notin fA$, and $fx = fa$ for some $a \in A$, then $ex = a$ and

$$\sigma^{-1} m(\sigma e, \sigma x) \;=\; \sigma^{-1}(fx) = a = m(e, x).$$

If finally $x \notin A$, $x \notin fA$, and $fx \notin fA$, then $fx = ex$ by (3), $fx \notin A$ (otherwise, $fx = ffx \in fA$), and

$$\sigma^{-1} m(\sigma e, \sigma x) \;=\; \sigma^{-1}(fx) = fx = m(e, x).$$

Thus $m_\sigma(e, x) = m(e, x)$ for all $x \leq c$. On the other hand,

$$\sigma^{-1} m(\sigma e, \sigma f) \;=\; \sigma^{-1}(fe) = \sigma^{-1} f = e < m(e, f).$$

Hence there is a least $d \in S$ such that $m_\sigma(e, d) \neq m(e, d)$. By the above, $d > c$. Since $<$ is a precedence order, we have $m_\sigma(e, d) > m(e, d)$; hence $d \neq f$. Thus $c < d < f$, $m_\sigma(e, d) > m(e, d)$, and $m_\sigma(e, x) = m(e, x)$ for all $x < d$.

We show that $A' = A \cup \{ d \}$, which has $r + 1$ elements and greatest element d, has properties (1), (2), and (3). Property (1) is clear.

If $a \in A$, then $d \neq a$ since $a \leq c < d$; $d \neq fa$, otherwise

$$\sigma^{-1} m(\sigma e, \sigma d) \;=\; \sigma^{-1}(fa) = a \leq c = ec \leq m(e, d)$$

by Lemma 1; $fd \neq a$, otherwise $a = fa$; and $fd \neq fa$, otherwise

$$\sigma^{-1} m(\sigma e, \sigma d) \;=\; \sigma^{-1}(fd) = a \leq m(e, d).$$

Thus, d and fd belong neither to A nor to fA.

We now have

$$m_\sigma(e, d) \;=\; \sigma^{-1} m(\sigma e, \sigma d) \;=\; \sigma^{-1}(fd) = fd.$$

Hence $ed < fd$. By Lemma 1, $c = ec \leq ed \leq d$; in fact $c < ed$, otherwise $fd = fed = fc \in fA$. Now assume that $ed < d$. Then

$$\sigma^{-1} m(\sigma e, \sigma(ed)) = m(e, ed) = ed.$$

Since $ed \neq a$ for all $a \in A$ this implies $m(\sigma e, \sigma(ed)) \neq \sigma a = fa$, $\sigma(ed) \neq a$, and $ed \neq fa$, for all $a \in A$. Hence

$$\sigma^{-1} m(\sigma e, \sigma(ed)) = \sigma^{-1}(fed) = \sigma^{-1}(fd) = fd,$$

contradicting $fd > ed$. Therefore $ed = d$. Then $d = ed < fd$ and (2) holds for A'.

Finally let $x \leq d$. If $x = d$, then $fx = fd$ and $ex = d$. Otherwise $x < d$ and $m_\sigma(e, x) = m(e, x)$. If $x = fa$ or $x = a$ for some $a \in A$, then $fx = fa$, $f \cdot \sigma x = fa$,

$$ex \ = \ \sigma^{-1} m(\sigma e, \sigma x) = \sigma^{-1}(f, \sigma x) = a,$$

and (3) holds. We may now assume $x \notin A$ and $x \notin fA$. Then

$$ex \ = \ \sigma^{-1} m(\sigma e, \sigma x) = \sigma^{-1}(fx).$$

Also $fx \neq fd$, otherwise $ex = \sigma^{-1}(fd) = fd > x$, contradicting Lemma 1. If now $fx = fa$ for some $a \in A'$, then $a \in A$ and $ex = \sigma^{-1}(fx) = a$. If $fx \notin fA'$, then $fx \notin A$, since $fx = a \in A$ would imply $ex = \sigma^{-1}(fx) = fa$ and $fx = fex = fa$; consequently $ex = \sigma^{-1}(fx) = fx$. This proves (3). □

Lemma 2 implies that e is a primitive idempotent of S. Then it follows (for instance) from Hall's $\mathcal{J}$-class Theorem [2] that e is in the kernel K of S: since the $\mathcal{J}$-class of e lies above the regular $\mathcal{J}$-class K (under the partial order on $S/\mathcal{J}$), Hall's Theorem implies that e lies above some idempotent of K (under the Rees order); since e is primitive, $e \in K$. This proves our Theorem. □

References

1. P. A. Grillet, Commutative semigroups of order 9, to appear.
2. T. E. Hall, On the natural ordering of $\mathcal{J}$-classes and of idempotents in a regular semigroup, *Glasgow Math. J.* **11** (1970), 167–168.
3. H. Jürgensen, *Annotated tables of semigroups of orders 2 to 6*, Report 231, Dept. of Computer Sci., Univ. Western Ontario, 1990.
4. G. Lallement, *Semigroups and combinatorial applications*, Wiley, New York 1979.