Can. J. Math., Vol. XXXIII, No. 4, 1981, pp. 893–900

THE WORD PROBLEM FOR ORTHOGROUPS

J. A. GERHARD AND MARIO PETRICH

A semigroup which is a union of groups is said to be *completely regular*. If in addition the idempotents form a subsemigroup, the semigroup is said to be *orthodox* and is called an *orthogroup*. A completely regular semigroup S is provided in a natural way with a unary operation of inverse by letting a^{-1} for $a \in S$ be the group inverse of a in the maximal subgroup of S to which a belongs. This unary operation satisfies the identities

(1) $aa^{-1}a = a$

(2) $aa^{-1} = a^{-1}a$

(3) $(a^{-1})^{-1} = a.$

In fact a completely regular semigroup can be defined as a unary semigroup (a semigroup with an added unary operation) satisfying these identities. An orthogroup can be characterized as a completely regular semigroup satisfying the additional identity

(4) $(aa^{-1}bb^{-1})^2 = aa^{-1}bb^{-1}.$

Since the idempotents of a completely regular semigroup S are the elements of the form aa^{-1} for $a \in S$, the identity (4) just states that the product of idempotents is idempotent. The free completely regular semigroup on a set was recently studied by Clifford [**1**].

In this paper we study the free orthogroup on a set X. It is described as a quotient of the free unary semigroup on the same set. Invariants are defined on words (elements of the free unary semigroup) and two words belong to the same class of the quotient if and only if their invariants are equal. In this way we give an algorithm to solve the word problem for free orthogroups in terms of words in the free unary semigroup. Since bands are a special case of orthogroups and the solution of the word problem for free bands is inductive on the number of variables occurring in words (see [**2**]) it is not surprising that the solution of the word problem for orthogroups is also inductive.

Section 1 gives background needed for the paper. In particular it contains a description of the free unary semigroup on X. In Section 2 we give the solution of the word problem for the free orthogroup on the set X, and in Section 3 we construct a model of this semigroup. Section 4

Received January 26, 1980. This research was supported by NSERC of Canada.

contains a description of the free semilattice of groups and Section 5 a description of the free orthocryptogroup (an orthogroup in which $\mathscr{H}$ is a congruence). Both of these are special cases of orthogroups.

1. Preliminaries. The free unary semigroup provides a natural setting for the study of word problems for semigroups with an added unary operation (including groups). Let F be the free semigroup on $X \cup \{(\ ,\ )^{-1}\}$ where (and $)^{-1}$ are two distinct elements not in X. The free unary semigroup on X, $U(X)$, is the smallest subset of F with the following properties,

(i) $X \subseteq U(X)$
(ii) $u \in U(X)$ implies $(u)^{-1} \in U(X)$
(iii) $u, v \in U(X)$ implies $uv \in U(X)$.

For technical reasons it is sometimes convenient to use the free unary monoid $U'(X)$ on X. This is obtained from $U(X)$ by adding the empty word ϕ and defining $\phi w = w\phi = w$ for all $w \in U'(X)$.

LEMMA 1.1. *Let S be an orthogroup. For a, b, $e \in S$ let $D_a = D_b \leqq D_e$ and $e = e^2$ (where for $x \in S$, D_x is the $\mathscr{D}$-class of S containing x). Then $ab = aeb$.*

Proof. Let a, b, e be idempotent. The idempotents of a given $\mathscr{D}$-class form a rectangular band and therefore

$$ab = a[b(ae)b] = abaeb = aeb.$$

For $a, b \in S$ not necessarily idempotent we have

$$ab = aa^{-1}abb^{-1}b = aa^{-1}aebb^{-1}b = aeb.$$

2. The word problem for orthogroups. Our first task is to define the invariants needed to describe the solution of the word problem for free orthogroups. The content $c(w)$ of the word $w \in U(X)$ is the set of variables (elements of X) occurring in w. The reduced word $r(w)$ associated with w is obtained from w by removing all occurrences of $u(u)^{-1}$, for u any word, which occur in w. If w is thought of as representing an element of the free group on X then $r(w)$ is the reduced form of w obtained from the solution of the word problem for free groups.

The start $s(w)$ of the word w is obtained as follows. If w has one variable (if $w = \phi$) let $s(w) = \phi$. Otherwise take the longest left segment of w (thought of as an element of F, the free semigroup on $X \cup \{(\ ,\ )^{-1}\}$) which contains all but one variable of w. The resulting element of F need not be an element of $U(X)$, but if all occurrences of (which are not matched with an occurrence of $)^{-1}$ are dropped, the result is an element of $U(X)$. This element is denoted by $s(w)$. More generally if $A \subseteq X$ and

$w \in U(X)$, let $s_A(w)$ be the longest left segment of w containing all but one of the variables in $c(w) - A$, where unmatched occurrences of (are dropped as in the definition of $s(w)$. In this case $s_A(w) = \phi$ if $|c(w) - A| \leqq 1$. Similarly define the end $e(w)$ to be the longest right segment of w containing all but one variable of w, this time dropping unmatched occurrences of $)^{-1}$, and $e_A(w)$ to be the longest right segment of w containing all but one variable of $c(w) - A$, again dropping unmatched occurrences of $)^{-1}$. Here $e(w)$ or $e_A(w)$ may equal ϕ. We often establish a result for $s(w)$ or $s_A(w)$ and omit the formulation and proof of the corresponding result for $e(w)$ or $e_A(w)$.

Let

$$s^0(w) = w$$
$$s^{k+1}(w) = s(s^k(w)) \quad \text{for all } k \geqq 1.$$

LEMMA 2.1. *For $w \in U(X)$ and $A \subseteq X$, $s_A(w) = s^k(w)$ for some $k \geqq 1$.*

Proof. If $s^k(w) \neq \phi$ then $s^{k+1}(w)$ has one less variable than $s^k(w)$. Let $k \geqq 1$ be the smallest integer such that

$$c(w) - A = c(s^{k-1}(w)) - A.$$

Then $s_A(w) = s^k(w)$.

LEMMA 2.2. *For any $u, w \in U(X)$,*

$$s(uw) = \begin{cases} s(u) \text{ if } c(w) \subseteq c(u) \\ u \cdot s_{c(u)}(w) \text{ if } c(w) \nsubseteq c(u). \end{cases}$$

Proof. If $c(w) \subseteq c(u)$ then clearly $s(uw) = s(u)$. If $c(w) \nsubseteq c(u)$, then the longest left segment of uw which contains all but one variable of uw is $u \cdot s_{c(u)}(w)$ by definition of $s_{c(u)}(w)$.

Definition 2.3. Let $w, w' \in U(X)$. Then $w \sim w'$ if and only if $c(w) = c(w')$, $r(w) = r(w')$, $s(w) \sim s(w')$ and $e(w) \sim e(w')$.

The definition of $\sim$ is by induction on the number of variables. In particular $x^k \sim x^l$ if and only if $k = l$.

THEOREM 2.4. *$U(X)/\sim$ is the free orthogroup on X.*

Proof. The proof that $\sim$ is an equivalence relation is an easy inductive argument. Assume $w \sim w'$. To show $\sim$ is a congruence we must show $wu \sim w'u$ and $uw \sim uw'$ for any $u \in U$ and that $(w)^{-1} \sim (w')^{-1}$. Since $c(w) = c(w')$ it follows that

$$c(wu) = c(w) \cup c(u) = c(w') \cup c(u) = c(w'u)$$

and similarly $c(uw) = c(uw')$. Also since $r(w) = r(w')$ it follows that

$$r(wu) = r(w) \cdot r(u) = r(w') \cdot r(u) = r(w'u)$$

where the product is taken in the free group. Similarly $r(uw) = r(uw')$. It is therefore enough to show that $s(uw) \sim s(uw')$ and $s(wu) \sim s(wu')$ in case $|c(uw)| \geqq 2$.

To show $s(uw) \sim s(uw')$ notice that if $c(w) \subseteq c(u)$ then $s(uw) = s(u) = s(uw')$ by Lemma 2.2 and there is nothing to prove. If $c(w) \nsubseteq c(u)$ then

$$s(uw) = u \cdot s_{c(u)}(w) \quad \text{and} \quad s(uw') = u \cdot s_{c(u)}(w')$$

again by Lemma 2.2. Since $c(w) = c(w')$ it follows by induction that $c(s^j(w)) = c(s^j(w'))$ for all j. By Lemma 2.3,

$$s_{c(u)}(w) = s^k(w) \quad \text{and} \quad s_{c(u)}(w') = s^k(w')$$

for some k. Since $w \sim w'$ it follows by induction that $s^k(w) \sim s^k(w')$ and therefore (again by induction) that

$$s(uw) = u \cdot s^k(w) \sim u \cdot s^k(w') = s(uw').$$

To show that $s(wu) \sim s(w'u)$ notice that if $c(u) \subseteq c(w) = c(w')$ then $s(wu) = s(w) \sim s(w') = s(w'u)$. Otherwise

$$s(wu) = w \cdot s_{c(w)}(u) \quad \text{and} \quad s(w'u) = w' s_{c(w')}(u),$$

(and $c(w) = c(w')$). Now $s_{c(w)}(u)$ has at least one less variable than u and so by induction on the number of variables

$$s(wu) = ws_{c(w)}(u) \sim w' s_{c(w')}(u) = s(w'u).$$

Let $w \sim w'$. The following calculations show that $(w)^{-1} \sim (w')^{-1}$.

$$c((w)^{-1}) = c(w) = c(w') = c((w')^{-1})$$
$$\mathrm{r}((w)^{-1}) = (r(w))^{-1} = (r(w'))^{-1} = r((w')^{-1})$$
$$s((w)^{-1}) = s(w) \sim s(w') = s((w')^{-1}).$$

To show that the unary semigroup $U(X)/\sim$ is an orthogroup we check that the identities (1)–(4) given in the introduction hold. This is equivalent to proving

$$a \sim aa^{-1}a$$
$$aa^{-1} \sim a^{-1}a$$
$$(a^{-1})^{-1} \sim a$$
$$(aa^{-1}bb^{-1})^2 \sim aa^{-1}bb^{-1}$$

for all $a, b \in U(X)$.

If $w \sim w'$ is one of these conditions it is trivial that $c(w) = c(w')$, $r(w) = r(w')$ and $s(w) = s(w')$. Therefore $U(X)/\sim$ is an orthogroup.

To show that $U(X)/\sim$ is the free orthogroup on X we prove that $\sim \subseteq \rho$ for any congruence ρ on $U(X)$ such that $U(X)/\rho$ is an orthogroup. Let $w \sim w'$. Then $c(w) = c(w')$. Since $(U(X)/\rho)/\mathscr{D}$ is a semilattice and the least semilattice congruence on $U(X)$ is obtained by identifying words which have the same content it follows that $\mathscr{D}_w = \mathscr{D}_{w'}$ in $U(X)/\rho$. Since $s(w) \sim s(w')$ and $e(w) \sim e(w')$ we can assume by induction that $s(w)\rho\, s(w')$ and $e(w)\rho\, e(w')$. Also $r(w) = r(w')$. In Lemma 5.1 of [**1**] it is shown that w may be written as $s(w)xw_1ye(w)$ where x and y are variables not in $s(w)$ and $e(w)$ respectively. If $u \in U(X)$ let $u^0 = u(u)^{-1}$. Then

$$w = (s(w)x)^0 w(ye(w))^0.$$

Now $r(w)$ is obtained from w by removing idempotents e, and these idempotents have the property that $D_e \geqq D_w$. Therefore:

$$\begin{aligned} w &= (s(w)x)^0 w(ye(w))^0 \\ &= (s(w)x)^0 r(w)(ye(w))^0 \quad \text{by Lemma 1.1} \\ &\rho (s(w')x)^0 r(w')(ye(w'))^0 \\ &= w'. \end{aligned}$$

3. A model of the free orthogroup. In this section we construct a model of the free orthogroup on the set X. The construction is inductive and mimics the inductive solution of the word problem given in Section 2. For convenience let $\mathscr{F}(\phi) = \phi$. If $\phi \neq A \subseteq X$, A finite, let $\mathscr{F}(A)$ be all quadruples $\mathfrak{A} = (\alpha, a, A, \mathfrak{a})$ where $a \in G(X)$, the free group on X, $c(a) \subseteq A$, $\alpha \in \mathscr{F}(A - \{x\})$ for some $x \in A$ and $\mathfrak{a} \in \mathscr{F}(A - \{y\})$ for some $y \in A$. Let

$$\mathscr{F} = \bigcup \{\mathscr{F}(A) | \phi \neq A \subseteq X, A \text{ finite}\}.$$

For $\mathfrak{A} \in \mathscr{F}$, let

$$\begin{array}{ll} \bar{s}^0(\mathfrak{A}) = \mathfrak{A} & \bar{e}^0(\mathfrak{A}) = \mathfrak{A} \\ \bar{s}(\mathfrak{A}) = \alpha & \bar{e}(\mathfrak{A}) = \mathfrak{a} \\ \bar{s}^{n+1}(\mathfrak{A}) = \bar{s}(\bar{s}^n(\mathfrak{A})) & \bar{e}^{n+1}(\mathfrak{A}) = \bar{e}(\bar{e}^n(\mathfrak{A})) \end{array}$$

where $\bar{s}(\phi) = \phi = \bar{e}(\phi)$. Also let $\bar{c}(\mathfrak{A}) = A$.

For $\mathfrak{A} = (\alpha, a, A, \mathfrak{a})$ and $\mathfrak{B} = (\beta, b, B, \mathfrak{b})$, two elements of $\mathscr{F}$, the product $\mathfrak{A}\mathfrak{B} = \mathfrak{C} = (\gamma, c, C, \mathfrak{c})$ will be defined by induction. Let

$$C = A \cup B$$

$$c = ab, \text{ the product taken in } G(X),$$

$$\gamma = \begin{cases} \alpha \text{ if } B \subseteq A \\ \mathfrak{A}\bar{s}^k(\beta) \text{ if } B \not\subseteq A \end{cases}$$

where $k \geqq 0$ is the smallest integer such that

$$|A \cup \bar{c}(\bar{s}^k(\beta))| + 1 = |A \cup B|$$

$$\mathfrak{c} = \begin{cases} \mathfrak{b} \text{ if } A \subseteq B \\ \bar{e}^k(\mathfrak{a})\mathfrak{B} \text{ if } A \not\subseteq B \end{cases}$$

https://doi.org/10.4153/CJM-1981-070-4 Published online by Cambridge University Press

where $k \geqq 0$ is the smallest integer such that

$$|B \cup \bar{c}(\bar{e}^k(\mathfrak{a}))| + 1 = |A \cup B|.$$

The definition is completed by letting $\mathfrak{A}\phi = \mathfrak{A} = \phi\mathfrak{A}$ for all $\mathfrak{A} \in \mathscr{F}$.

For $w \in U(X)$ let $w\varphi = (s(w)\varphi, r(w), c(w), e(w)\varphi)$ where the inductive definition is completed by letting $\phi\varphi = \phi$. The mapping $\varphi: U(X) \to \mathscr{F}$ is easily seen to be a homomorphism onto $\mathscr{F}$ with kernel $\sim$. Therefore $\mathscr{F} \cong U(X)/\sim$ and $\mathscr{F}$ is a model of the free orthogroup on X.

4. The free semilattice of groups. A *semilattice of groups* is a completely regular semigroup where idempotents belong to the centre. In terms of identities this means that in addition to identities (1)–(3) of the introduction a semilattice of groups satisfies

(5) $axx^{-1} = xx^{-1}a$.

It is clear that a semilattice of groups is an orthogroup. The free semilattice of groups has been described by Liber [**3**]. In this section we give a description of the free semilattice of groups by modifying the methods developed in Sections 2 and 3.

Definition 4.1. Let $w, w' \in U(X)$. Then $w \approx w'$ if and only if $c(w) = c(w')$ and $r(w) = r(w')$.

THEOREM 4.2. *$U(X)/\approx$ is the free semilattice of groups on X.*

Proof. The proof that $\approx$ is a congruence on $U(X)$ is part of the proof of Theorem 2.4. It is also clear that $axx^{-1} \approx xx^{-1}a$ for any $a, x \in U(X)$ and therefore that $U(X)/\approx$ is a semilattice of groups.

To show that $U(X)/\approx$ is free we show that $\approx \subseteq \rho$ for any congruence ρ such that $U(X)/\rho$ is a semilattice of groups. Let $c(w) = \{x_1, \ldots, x_n\}$. Then since $x_i(x_i)^{-1}$ is idempotent and its congruence class is therefore in the centre of $U(X)/\rho$, it follows that

$$w \,\rho\, r(w)x_1(x_1)^{-1} \ldots x_n(x_n)^{-1}.$$

Let $w \approx w'$. Then

$$\begin{aligned} w \,\rho\, r(w)&x_1(x_1)^{-1} \ldots x_n(x_n)^{-1} \\ &= r(w')x_1(x_1)^{-1} \ldots x_n(x_n)^{-1} \\ &\rho w'. \end{aligned}$$

We can also give a model for the free semilattice of groups on X. Let $\mathscr{S}$ be all pairs (g, A) where $g \in G(X)$, $A \subseteq X$, A finite and $c(g) \subseteq A$. Let (g, A), $(A, B) \in \mathscr{S}$ and define

$$(g, A)(h, B) = (gh, A \cup B)$$

where gh is the product in $G(X)$. The mapping $w \to (r(w), c(w))$ is a homomorphism of $U(X)$ onto $\mathscr{S}$ with kernel $\approx$. Therefore $\mathscr{S}$ is the free semilattice of groups on X.

A *strong semilattice of groups* is a triple $[(Y; G_\alpha, \psi_{\alpha,\beta})]$ where Y is a semilattice, G_α is a group for each $\alpha \in Y$, the G_α are pairwise disjoint and for $\alpha \geqq \beta$, $\psi_{\alpha\beta}: G_\alpha \to G_\beta$ is a homomorphism such that

(i) $\psi_{\alpha,\alpha}$ is the identity on G_α, and
(ii) $\psi_{\alpha,\beta} \circ \psi_{\beta,\gamma} = \psi_{\alpha,\gamma}$ if $\alpha \geqq \beta \geqq \gamma$.

Multiplication is defined on $X = \bigcup \{G_\alpha | \alpha \in Y\}$ by

$$xy = (x\psi_{\alpha,\alpha\beta})(y\psi_{\beta,\alpha\beta})$$

where $x \in G_\alpha$, $y \in G_\beta$ and $\alpha\beta$ is the product in Y.

Every semilattice of groups is a strong semilattice of groups. Let $L(X)$ be the free semilattice on X thought of as the set of all finite, non-empty subsets of X with union as product. The free semilattice of groups on X is the strong semilattice $(L(X), G(A), \psi_{AB})$ where for every pair A, B of finite non-empty subsets of X with $A \subseteq B$ ($A \geqq B$ in $L(X)$), $\psi_{AB}: G(A) \to G(B)$ is the unique homomorphism of the free group $G(A)$ obtained by extending the inclusion mapping of A into B.

5. The free orthocryptogroup. A semigroup is an *orthocryptogroup* if it is an orthogroup in which $\mathscr{H}$ is a congruence. An orthocryptogroup can be characterized by the identities (1)–(3) of the introduction together with

(6) $\quad aa^{-1}bb^{-1} = (ab)(ab)^{-1}$

(see [**4**]). It is clear that (6) implies (4).

In order to describe the least orthocryptogroup congruence on $U(X)$ we need a description of the least band congruence β on $U(X)$. The free band is usually given as a quotient of $S(X)$, the free semigroup on X. For any word $w \in U(X)$ let $\bar{w} \in S(X)$ be obtained from w by removing all occurrences of (and $)^{-1}$. Since, in a band, $x = x^{-1}$ it is clear that for $w, w' \in U(X)$, $w\beta w'$ if and only if $\bar{w}\bar{\beta}\bar{w}'$, where $\bar{\beta}$ is the least band congruence on $S(X)$. The congruence $\bar{\beta}$ can be described as follows (see e.g. [**2**], Lemma 4.6 of Chapter IV). If $u \in S(X)$ define $s(u)$, $e(u)$ and $c(u)$ as before. Then for $u, v \in S(X)$ $u\bar{\beta}v$ if and only if $c(u) = c(v)$, $s(u)\bar{\beta}s(v)$ and $e(u)\bar{\beta}e(v)$.

Definition 5.1. Let $w, w' \in U(X)$. Then $w\pi w'$ if and only if $r(w) = r(w')$ and $w\beta w'$.

THEOREM 5.2. *$U(X)/\pi$ is the free orthocryptogroup on X.*

Proof. It is easy to check that π is a congruence. In fact it is the intersection of the least group congruence and the least band congruence on

$U(X)$. The latter fact immediately gives $U(X)/\pi$ a subdirect product of the free group on X and the free band on X which in turn implies that $U(X)/\pi$ is an orthocryptogroup. (This may also easily be shown by checking that the identities (1)–(3) and (6) hold in $U(X)/\pi$.)

To show that $U(X)/\pi$ is free, let ρ be any congruence such that $U(X)/\rho$ is an orthocryptogroup and prove that $\pi \subseteq \rho$. It was shown by Yamada [**5**] that an orthocryptogroup is a subdirect product of a semilattice of groups and a band. Choose T, a semilattice of groups, and B, a band, so that $U(X)/\rho$ is a subdirect product of T and B. In fact $T = U(X)/\tau$ and $B = U(X)/\gamma$ and $\rho = \tau \cap \gamma$. Now $\tau \supseteq \nu$, where ν is the least semilattice of groups congruence on $U(X)$, $\gamma \supseteq \beta$ where β is the least band congruence on $U(X)$ and therefore $\pi = \nu \cap \beta \subseteq \tau \cap \gamma = \rho$.

A model for the free orthocryptogroup can be obtained from $G(X)$, the free group on X, and $B(X)$ the free band on X as follows. Let

$$\mathscr{C} = \{(g, b) | g \in G(X), b \in B(X), c(g) \subseteq c(b)\}$$

and let multiplication on $\mathscr{C}$ be defined by

$$(g, b)(g', b') = (gg', bb')$$

Then $\mathscr{C}$ with this product is the free orthocryptogroup on X.

The free objects in the subvarieties of orthogroups we have discussed can be described in terms of the quadruples introduced in Section 3. Let $\mathfrak{A} = (\alpha, a, A, \mathfrak{a})$ and $\mathscr{C} = (\gamma, c, C, \mathfrak{c})$ be two quadruples of $\mathscr{F}$. The free group on X is $\mathscr{F}/\sigma$ where σ is the congruence defined by $\mathfrak{A}\ \sigma\ \mathscr{C}$ if and only if $a = c$. The free semilattice on X is $\mathscr{F}/\eta$ where η is the congruence defined by $\mathfrak{A}\eta\mathscr{C}$ if and only if $A = C$. The free band on X is $\mathscr{F}/\beta$ where $\mathfrak{A}\beta\mathscr{C}$ if and only if $A = C$, $\alpha\beta\gamma$ and $\mathfrak{a}\beta\mathfrak{c}$. The congruence $\nu = \sigma \cap \eta$ gives the free semilattice of groups and the congruence $\pi = \sigma \cap \beta$ gives the free orthocryptogroup.

References

1. A. H. Clifford, *The free completely regular semigroup on a set*, J. Algebra *59* (1979), 434–451.

2. J. M. Howie, *An introduction to semigroup theory* (Academic Press, London, 1976).

3. S. A. Liber, *On free algebras of normal closures of varieties*, Ordered Sets and Lattices, Issue *2*, Saratov (1974), 51–53. (In Russian).

4. M. Petrich, *Varieties of orthodox bands of groups*, Pacific J. Math. *58* (1975), 209–217.

5. M. Yamada, *Strictly inversive semigroups*, Bull. Shimane Univ. *13* (1964), 128–138.

University of Manitoba,
Winnipeg, Canada