ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 17, Number 3, Summer 1987

IMPLICATIONS FOR SEMIGROUPS EMBEDDABLE IN ORTHOCRYPTOGROUPS

KARL BYLEEN AND FRANCIS PASTIJN

Malcev [**13**] was the first to give necessary and sufficient conditions for the embeddability of a semigroup in a group. His conditions are countably infinite in number. No finite number of these conditions is sufficient to ensure embeddability. A similar set of conditions, but involving geometrical concepts, was given by Lambek [**12**]. An account of these results, and of the necessary and sufficient conditions for the embeddability of a semigroup in a group due to Pták [**17**], is presented in Chapter 12 of Clifford and Preston [**5**]. The account of Clifford and Preston employs the concept of a free group on a semigroup. If S is any semigroup then the pair (G,γ), where G is a group and $\gamma : S \rightarrow G$ is a homomorphism for which $S\gamma$ is a set of group generators for G, is said to be a free group on the semigroup S if it satisfies the following universal property: if H is a group and $\eta : S \rightarrow H$ is a homomorphism such that $S\eta$ is a set of group generators for H, then there exists a homomorphism $\theta : G \rightarrow H$ such that $\gamma\theta = \eta$. The existence and uniqueness of the free group on a semigroup are established, and it is shown that a semigroup S is embeddable in a group if and only if the canonical homomorphism γ of S into the free group on S is an embedding. Various aspects of the work of Malcev and Lambek have been considered by Bush [**4**], Bouleau [**3**], and Osondu [**15**]. Simpler conditions which are sufficient to ensure the embeddability of a semigroup in a group have been given by Doss [**6**], Trotter [**23**], and Bouleau [**2**]. Schein [**18, 19**] has given necessary and sufficient conditions for a semigroup to be embeddable in an inverse semigroup.

A semigroup which is a union of groups is said to be *completely regular*. A completely regular semigroup S comes naturally equipped with a unary operation of inverse by letting a^{-1}, for $a \in S$, be the inverse of a in the maximal subgroup of S which contains a. The class of completely regular semigroups forms a variety of type $\langle 2,1\rangle$ which has the defining identities $a(bc) = (ab)c, aa^{-1}a = a, aa^{-1} =$

Received by the editors on February 8, 1985 and in revised form on September 19, 1985.

$a^{-1}a$, and $(a^{-1})^{-1} = a$. A completely regular semigroup which is orthodox, that is, in which the idempotents form a subsemigroup, is said to be an *orthogroup*. An orthogroup in which Green's relation $\mathcal{H}$ is a congruence is said to be an *orthocryptogroup*. The classes of orthogroups and orthocryptogroups are both subvarieties of the variety of all completely regular semigroups which have as defining identities those for completely regular semigroups supplemented by $(aa^{-1}bb^{-1})^2 = aa^{-1}bb^{-1}$ or $aa^{-1}bb^{-1} = ab(ab)^{-1}$ respectively [**16**]. The word problems for free orthogroups and free orthocryptogroups were solved by Gerhard and Petrich [**9**]. If a is an element of a completely regular semigroup it is often convenient to denote by a^0 the identity element of the maximal subgroup to which a belongs, so that $a^0 = aa^{-1}$.

An *equational implication* is a formula of the form $\{u_\alpha = v_\alpha\}_{\alpha \in A} \to w = z$, where A is a finite set and $u_\alpha, v_\alpha (\alpha \in A)$, w and z are words in a free semigroup on a set of variables. The purpose of this paper is to obtain a set F of equational implications which defines the class of all semigroups which are embeddable in orthocryptogroups (in the sense that a semigroup S is embeddable in an orthocryptogroup if and only if S satisfies each implification in F). In §1 we apply a general result to guarantee that this class of semigroups can be defined by implications. We also show that a cancellative semigroup can be embedded in an orthogroup if and only if it can be embedded in a group, and we give an example of a cancellative semigroup which is embeddable in a completely simple semigroup but not in a group. In §2 we obtain necessary and sufficient conditions for a semigroup with identity to be embeddable in an orthocryptogroup. In §3 we obtain equational implications which define the class of all semigroups which are embeddable in $\mathcal{V}$-orthocryptogroups, where $\mathcal{V}$ is any variety of bands (an orthocryptogroup is said to be a $\mathcal{V}$-*orthocryptogroup* if its greatest band homomorphic image belongs to $\mathcal{V}$).

For general terminology and notation related to semigroup theory we refer the reader to Howie [**11**], and, for that related to universal algebra, to Grätzer [**10**].

1. Generalities and examples. Classes of algebras which are definable by equational implications are known as quasivarieties. General results on quasi-varieties are discussed in Malcev [**14**] and in Taylor's survey article [**22**]; an abridged version of this article appears as §63 of Grätzer [**10**]. In particular, a class $\mathcal{E}$ of algebras is a quasi-variety if and only if $\mathcal{E}$ is closed under the formation of isomorphic images, products, subalgebras and direct limits. This characterization of quasi-varieties may be applied to yield the following result, which appears as Corollary 5 (p. 216) of [**14**].

THEOREM 1.1. *Let τ and η be types and suppose that η is larger than τ. Let $\mathcal{V}$ be a quasi-variety of algebras of type η. Let $\mathcal{E}$ be the class of all the algebras of type τ which are subalgebras of τ-reducts of algebras of $\mathcal{V}$. Then $\mathcal{E}$ is itself a quasi-variety.*

Completely regular semigroups and inverse semigroups are algebras of type $\langle 2, 1\rangle$ whose $\langle 2\rangle$-reducts are semigroups. The following corollary of Theorem 1.1 thus guarantees that the class of semigroups described in the title is definable by equational implications.

COROLLARY 1.2. *Let $\mathcal{V}$ be a variety of completely regular [inverse] semigroups. The class $\mathcal{E}$ of all semigroups which are embeddable in members of $\mathcal{V}$ is definable by equational implications.*

Let S be a subsemigroup of a completely regular semigroup D. Even if S is embeddable in a group, S need not be embedded in a subgroup of D. Indeed, let X be a set and let $\mathcal{V}$ be a variety of completely regular semigroups which contains the variety of all groups. Since the free semigroup F_X on X can be embedded in the free group on X, the subsemigroup of the free object $F_X^{\mathcal{V}}$ in $\mathcal{V}$ on X which is generated by X is a copy of F_X. This copy of F_X intersects all $\mathcal{D}$-classes of F_X in case $\mathcal{V}$ contains the variety of all semilattices. Also, this copy of F_X intersects all $\mathcal{H}$-classes of F_X if $\mathcal{V}$ is a variety of completely simple semigroups.

Obviously a semigroup which is embeddable in a completely regular semigroup need not be embeddable in a group. We have however the following theorem which was proved in special cases by Schutt [**20**].

THEOREM 1.3. *A cancellative semigroup is embeddable in an orthogroup if and only if it is embeddable in a group.*

PROOF. Let S be a cancellative semigroup which is embedded in the orthogroup O. We may suppose that O is generated as an algebra of type $< 2, 1 >$ by the elements of S. Then S has a non-void intersection with every $\mathcal{D}$ class of O.

One easily verifies that the least group congruence σ on O is given by

$x\sigma y \Leftrightarrow zxz = zyz$ for some $z \in 0$ such that $D_z \leq D_x$ and $D_z \leq D_y$ in $O/\mathcal{D}(x, y \in 0)$. If, for $x, y, z \in 0$, we have $zxz = zyz$ and $D_z \leq D_x$ and $D_z \leq D_y$ in $O/\mathcal{D}$, then $cxc = cyc$ for all $c \in D_z$. Since every $\mathcal{D}$-class of O contains an element of S the condition above may be replaced by $x\sigma y \Leftrightarrow cxc = cyc$ for some $c \in S$ such that $D_c \leq D_x$ and $D_c \leq D_y$ in $O/\mathcal{D}(x, y \in O)$. Hence if $a, b \in S$ and $a\sigma b$, then $cac = cbc$ for some $c \in S$, and thus $a = b$ since S is cancellative. From this we infer that σ separates the elements of S. Therefore $\sigma^\natural$ embeds S isomorphically into the group O/σ.

COROLLARY 1.4. *Let $\mathcal{V}$ be a variety of orthogroups which contains the variety of all groups. Let $\mathcal{E}$ be the class of all the semigroups which are embeddable in members of $\mathcal{V}$. Then $\mathcal{E}$ cannot be defined by a finite set of equational implications.*

PROOF. Let $\mathcal{E}$ be defined by the set Σ of equational implications. The set Σ supplemented by the implications

$$xz = yz \rightarrow x = y \text{ and } zx = zy \rightarrow x = y$$

will be denoted by Σ'. Since $\mathcal{V}$ contains the variety of all groups, by Theorem 1.3, a semigroup with identity is embeddable in a group if and only if it satisfies the implications of Σ'. In [**13**(1939)] Malcev establishes a countably infinite set M of equational implications which determines the class of all semigroups with identity which are embeddable in groups. The implications in Σ' can be derived from the implications in a subset M' of M according to the rules prescribed by Selman [**21**]. If Σ is finite, then Σ' is finite and M' can be chosen to be finite. The set M' would then be a finite set of implications which determines the class of all semigroups embeddable in a group. According to Malcev [**13** (1940)] this is impossible. Hence Σ is infinite.

The following example shows that Theorem 1.3 does not necessarily apply in a more general situation: we give an example of a cancellative semigroup which is embeddable in a completely simple semigroup but which is not embeddable in a group.

EXAMPLE 1.5. Let F be the free group on $\{a, c, p, v, y, z\}$, let $I = \Lambda = \{1, 2\}$ and let $P = \begin{pmatrix} 1 & 1 \\ 1 & p \end{pmatrix}$. Let D denote the Rees matrix semigroup $\mathcal{M}(I, F, \Lambda; P)$ and let S be the subsemigroup of D generated by the elements $\bar{a} = (1,a,1), \bar{b} = (1,za,1), \bar{c} = (2,c,1), \bar{d} = (1,zc,1), \bar{x} = (1,yz,1), \bar{y} = (1,y,1), \bar{u} = (1,vz,2)$, and $\bar{v} = (1,v,1)$. One verifies that S is cancellative by considering several cases. In S we have $\bar{x}\bar{a} = \bar{y}\bar{b}, \bar{x}\bar{c} = \bar{y}\bar{d}, \bar{u}\bar{a} = \bar{v}\bar{b}$, but $\bar{u}\bar{c} \neq \bar{v}\bar{d}$. Thus S does not satisfy the quotient condition and is therefore not embeddable in a group (see Lemma 12.11 of [**5**]). Furthermore, S^1 is cancellative and, although embeddable in a completely regular semigroup, is not embeddable in a completely simple semigroup.

2. Semigroups embeddable in orthocryptogroups. A semigroup S is embeddable in an orthocryptogroup if and only if S^1 is. Therefore, in order to characterize those semigroups which are embeddable in orthocryptogroups, we shall find implications which a semigroup with identity satisfies if and only if it is embeddable in an orthocryptogroup. If S is any semigroup we denote the least semilattice congruence on S by η. The η-classes of any completely regular semigroup coincide with its $\mathcal{D}$-classes. We make frequent use of the following lemma from [**9**].

LEMMA 2.1. ([**9**]). *Let S be an orthogroup. For $a, b, e \in S$ with $e = e^2$ let $D_a = D_b \leq D_e$. Then $ab = aeb$.*

If S is any semigroup then the least band congruence β on S is generated by the relation $\beta_0 = \{(x, x^2) : x \in S\}$. Two elements s and t of S are β-related if and only if there exists a finite sequence of elementary β_0-transitions from s to t. (If R is any relation on a semigroup S, then elements $s, s' \in S$ are said to be connected by an elementary R-transition if $s = xpy, s' = xqy$ for some $x, y \in S^1$ where either $p = q$ or $(p,q) \in R$ or $(q,p) \in R$). The existence of such a sequence of elementary β_0-transitions is equivalent to the existence of elements of S which satisfy a certain set of equations. We describe such a set of equations for the case in which S has an identity element.

For any $m \geq 1$ let J_m denote the following sequence of $2m+1$ equations $E_0, E_1, \ldots, E_{2m}$ in the $6m+2$ variables $x, y, x_i, g_i, h_i (i = 1, 2, \ldots, 2m)$.

$$
\begin{aligned}
&E_0 : \ x = g_1 x_1 h_1 \\
&E_{2i-1} : \ g_{2i-1}(x_{2i-1})^2 h_{2i-1} = g_{2i}(x_{2i})^2 h_{2i} \quad (i = 1, 2, \ldots, m) \\
&E_{2i} : \ g_{2i} x_{2i} h_{2i} = g_{2i+1} x_{2i+1} h_{2i+1} \quad (i = 1, 2, \ldots, m-1) \\
&E_{2m} : \ g_{2m} x_{2m} h_{2m} = y
\end{aligned}
$$

LEMMA 2.2. *Let S be a semigroup with identity. Then $a\beta b$ if and only if there exists a positive integer m and elements of S for which the equations in J_m are satisfied when the values a and b are assigned to x and y respectively.*

PROOF. If $a\beta b$, then there is a sequence of elementary β_0-transitions from a to b. Since S has an identity element, elementary β_0-transitions of the form $u1v \to u1^2v$ or $u1^2v \to u1v$ may be inserted to produce a sequence of elementary β_0-transitions from a to b in which expansions and contradictions alternate, ensuring that the equations in J_m for some m are satisfied. Conversely, if the equations in J_m are satisfied, then there is a sequence of elementary β_0-transitions from a to b, so $a\beta b$.

LEMMA 2.3. *Let S be a semigroup with identity. If S is embeddable in an orthogroup, then S satisfies the following implication for each positive integer m:*

$$
\left.
\begin{aligned}
r_1 z r_2 &= r_1 w r_2 \\
y &= x r_1 z r_2 x \\
J_m &
\end{aligned}
\right\} \rightarrow xzx = xwx
$$

PROOF. Let S be embedded in the orthogroup T and suppose that the elements $\underline{r}_1, \underline{r}_2, \underline{z}, \underline{w}$, and x of S satisfy the equations on the left-hand side of (K_m) when substituted for r_1, r_2, z, w, and x, respectively. Then $\underline{r}_1 \underline{z}\, \underline{r}_2 = \underline{r}_1 \underline{w}\, \underline{r}_2$ and, by Lemma 2.2, $\underline{x}\beta\underline{x}\,\underline{r}_1\, \underline{z}\,\underline{r}_2\,\underline{x}$. Since $\beta \subseteq \eta$ we have $\underline{x}\eta\underline{x}\,\underline{r}_1\underline{z}\,\underline{r}_2\,\underline{x}$, so $\underline{x}\eta \le \underline{r}_1\eta, \underline{x}\eta \le \underline{r}_2\eta$, $\underline{x}\eta \le \underline{z}\eta$, and $\underline{x}\eta \le \underline{w}\eta$. Thus, by Lemma 2.1, we have $\underline{x}\,\underline{z}\,\underline{x} = \underline{x}(\underline{r}^{-1}1\underline{r}_1)\underline{z}(\underline{r}_2\,\underline{r}_2^{-1})\underline{x} = \underline{x}\,\underline{r}_1^{-1}(\underline{r}_1\,\underline{z}\,\underline{r}_2)\,\underline{r}_2^{-1}\underline{x} = \underline{x}\,\underline{r}_1^{-1}(\underline{r}_1\underline{w}\,\underline{r}_2)\underline{r}_2^{-1}\underline{x} = \underline{x}\,\underline{w}\,\underline{x}$ as required.

If S is any semigroup with least semilattice congruence η and $i \in S/\eta$ we let $S_i = \{s \in S : s\eta \ge i\}$. If $r \in S$ such that $r\eta = i$ we define the relation τ_r on S_i by $s\tau_r t \Leftrightarrow rsr = rtr (s, t \in S_i)$.

LEMMA 2.4. *Let S be a semigroup with identity which satisfies (K_m) for all $m \geq 1$. Then:*
(i) $u\eta \leq r\eta = i$ *implies* $\tau_u | S_i \supseteq \tau_r$;
(ii) $\tau_u = \tau_r$ *if and only if* $u\eta r$.
Furthermore, denoting by τ_i the common value of τ_r for $r \in i\eta^{-1}$
(iii) τ_i *is a congruence on S_i for all $i \in S/\eta$; and*
(iv) $\tau = \bigcup_{i \in S/\eta} \tau_i | i\eta^{-1}$ *is a congruence on S.*

PROOF. (i). Suppose that $u\eta \leq r\eta = i$ and let $s\tau_r t (s, t \in S_i)$ so that $rsr = rtr$. Then $(rsr)\eta = r\eta \geq u\eta$ and $(ursru)\eta = u\eta$, thus $(ursru)\beta u$. By (K_m) for some sufficiently large m we have $usu = utu$, so $s\tau_u t$. (ii) follows immediately from (i). (iii). Suppose $r\eta = i$ and $s\tau_i t (s, t \in S_i)$. Let $c \in S_i$. Then $rsr = rtr$ implies $crc \cdot s \cdot crc = crc \cdot t \cdot crc$ by (ii) since $crc\eta r$. Furthermore, $r(crc \cdot s \cdot crc)r\eta r$ implies $r(crc \cdot s \cdot crc)r\beta r$, so by (K_m) for some sufficiently large m, $rcsr = rctr$ and $rscr = rtcr$, that is, $cs\tau_i ct$ and $sc\tau_i tc$. (iv). Suppose $s\tau t$ for some $s, t \in S$ and let $c \in S$. Then there exists $i \in S/\eta$ such that $s\eta = t\eta = i$ and $s\tau_i t$. We put $(sc)\eta = (tc)\eta = j$ and note that $j \leq i$ in S/η. By (i) we conclude that $s\tau_j t$. So by (iii), $sc\tau_j tc$ and $cs\tau_j ct$. Thus $sc\tau tc$ and $cs\tau ct$.

Let $M = \{(M_m) : m = 1, 2, 3, \dots\}$ be a family of implications such that a semigroup with identity is embeddable in a group if and only if it satisfies each implication in M. We can, for example, take M to be the family of implications of Malcev [**13**] which are described in [**5**]. For any positive integer m we write (M_m) as $\{u_\alpha = v_\alpha\}_{\alpha \in A_m} \to w_m = z_m$, where the sets A_m for $m \geq 1$ are finite and disjoint. For each m let P_m denote the set of all variables which appear in $u_\alpha, v_\alpha (\alpha \in A_m), w_m$ and z_m. For each m choose a word p_m which contains all the variables in P_m and no other variables. Let y be a variable which does not belong to any $P_m (m \geq 1)$.

LEMMA 2.5. *Let S be a semigroup. If S is embeddable in an orthogroup, then S satisfies the following implication for every positive integer m:*

$$(\overline{M}_m) \qquad \{p_m y u_\alpha p_m y = p_m y v_\alpha p_m y\}_{\alpha \in A_m} \to p_m y w_m p_m y = p_m y z_m p_m y.$$

PROOF. Let $x_1, x_2, \dots, x_n$ be the elements of P_m. We can consider

$u_\alpha, v_\alpha (\alpha \in A_m), w_m$ and z_m to be n-ary polynomials in these variables,

$$\begin{aligned} p_m &= p_m(x_1, x_2, \dots, x_n) \\ u_\alpha &= u_\alpha(x_1, x_2, \dots, x_n) \quad (\alpha \in A_m) \\ v_\alpha &= v_\alpha(x_1, x_2, \dots, x_n) \quad (\alpha \in A_m) \\ w_m &= w_m(x_1, x_2, \dots, x_n) \\ z_m &= z_m(x_1, x_2, \dots, x_n) \end{aligned}$$

where every variable of course need not occur in each polynomial.

Let $a_1, a_2, \dots, a_n$, b be elements of S such that, for each $\alpha \in A_m$,

$$\begin{aligned} &p_m(a_1, \dots, a_n) b u_\alpha(a_1, \dots, a_n) p_m(a_1, \dots, a_n) b \\ &= p_m(a_1, \dots, a_n) b v_\alpha(a_1, \dots, a_n) p_m(a_1, \dots, a_n) b^{\cdot} \end{aligned}$$

We must show that

$$\begin{aligned} &p_m(a_1, \dots, a_n) b w_m(a_1, \dots, a_n) p_m(a_1, \dots, a_n) b \\ &= p_m(a_1, \dots, a_n) b z_m(a_1, \dots, a_n) p_m(a_1, \dots, a_n) b. \end{aligned}$$

Let T be an orthogroup in which S is embedded. Let η_T be the least semilattice congruence on T. Since p_m contains all of the variables which occur in (M_m) we have

$$(p_m(a_1, \dots, a_n) b)\eta_T \leq u_\alpha(a_1, \dots, a_n)\eta_T \quad (\alpha \in A_m)$$

and

$$(p_m(a_1, \dots, a_n) b)\eta_T \leq v_\alpha(a_1, \dots, a_n)\eta_T \quad (\alpha \in A_m).$$

Let $j = (p_m(a_1, \dots, a_n) b)\eta_T$ and let $T_j = \{x \in T : j \leq x\eta_T\}$. We define the mapping $\phi : T_j \to H_{p_m(a_1, \dots, a_n) b}$ by

$$\begin{aligned} s\phi &= (p_m(a_1, \dots, a_n) b)^0 s (p_m(a_1, \dots, a_n) b)^0. \text{ Let } s, t \in T_j. \text{ Then} \\ s\phi \cdot t\phi &= (p_m(a_1, \dots, a_n) b)^0 s ((p_m(a_1, \dots, a_n) b)^0)^2 t (p_m(a_1, \dots, a_n) b)^0 \\ &= (p_m(a_1, \dots, a_n) b)^0 s (p_m(a_1, \dots, a_n) b)^0 t (p_m(a_1, \dots, a_n) b)^0 \\ &= (p_m(a_1, \dots, a_n) b)^0 st (p_m(a_1, \dots, a_n) b)^0 = (st)\phi, \end{aligned}$$

where the third equality follows from Lemma 2.1. Thus ϕ is a homomorphism of T_j onto the maximal subgroup $H_{p_m(a_1, \dots, a_n) b}$. Hence, for $\alpha \in A_m$,

$$(p_m(a_1,\dots,a_n)b)^0u_\alpha(a_1,\dots,a_n)(p_m(a_1,\dots,a_n)b)^0 = u_\alpha(a_1\phi,\dots,a_n\phi),$$
$$(p_m(a_1,\dots,a_n)b)^0v_\alpha(a_1,\dots,a_n)(p_m(a_1,\dots,a_n)b)^0 = v_\alpha(a_1\phi,\dots,a_n\phi),$$
$$(p_m(a_1,\dots,a_n)b)^0w_m(a_1,\dots,a_n)(p_m(a_1,\dots,a_n)b)^0 = w_m(a_1\phi,\dots,a_n\phi),$$
$$(p_m(a_1,\dots,a_n)b)^0z_m(a_1,\dots,a_n)(p_m(a_1,\dots,a_n)b)^0 = z_m(a_1\phi,\dots,a_n\phi).$$

Since $a_1\phi,\dots,a_n\phi$ belong to the same subgroup and since $u_\alpha(a_1\phi,\dots,a_n\phi) = v_\alpha(a_1\phi,\dots,a_n\phi)$ for all $\alpha \in A_m$, we conclude by the definition of the family M of implications that $w_m(a_1\phi,\dots,a_n\phi) = z_m(a_1\phi,\dots,a_n\phi)$, from which we deduce that the required equality is satisfied.

LEMMA 2.6. *Let S be a semigroup with identity which satisfies (K_m) and $(\overline{M}_m)$ for all $m \geq 1$. Then S_i/τ_i is embeddable in a group for all $i \in S/\eta$.*

PROOF. To establish the result we show that S_i/τ_i satisfies each implication (M_m) in the family M. Let $a_1, a_2, \dots, a_n$ be any elements of S_i such that $a_1\tau_i, a_2\tau_i, \dots, a_n\tau_i$ satisfy the equations $u_\alpha = v_\alpha, \alpha \in A_m$. Then $u_\alpha(a_1,\dots,a_n)\tau_i = u_\alpha(a_1\tau_i,\dots,a_n\tau_i) = v_\alpha(a_1\tau_i,\dots,a_n\tau_i) = v_\alpha(a_1,\dots,a_n)\tau_i$. Hence, for $b \in i\eta^{-1}, p_m(a_1,\dots,a_n)b \in i\eta^{-1}$, and thus, by Lemma 2.4 we have

$$\begin{aligned}&(p_m(a_1,\dots,a_n)b)u_\alpha(a_1,\dots,a_n)(p_m(a_1,\dots,a_n)b)\\ =&(p_m(a_1,\dots,a_n)b)v_\alpha(a_1,\dots,a_n)(p_m(a_1,\dots,a_n)b)\end{aligned}$$

for each $\alpha \in A_m$. But S satisfies $(\overline{M}_m)$ so

$$\begin{aligned}&(p_m(a_1,\dots,a_n)b)w_m(a_1,\dots,a_n)(p_m(a_1,\dots,a_n)b)\\ =&(p_m(a_1,\dots,a_n)b)z_m(a_1,\dots,a_n)(p_m(a_1,\dots,a_n)b).\end{aligned}$$

Therefore, by Lemma 2.4, $w_m(a_1\tau_i,\dots,a_n\tau_i) = w_m(a_1,\dots,a_n)\tau_i = z_m,(a_1,\dots,a_n)\tau_i = z_m(a_1\tau_i,\dots,a_n\tau_i)$, as required.

LEMMA 2.7. *Let S be a semigroup with identity. If S is embeddable in an orthocryptogroup, then S satisfies the following implication for every positive integer m:*

$$(L_m) \qquad \left.\begin{array}{c} x^3 = xyx \\ J_m \end{array}\right\} \to x = y$$

PROOF. Suppose S is embedded in the orthocryptogroup T and let a and b be elements of S which satisfy the left-hand side of (L_m), that is, suppose $a^3 = aba$ and, by Lemma 2.2, $a\beta b$. Since T is an orthocryptogroup, $a\beta b$ implies that a and b belong to the same maximal subgroup of T. Therefore since $a^3 = aba$ we conclude that $a = b$.

LEMMA 2.8. *Let S be a semigroup with identity which satisfies (K_m) and (L_m) for all $m \geq 1$. Then $\beta \bigcap \tau$ is the equality on S.*

PROOF. Suppose that $(a, b) \in \beta \bigcap \tau$. Then by the definition of τ, $a\eta = b\eta = i$ for some $i \in S/\eta$ and $a\tau_i b$. By Lemma 2.4 we have $\tau_i = \tau_a$, thus $a^3 = aba$. Since $a\beta b$, there exists, by Lemma 2.2, some m such that a and b satisfy J_m, and hence by applying (L_m) we conclude that $a = b$.

THEOREM 2.9. *A semigroup S with identity is embeddable in an orthocryptogroup if and only if S satisfies the implications $(K_m), (\overline{M}_m)$ and (L_m) for all $m \geq 1$.*

PROOF. The direct part is immediate from Lemmas 2.3, 2.5 and 2.7. Suppose, conversely, that S satisfies the implications $(K_m), (\overline{M}_m)$ and (L_m) for all $m \geq 1$. By Lemma 2.4, τ_i is a congruence on S_i for each $i \in S/\eta$; let G_i be the free group on the semigroup S_i/τ_i. By Lemma 2.6, the canonical homomorphism $\theta_i : S_i/\tau_i \to G_i$ is an embedding. If $i \geq j$ in S/η, then, by Lemma 2.4, the mapping $S_i/\tau_i \to S_j/\tau_j$ defined by $s\tau_i \to s\tau_j$ is a homomorphism which, by the universal property of the free group on a semigroup, can be extended in a unique way to a homomorphism ϕ_{ij} of G_i into G_j. Let T be the semilattice of groups $G_i, i \in S/\eta$, which is obtained in this way.

By Lemma 2.4 τ is a congruence on S. Let $\psi : S/\tau \to T$ be the mapping defined by $s\tau \to (s\tau_i)\theta_i$ where $i = s\eta$. Then ψ is injective since each θ_i is an embedding. Furthermore, if $s, t \in S$ with $s\eta = i, t\eta = j$, then, setting $(st)\eta = k$, we have $((s\tau)(t\tau))\psi = ((st)\tau)\psi = ((st)\tau_k)\theta_k = ((s\tau_k)(t\tau_k))\theta_k = ((s\tau_k)\theta_k)((t\tau_k)\theta_k) = ((s\tau_i)\theta_i)\phi_{ik} \cdot ((t\tau_j)\theta_j)\phi_{jk} = (s\tau)\psi \cdot (t\tau)\psi$, so ψ is also a homomorphism, and thus an embedding of S/τ in

T.

The mapping $\xi : S \to S/\beta \times T$ defined by $s \to (s\beta, (s\tau)\psi)$ is a homomorphism since β and τ are congruences and ψ is a homomorphism. If $s, t \in S$ and $s\xi = t\xi$, then $s\beta t$ and, since ψ is injective, $s\tau t$. Therefore $s = t$ by Lemma 2.8, so ξ is also injective and is thus an embedding of S in the orthocryptogroup $S/\beta \times T$.

We note that a semigroup S with identity satisfies both of the implications $\{u_\alpha = v_\alpha\}_{\alpha \in A} \to w = z$ and $\{u_\beta = v_\beta\}_{\beta \in B} \to w' = z'$ (where we assume that the sets of variables appearing in the two implications are disjoint) if and only if S satisfies the implication $\{u_\alpha = v_\alpha\}_{\alpha \in A}, \{u_\beta = v_\beta\}_{\beta \in B} \to ww' = zz'$. Therefore the implications of Theorem 2.9 can be replaced by a countable sequence $(I_1), (I_2), (I_3), \ldots$ of implications with the property that if S satisfies (I_n), then S satisfies (I_k) for $k \leq n$.

3. Semigroups embeddable in $\mathcal{V}$-orthocryptogroups. Let $\mathcal{V}$ be a variety of bands. An *orthocryptogroup* S is said to be a *$\mathcal{V}$-orthocryptogroup* if the greatest band homomorphic image of S belongs to $\mathcal{V}$, that is, if S is an orthodox $\mathcal{V}$-band of groups. The class of $\mathcal{V}$-orthocryptogroups is clearly a variety of type $\langle 2, 1 \rangle$. Unlike the situation for orthocryptogroups in general, it is not necessarily true that S is embeddable in a $\mathcal{V}$-orthocryptogroup if and only if S^1 is. Therefore, unlike §2 in which conditions for embeddability were given in terms of semigroups with identity, we now obtain implications which define the class of *semigroups* which are embeddable in $\mathcal{V}$-orthocryptogroups.

We begin by obtaining implications which define the class of semigroups which are embeddable in groups. As in §2 $M = \{(M_m) : m = 1, 2, 3, \ldots\}$ denotes a family of implications such that a semigroup S with identity is embeddable in a group if and only if S satisfies each $(M_m), m \geq 1$. The complication which results from working with semigroups rather than semigroups with identity is that each implication (M_m) must be replaced by a finite set M_m^* of implications. We use the notation preceeding Lemma 2.5. For each subset Q of P_m let $(M_m(Q))$ denote the implication obtained by substituting the empty word Λ for each variable from Q which appears in (M_m), and then replacing each equation of the form $t = \Lambda$ or $\Lambda = t$ (where $t \neq \Lambda$) by $t = t^2$, and replacing each equation of the form $\Lambda = \Lambda$ by $u = u$ (where u is any variable). Let $M_m^* = \{(M_m(Q)) : Q \subseteq P_m\}$, let (M_0) denote the implication $u = u^2, v = v^2 \to u = v$, and let $M^* = (\bigcup_{m=1}^{\infty} M_m^*) \cup (M_0)$.

LEMMA 3.1. *A semigroup S is embeddable in a group if and only if S satisfies each implication in M^*.*

PROOF. Suppose S is embedded in the group G. Then S^1 is embedded in G and the sole idempotent 1 of S is the identity of G. The implication (M_0) is clearly satisfied by S. Let m be a positive integer, let Q be a subset of P_m, and suppose the equations on the left-hand side of the implication $(M_m(Q))$ are satisfied by elements of S. Then these same elements of S, together with 1, comprise a set of elements from S^1 which satisfy (M_m) when all variables in Q are set equal to 1 (for, since S is embedded in G, if $a_1, \ldots, a_n$ are elements of S which satisfy $t = t^2$ where $t = t(x_1, \ldots, x_n)$, then $t(a_1, \ldots, a_n) = 1$ in S^1). Therefore the right-hand side, say $w = z$, of (M_m) is satisfied by these elements of S^1, and thus the right-hand side, say $w' = z'$, of $(M_m(Q))$ is satisfied by the required elements of S.

Conversely, suppose that S satisfies each implication in M^*. Let m be a positive integer and suppose the equations on the left-hand side of (M_m) are satisfied by elements of S^1. Then these elements, other than 1, satisfy the equations on the left-hand side of $M_m(Q)$ where Q is the set of variables in (M_m) which are assigned the value 1. Hence the right-hand side, say $w' = z'$, of $(M_m(Q))$ is satisfied, and hence the right-hand side, say $w = z$, of (M_m) is satisfied (in case $w' = z'$ has the form $t = t^2$ and $t(a_1, \ldots, a_n) = t(a_1, \ldots, a_n)^2$, we conclude that $t(a_1, \ldots, a_n) = 1$ applying (M_0)). Since each (M_m) is thus satisfied by S^1 we conclude that S^1, and thus S, is embeddable in a group.

We let $\overline{M^*}$ be the family of implications obtained from M^* in the same way that $\overline{M}$ was obtained from M; that is, if the implication (I) belongs to M^*, then each side of each equation of (I) is pre-multiplied and post-multipled by $p_I y$, where p_I is a word containing all the variables used in (I) and no other variables, and where y is a variable which does not appear in (I).

Any variety $\mathcal{V}$ of bands is, apart from the equation which guarantees associativity, determined by the equation $x = x^2$ and, in case $\mathcal{V}$ is a proper subvariety of the variety of all bands, by one more equation of the form $u = v$ [**1,7,8**]. If S is any semigroup, then the least $\mathcal{V}$-congruence $\beta_{\mathcal{V}}$ on S is generated by the relation $\{(x, x^2), (u(x_1, \ldots, x_n), v(x_1, \ldots, x_n)) : x, x_1, \ldots, x_n \in S\}$. A family of equations can be used to characterize those pairs of elements which are $\beta_{\mathcal{V}}$-related in S, by analogy with Lemma 2.2.

First suppose $\mathcal{V}$ is a proper subvariety of the variety of all bands. A *$\beta_{\mathcal{V}}$-sequence* is a finite sequence $b_1, b_2, \ldots, b_m$ of length $m \geq 1$ where each b_i is one of the symbols in the set $\{L, L^*, R, R^*\}$. Any $\beta_{\mathcal{V}}$-sequence B of length m determines a sequence B_m of $m+1$ equations $F_0, F_1, \ldots, F_m$ in the $m(n+2)+2$ variables x, y, x_{ij}, g_i, h_i, where $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots n$, as follows.

$$F_0 : x = g_1 z_0 h_1,$$
$$F_i : g_i w_i h_i = g_{i+1} z_i h_{i+1}, \; i = 1, 2, \ldots, m-1,$$
$$F_m : g_m w_m h_m = y,$$

where, for $i = 0, 1, \ldots, m-1$

$$z_i = \begin{cases} x_{i+1} & \text{if } b_{i+1} = L \\ x_{i+1}^2 & \text{if } b_{i+1} = L^* \\ u(x_{1,i+1}, \cdots, x_{n,i+1}) & \text{if } b_{i+1} = R \\ v(x_{1,i+1}, \cdots, x_{n,i+1} & \text{if } b_{i+1} = R^*, \end{cases}$$

and, for $i = 1, 2, \ldots, m$,

$$w_i = \begin{cases} x_i & \text{if } b_i = L^* \\ x_i^2 & \text{if } b_i = L \\ u(x_{1,i+1}, \cdots, x_{n,i+1}) & \text{if } b_i = R^* \\ v(x_{1,i+1}, \cdots, x_{n,i+1}) & \text{if } b_i = R. \end{cases}$$

If $\mathcal{V}$ is the variety of all bands the situation is simplified by the absence of the equation $u = v$. Specifically, a $\beta_{\mathcal{V}}$-sequence is now a finite sequence $b_1, b_2, \cdots, b_m$ of length $m \geq 1$ where each $b_i \in \{L, L^*\}$. Any $\beta_{\mathcal{V}}$-sequence B of length m determines a sequence B_m of $m+1$ equations $F_0, F_1, \cdots, F_m$ as defined above in the $3m+2$ variables x, y, x_i, g_i, h_i where $i = 1, 2, \cdots, m$.

Now if $\mathcal{V}$ is either the variety of all bands or a proper subvariety, for every subset Q of the set $G_m = \{g_i, h_i : i = 1, 2, \cdots, m\}$, let $B_m(Q)$ denote the sequence of equations obtained from B_m by deleting each occurence of each element of Q in the equations of B_m. Let $B_m^* = \{B_m(Q) : Q \subseteq G_m\}$ and let $J_{\mathcal{V}}^* = \bigcup_{m=1}^{\infty} B_m^*$. The elements of $J_{\mathcal{V}}^*$ are thus finite sequences of equations. Since each sequence of elementary $(\beta_{\mathcal{V}})_0$-transitions is associated with some element of $J_{\mathcal{V}}^*$ we have the following result.

LEMMA 3.2. *Let S be a semigroup. Then $a\beta_{\mathcal{V}}b$ if and only if there exists some element J of $J_{\mathcal{V}}^*$ and elements of S for which the equations* *in J are satisfied when the values a and b are assigned to x and y respectively.*

Let $K^*_{\mathcal{V}}$ denote the family consisting of all implications

$$\left.\begin{array}{r} r_1zr_2 = r_1wr_2 \\ y = xr_1zr_2x \\ J \end{array}\right\} \rightarrow xzx = xwx$$

for J an element of $J^*_{\mathcal{V}}$ and let $L^*_{\mathcal{V}}$ denote the family consisting of all implications

$$\left.\begin{array}{r} x^3 = xyx \\ J \end{array}\right\} \rightarrow x = y$$

for J an element of $J^*_{\mathcal{V}}$.

THEOREM 3.3. *Let $\mathcal{V}$ be a variety of bands. A semigroup S is embeddable in a $\mathcal{V}$-orthocryptogroup if and only if S satisfies each implication in $K^*_{\mathcal{V}}, L^*_{\mathcal{V}}$ and $\overline{M^*}$.*

PROOF. The result follows from the observation that Lemmas 2.2 through 2.8 hold if "semigroup with identity" is replaced by "semigroup", "orthogroup" and "orthocryptogroup" are replaced by "$\mathcal{V}$-orthocryptogroup", "β" is replaced by "$\beta_{\mathcal{V}}$", and the families $\{J_m : m \geq 1\}, \{(K_m) : m \geq 1\}, \{(L_m) : m \geq 1\}$ and $\{(\overline{M}_m) : m \geq 1\}$ are replaced by $J^*_{\mathcal{V}}, K^*_{\mathcal{V}}, L^*_{\mathcal{V}}$ and $\overline{M^*}$ respectively. In fact, with these replacements the proofs of the lemmas hold verbatim with one exception; in Lemma 2.3 the fact that $\beta \subseteq \eta$ was used. In general, for a semigroup S, $\beta_{\mathcal{V}}$ need not be contained in η. If $\mathcal{V}$ contains the variety of semilattices, however, then $\beta_{\mathcal{V}} \subseteq \eta$ and the proof of Lemma 2.3, with the replacements above, is valid. It remains to establish the analogue of Lemma 2.3 for $\mathcal{V}$ a variety of bands contained in the variety of rectangular bands. So suppose the semigroup S is embedded in the rectangular group T. If a, b, c_1, c_2 and d are elements of S such that $c_1ac_2 = c_1bc_2$, then since T is a rectangular group we have $a\sigma_T b$, where σ_T denotes the least group congruence on T. Hence $dad\sigma_T dbd$. But dad and dbd belong to the same maximal subgroup of T and so $dad = dbd$ since σ_T restricts to the equality on subgroups of a rectangular group. Therefore S satisfies the implication $r_1zr_2 = r_1wr_2 \rightarrow xzx = xwx$, and thus S satisfies each implication in $K^*_{\mathcal{V}}$. This establishes the analogue of Lemma 2.3 and thus completes the proof of the theorem.

Acknowledgement. The authors wish to thank R.A. Schutt for some stimulating questions concerning the possible existence of cancellative semigroups which are embeddable in certain classes of completely regular semigroups but are not embeddable in groups.

References

1. A.P. Birjukov, *Varieties of idempotent semigroups,* Algebra i Logika **9**(1970), 255-273 (in Russian); Transl. Algebra and Logic, Consult. Bureau **9** (1970), 153-164.

2. N. Bouleau, *Classes de semigroupes immersibles dans des groupes,* Semigroup Forum **6** (1973), 100-112.

3. N. Bouleau, *Conditions unilatérales d'immersibilité d'un semigroupe dans un groupe et un contre-exemple a un resultat de A.H. Clifford et G. B. Preston,* J. Algebra **24** (1973), 213-218.

4. G. Bush, *The embedding theorems of Malcev and Lambek,* Canad. J. Math. **15** (1963), 49-58.

5. A.H. Clifford and G.B. Preston, *The Algebraic Theory of Semigroups,* Vol. 2, American Mathematical Society, Providence, 1967.

6. R. Doss, *Sur l'immersion d'un semi-groupe dans un groupe,* Bull. Sci. Math. (2) **72**(1948), 139-150.

7. C.F. Fennemore, *All varieties of bands,* Math. Nachr. **48** (1971), I:237-252, II: 253-262.

8. J.A. Gerhard, *The lattice of equational classes of idempotent semigroups,* J. Algebra **15** (1970), 195-224.

9. J.A. Gerhard and M. Petrich, *The word problem for orthogroups,* Canad. J. Math. **33** (1981), 893-900.

10. G. Grätzer, *Universal algebra,* Second edition, Springer-Verlag, New York, 1979.

11. J.M. Howie, *An Introduction to Semigroup Theory,* Academic Press, New York, 1979.

12. J. Lambek, *The immersibility of a semigroup into a group,* Canad. J. Math. **3** (1951), 34-43.

13. A.I. Malcev, *On the immersion of associative systems in groups,* Mat. Sbornik (N.S.) **6** (1939), 331-336 and **8** (1940), 251-264 (in Russian).

14. A.I. Malcev, *Algebraic Systems,* Springer-Verlag, Berlin, 1973.

15. K. Osondu, *The universal group of homogeneous quotients,* Semigroup Forum **21** (1980), 143-152.

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

17. V. Pták, *Immersibility of semigroups,* Acta Fac. Nat. Univ. Carol. Prague **192** (1949), 16 pp.

18. B.M. Schein, *Embedding semigroups in generalized groups,* Mat. Sbornik (N.S.) **55**(1961), 379-400 (in Russian).

19. B.M. Schein, *A system of axioms for semigroups imbeddable in generalized groups,* Soviet Math. **1** (1960), 1180-1183.

20. R.A. Schutt, private communication.

21. A. Selman, *Completeness of calculi for axiomatically defined classes of algebras,* Alg. Univ. **2** (1972), 20-32.

22. W. Taylor, *Equational logic,* Houston J. Math. (1979), (iii), 83.

23. P.G. Trotter, *A class of semigroups embeddable in groups,* Semigroup Forum **5** (1972), 1-13.

Department of Mathematics, Marquette University, Milwaukee, WI 53233.