TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 172, October 1972

FINITE COMMUTATIVE SUBDIRECTLY IRREDUCIBLE SEMIGROUPS

BY

PHILLIP E. McNEIL

ABSTRACT. This paper is devoted to completing the solution to the problem of constructing all finite commutative subdirectly irreducible semigroups. Those semigroups of this type which were formerly unknown are realized as certain permutation group extensions of nilpotent semigroups. The results in this paper extend the efforts in this area by G. Thierrin and B. M. Schein.

1. **Introduction.** One approach to the problem of determining the structure of algebraic semigroups is the well-known theorem of G. Birkhoff [1] applied to semigroups: Every semigroup has a decomposition into a subdirect product of subdirectly irreducible semigroups. This leads naturally to a search for the structure of these latter semigroups, and in particular, those which are finite and commutative. G. Thierrin [10] and B. M. Schein [7] pioneered the efforts in this area, and D. Zitarelli [13] has made a study of inverse subdirectly irreducible semigroups. In this paper we present the structure of all finite commutative subdirectly irreducible semigroups which were heretofore unknown, namely, those which are ideal extensions of nilpotent semigroups by groups with zero (we will refer to these as *group extensions*). Our results rest heavily upon extension theory of semigroups, and we refer the reader to Clifford and Preston [4] for background material. Moreover, we show a connection with the theory of finite permutation groups, and our terminology in this area is that of Wielandt [11].

2. **Preliminaries.** Let S be a semigroup. A transformation λ of S, written as a left operator, is a *left translation* of S if $\lambda(xy) = (\lambda x)y$ for all x, y in S; a transformation ρ of S, written as a right operator, is a *right translation* of S if $(xy)\rho = x(y\rho)$ for all x, y in S. A pair (λ, ρ) consisting of a left translation λ and a right translation ρ with the property that $x(\lambda y) = (x\rho)y$ for all x, y in S is called a *bitranslation* of S. The collections $\Lambda(S)$, $P(S)$ of all left translations, right translations of S are semigroups under the operation of mapping composition; the collection $\Omega(S)$ of all bitranslations of S with multiplication induced by the direct product $\Lambda(S) \times P(S)$ is a semigroup called the *translational hull* of S.

Presented to the Society, September 3, 1971; received by the editors June 2, 1971.
AMS 1970 *subject classifications.* Primary 20M10.
Key words and phrases. Subdirectly irreducible semigroup, nilpotent semigroup, permutation group, ideal extension.

Definition. A semigroup S with zero having more than one element is called *nilpotent* if there is a positive integer n such that the product of any n elements is zero. If h is the smallest such positive integer, we say that S has *height* h.

What follows is a list of known properties of finite nilpotent semigroups; see Tamura [9], Sedlock [8] or McNeil [5] for proofs and details. Let N be a finite nilpotent semigroup of height h, and let $x, y \in N$. The element x is said to be a *multiple* of y if

$$x \in Ny \cup yN \cup NyN$$

(Ny denotes the set of all elements in N of the form ay, $a \in N$). The relation $\leq$ defined on N by "$x \leq y$ if and only if $x = y$ or x is a multiple of y" is a partial ordering of N. The elements of N which are maximal relative to $\leq$ are called *primes*. Since N is finite, it has at least one prime, and the set X of all primes of N is the unique minimum set of generators for N. Let $x_1, \cdots, x_m$ denote the elements of X. A relation $x_{i_1} \cdots x_{i_r} = x_{j_1} \cdots x_{j_s}$ among the generators is called *nontrivial* if at least one of the integers r, s is less than h and $x_{i_\alpha} \neq x_{j_\alpha}$ for some α, $1 \leq \alpha \leq \min\{r, s\}$. The triple (X, R, h) consisting of the minimum generating set X, the nontrivial relations R on X and the height h completely determine N except for isomorphism; hence we write $N = (X, R, h)$. Note that if $h = 2$, R is empty.

For each positive integer r we refer to the set $L_r = \{s \in N \mid s$ is a product of r generators$\}$ as *layer* r *of* N. Note that $L_1 = X$ and $L_r = \{0\}$ for all $r \geq h$ (*zero layers*); also, if $1 \leq r < h$, L_r has at least one nonzero element, otherwise the minimality of h is violated.

A nontrivial relation $x_{i_1} \cdots x_{i_r} = x_{j_1} \cdots x_{j_s}$ is called a *layer* r *relation* if $r = s$, otherwise it is referred to as a *skew relation*. If the layer relations $x_i x_j = x_j x_i$ hold in N for all i, j, $1 \leq i, j \leq m$, then N is commutative. For the remainder of this paper all nilpotent semigroups discussed will be assumed finite and commutative.

Let $x_{i_1} \cdots x_{i_r} = x_{j_1} \cdots x_{j_r}$ be any layer r relation of N. If s is an integer such that $r < s < h$, then the relations

$$\{(x_{i_1} \cdots x_{i_r})a = (x_{j_1} \cdots x_{j_r})a \mid a \in L_{s-r}\}$$

are called the *layer* s *relations induced by* $x_{i_1} \cdots x_{i_r} = x_{j_1} \cdots x_{j_r}$.

If $|X| = m = p^n$, some prime p and positive integer n, we denote by $\mathfrak{R}$ the following layer relations in N:

$$\mathfrak{R} = \left\{ x_{i_1} \cdots x_{i_r} = x_{j_1} \cdots x_{j_r} \;\middle|\; \sum_{\alpha=1}^{r} i_\alpha \equiv \sum_{\alpha=1}^{r} j_\alpha \pmod{p^n},\ r = 2, \cdots, h-1 \right\}.$$

3. **Permutation extensions.** Given semigroups S and T, a semigroup U is called an *ideal extension of* S *by* T^0 (T with zero) if S is an ideal of U and the Rees quotient U/S is isomorphic to T^0.

Definition. Let G be a group and N be a nilpotent semigroup. A homomorphism $\phi: G \to \Lambda(N) \times P(N)$ is called *permutable* if, for any g, h in G and s in N, $(\lambda_g s)\rho_h = \lambda_g(s\rho_h)$, where (λ_g, ρ_g) and (λ_h, ρ_h) denote the images of g and h under ϕ, respectively.

The following theorem is an analogue of a theorem of Clifford [3] and is a special case of a result due to Yoshida [12]:

Theorem 3.1. *Let $S = G \cup N$, where G is a group and N is a nilpotent semigroup, and let $\phi: g \to (\lambda_g, \rho_g)$ be a permutable homomorphism of G into $\Omega(N)$. Denoting multiplication in N and in G by juxtaposition, define a multiplication $\circ$ on the set S by*

$$\begin{aligned} s \circ t &= st && (s, t \in N),\\ g \circ h &= gh && (g, h \in G),\\ g \circ s &= \lambda_g s && (g \in G, s \in N),\\ s \circ g &= s\rho_g && (s \in N, g \in G). \end{aligned}$$

Then $(S, \circ)$ is a group extension of N by G^0. Conversely, any group extension of N is determined in this manner by a permutable homomorphism.

We now construct a particular group extension which plays a prominent role in our discussion of subdirectly irreducible semigroups. Let $N = (X, R, h)$ be a nilpotent semigroup with generators $X = \{x_1, \cdots, x_{p^n}\}$ for some prime p and positive integer n. For each j, $1 \le j \le p^n$, define a permutation g_j of X as follows: for $x_i \in X$,

$$g_j: x_i \to x_k \quad \text{if } k \equiv i + j - 1 \pmod{p^n}.$$

One can verify that the collection $\mathfrak{G}(X) = \{g_1, \cdots, g_{p^n}\}$ forms a cyclic transitive group of permutations on X; indeed, since $|X| = |\mathfrak{G}(X)| = p^n$, it is up to isomorphism the only cyclic transitive permutation group on X. We note that g_j is a generator of $\mathfrak{G}(X)$ if and only if $\gcd\{j - 1, p^n\} = 1$.

For each g_j in $\mathfrak{G}(X)$ define mappings λ_j, ρ_j on N as follows: $\lambda_j x_i = x_i \rho_j = g_j x_i$ for all $x_i \in X$ and

$$\lambda_j(x_{i_1} \cdots x_{i_r}) = (g_j x_{i_1})(x_{i_2} \cdots x_{i_r}),$$

$$(x_{i_1} \cdots x_{i_r})\rho_j = (x_{i_1} \cdots x_{i_{r-1}})(g_j x_{i_r}),$$

$$(x_{i_1} \cdots x_{i_r} \in N,\ r \ge 2).$$

It is easy to see that $\lambda_j \in \Lambda(N)$ and $\rho_j \in P(N)$. Further, $\Gamma(N) = \{(\lambda_j, \rho_j) \mid j = 1, \cdots, p^n\}$ is a subgroup of $\Lambda(N) \times P(N)$ which is isomorphic to $\mathfrak{G}(X)$, for the mapping $\phi: g_j \to (\lambda_j, \rho_j)$ is a permutable isomorphism. If $h = 2$, then $\Gamma(N) \subseteq \Omega(N)$, and, by Theorem 3.1, ϕ determines a group extension of N by $\mathfrak{G}(X)$. However, $\Gamma(N)$ is not necessarily a subset of $\Omega(N)$ for $h > 2$. The following theorem provides a condition on N which assures that the isomorphism ϕ determines an extension.

Theorem 3.2. *If N, $\mathfrak{G}(X)$, $\Gamma(N)$ are as described above with $h > 2$, then the isomorphism ϕ: $g_j \to (\lambda_j, \rho_j)$ determines an extension of N by $\mathfrak{G}(X)$ in the sense of Theorem 3.1 if and only if $\mathfrak{R} \subseteq R$.*

Proof. Sufficiency. By Theorem 3.1 we need only show that $\Gamma(N) \subseteq \Omega(N)$. Let $(\lambda_j, \rho_j) \in \Gamma(N)$, and let x_i, x_k be any two elements of X. Then

$$x_i(\lambda_j x_k) = x_i x_u \quad \text{where} \quad u \equiv j + k - 1 \pmod{p^n},$$

$$(x_i \rho_j) x_k = x_v x_k \quad \text{where} \quad v \equiv i + j - 1 \pmod{p^n}.$$

It follows that $i + u \equiv v + k \pmod{p^n}$, whence $x_i x_u = x_v x_k$ since $\mathfrak{R} \subseteq R$. Thus (λ_j, ρ_j) satisfies the bitranslation property for any two generators of N; it is immediate that $(\lambda_j, \rho_j) \in \Omega(N)$.

Necessity. Assume that ϕ determines a group extension $S = \mathfrak{G}(X) \cup N$. (For convenience of notation here and in the remainder of the paper, we denote all multiplication in S by juxtaposition. Thus if $g_i \in \mathfrak{G}(X)$ and $x_{i_1} \cdots x_{i_r} \in N$, then $g_i(x_{i_1} \cdots x_{i_r})$ denotes the multiplication of these two elements in the semigroup S as determined by the isomorphism ϕ: $g_j \to (\lambda_j, \rho_j)$ and Theorem 3.1. Accordingly, if $r > 1$, then $g_i(x_{i_1} \cdots x_{i_r}) = (g_i x_{i_1})(x_{i_2} \cdots x_{i_r})$, where $g_i x_{i_1}$ denotes the image of x_{i_1} under the permutation g_i.) That the relations $\mathfrak{R}$ hold in N will be a consequence of the following claim:

Claim 3.3. For any r, $1 < r < h$, each element of L_r equals one of the elements

$$x_1^r,\ x_1^{r-1}x_2,\ \cdots,\ x_1^{r-1}x_{p^n}. \tag{1}$$

Proof of the claim. First consider the case in which $r = 2$, and let $x_i x_j$ be any element in L_2. By the commutativity of N, we have $g_i(x_1 x_j) = g_i(x_j x_1)$, whence by the definition of g_i,

$$x_i x_j = x_k x_1 = x_1 x_k \quad \text{where } k \equiv i + j - 1 \pmod{p^n}. \tag{2}$$

Thus if $x_{i_1} \cdots x_{i_r}$ is any element in L_r, $2 < r < h$, repeated application of (2) yields

$$x_{i_1} \cdots x_{i_r} = x_1^{r-1} x_k \quad \text{where} \quad \sum_{\alpha=1}^{r} i_\alpha \equiv (r-1) + k \pmod{p^n},$$

completing the proof of the claim.

Now, for any r, $1 < r < h$, let $x_{i_1} \cdots x_{i_r}$ and $x_{j_1} \cdots x_{j_r}$ be elements in L_r such that $\Sigma i_\alpha \equiv \Sigma j_\alpha \pmod{p^n}$. By Claim 3.3 we have

$$x_{i_1} \cdots x_{i_r} = x_1^{r-1} x_k \quad \text{where} \quad \sum i_\alpha \equiv (r-1) + k \pmod{p^n}.$$

$$x_{j_1} \cdots x_{j_r} = x_1^{r-1} x_l \quad \text{where} \quad \sum j_\alpha \equiv (r-1) + l \pmod{p^n}.$$

Therefore $(r-1) + k \equiv (r-1) + l \pmod{p^n}$, and since $k, l \leq p^n$, we must have $k = l$, and consequently $x_{i_1} \cdots x_{i_r} = x_{j_1} \cdots x_{j_r}$.

Definition. If $N = (X, R, b)$ with $|X| = p^n$ and $\mathfrak{R} \subseteq R$, the group extension of N determined by the isomorphism ϕ: $\mathfrak{G}(X) \to \Gamma(N)$ described above is called the *permutation extension* of N.

We conclude this section by listing further properties of permutation extensions. For the remainder of this section let $\mathfrak{G}(X) \cup N$ be a fixed permutation extension.

Property 3.4. All of the elements in any layer L_r of N, $r > 1$, can be obtained by multiplying each generatior by x_1^{r-1}. (This follows from Claim 3.3.)

Property 3.5. $\mathfrak{R} = R$ if and only if for each r, $1 < r < n$, no two elements of (1) are equal. (In this case each nonzero layer L_r consists of the p^n distinct elements of the form (1).)

Proof. Necessity. If $\mathfrak{R}$ are the only nontrivial relations on N, then since the integers $(r-1) + 1, (r-1) + 2, \cdots, (r-1) + p^n$ form a complete residue class modulo p^n, it is clear that the elements in (1) are distinct for each r, $1 < r < b$.

Sufficiency. It is evident from Claim 3.3 that if the elements in (1) are distinct in all nonzero layers, then $\mathfrak{R}$ are the only layer relations which hold in N. We need only show that under the same hypothesis, N has no skew relations. Seeking a contradiction, suppose that N has a skew relation, $x_1^{r-1}x_i = x_1^{s-1}x_j$, $s > r$ (recall Property 3.4). Since $\mathfrak{G}(X)$ is transitive on X, there is an element $g \in \mathfrak{G}(X)$ which maps x_i onto x_1. Multiplying both sides of the relation by g yields a relation of the form

$$x_1^r = x_1^{s-1}x_k, \qquad s > r. \tag{3}$$

Now if we multiply both sides of (3) by x_1^{b-r-1}, we have $x_1^{b-1} = 0$, since $x_1^{s-1}x_k x^{b-r-1}$ belongs to a zero layer. Similarly, if we multiply both sides of (3) by $x_1^{b-r-2}x_j$, with $j \neq 1$, we obtain $x_1^{b-2}x_j = 0$. The foregoing shows that $x_1^{b-1} = x_1^{b-2}x_j$, $j \neq 1$, in layer $b-1$, and this contradicts the hypothesis that the elements of (1) are distinct in all nonzero layers, completing the proof of the property.

Let g be any element in $\mathfrak{G}(X)$, and let $g = (x_{i_1} \cdots x_{i_k})(x_{j_1} \cdots x_{j_l}) \cdots$ be the decomposition of g into disjoint cycles. Writing $C_1 = \{x_{i_1}, \cdots, x_{i_k}\}$, $C_2 = \{x_{j_1}, \cdots, x_{j_l}\}, \cdots$, we use the notation $g = C_1C_2 \cdots$ to denote the cycle decomposition of g. For any r, $1 < r < b$, the sets $C_1^r = \{x_1^{r-1}x_{i_1}, \cdots, x_1^{r-1}x_{i_k}\}$, $C_2^r = \{x_1^{r-1}x_{j_1}, \cdots, x_1^{r-1}x_{j_l}\}, \cdots$ are called rth *layer cycles* of g. Applying Property 3.5 we obtain

Property 3.6. If $\mathfrak{R} = R$, the rth layer cycles of any element of $\mathfrak{G}(X)$ are disjoint sets, and no two elements in a given nonsingleton rth layer cycle are equal.

Definition 3.7. Let $x_{i_1} \cdots x_{i_r} = x_{j_1} \cdots x_{j_r}$ be a layer r relation in N, $1 < r < b$. The set of layer r relations

$$\{(x_{i_1} \cdots x_{i_r})g_j = (x_{j_1} \cdots x_{j_r})g_j \mid j = 1, 2, \cdots, p^n\}$$

is called the layer r relations *induced by* $\mathfrak{G}(X)$ *acting on* $x_{i_1} \cdots x_{i_r} = x_{j_1} \cdots x_{j_r}$.

4. **Finite commutative subdirectly irreducible semigroups.** The starting point for any discussion of these semigroups must be the following result due to B. M. Schein [7]:

Theorem 4.1. *A finite commutative subdirectly irreducible semigroup is either* (i) *a nilpotent semigroup,* (ii) *a group (possibly with zero), or* (iii) *a group extension of a nilpotent semigroup; moreover if the group is nontrivial in* (ii) *and* (iii), *it is a cyclic p-group for some prime p.*

Since Schein has characterized subdirectly irreducible nilpotent semigroups in [7], and since it is easily shown that any cyclic p-group is subdirectly irreducible, the question remaining is: which of the semigroups of type (iii) are subdirectly irreducible? The author has constructed a number of semigroups of type (iii) which are subdirectly irreducible (see Theorem 4.9 below or [6]), but the general problem has been heretofore unsolved. In this section we establish the following solution to the problem: a type (iii) semigroup (with nontrivial group) is subdirectly irreducible if and only if it is a permutation extension of a nilpotent semigroup whose only nontrivial relations are $\mathfrak{R}$.

We will first of all list some general properties of subdirectly irreducible semigroups as well as some properties of subdirectly irreducible semigroups of type (iii).

Property 4.2. A semigroup S is subdirectly irreducible if and only if the intersection of all nonequality congruences on S is not the equality congruence (Birkhoff [2]).

Property 4.3. If S is subdirectly irreducible and commutative, then any idempotent of S is either the zero element or the identity element of S (Thierrin [10]).

Property 4.4. A semigroup S is subdirectly irreducible if and only if S^0 (S^1) is subdirectly irreducible (Schein [7]).

Definition. Let S be a semigroup with zero. The relation ρ defined on S by "$a \equiv b(\rho)$ if for any $x, y, \in S^1$, $xay = 0$ if and only if $xby = 0$" is a congruence. If ρ is the equality congruence, then 0 is said to be *disjunctive.*

Property 4.5. A nilpotent semigroup is subdirectly irreducible if and only if its zero is disjunctive (Schein [7]).

For the remainder of the properties assume that S is a finite commutative subdirectly irreducible semigroup which is an extension of a nilpotent semigroup $N = (X, R, b)$ by a group G with zero, and let $\phi: g \to (\lambda_g, \rho_g)$ denote the homomorphism determining the extension. Notice that if $|G| = 1$, then the Properties 4.3 and 4.5 are applicable, so we assume in sequel that G is cyclic of order p^n, some prime p and positive integer n (recall Theorem 4.1).

Property 4.6. The homomorphism ϕ is 1-1, and it maps G into the diagonal of $\Omega(N)$, i.e. those $(\lambda, \rho) \in \Omega(N)$ such that $\lambda s = s\rho$ for all $s \in N$.

Proof. If ϕ is not 1-1, then the equivalence relation σ defined on S by "$a \equiv b(\sigma)$ if $\phi a = \phi b$ or $a = b$" is a nonequality congruence. If τ is the nonequality congruence on S whose only nonsingleton class is the set N, then $\sigma \cap \tau$ is the equality congruence, and we have contradicted the subdirect irreducibility of S by Property 4.2.

Let $s \in N$ and $g \in G$. Then since S is commutative, $\lambda_g s = gs = sg = s\rho_g$, whence (λ_g, ρ_g) is in the diagonal of $\Omega(N)$.

Property 4.7. G is isomorphic to a subgroup of $\mathfrak{P}(X)$, the group of permutations on X.

Proof. First note that by Property 4.3 the identity 1 of G is the identity for all of S. This implies that $\phi 1 = (\lambda_1, \rho_1)$ is the identity bitranslation of $\Omega(N)$. It follows that $\phi(G)$ is a subgroup of the maximal subgroup of $\Omega(N)$ containing the identity bitranslation. Further, since from Property 4.6 ϕ is an isomorphism into the diagonal of $\Omega(N)$, it is clear that G is isomorphic to a subgroup of the maximal subgroup of $\Lambda(N)$ containing the identity left translation, ι. (To see this, merely project the image $\phi(G)$ into $\Lambda(N)$.) Denote this latter maximal subgroup by H_ι.

If λ is any element in H_ι, then λ maps the generators X into themselves. For if $\lambda x_i \in L_r$, some $x_i \in X$ and $r > 1$, then clearly $\lambda^m x_i \neq x_i$ for all positive integers m, contradicting the fact that some power of λ equals ι. Thus we may regard H_ι as a group of permutations on the set X, and since $\mathfrak{P}(X)$ is the maximal such group, the property has been proved.

Definition. Let G be a permutation group on X and let x be an element in X. The set $\{y \in X \mid gy = x \text{ for some } g \in G\}$ is called the *orbit* of x.

Note that G is transitive if and only if the orbits of any two of its elements have a nonempty intersection or, equivalently, the orbit of each element of X is X itself.

Property 4.8. $|X| = p^n$, $\mathfrak{R} \subseteq R$ and S is isomorphic to the permutation extension of N.

Proof. Using Property 4.7, identify G and its isomorphic copy in $\mathfrak{P}(X)$. We claim that G is a transitive group of permutations on X. For suppose that Y and Z are disjoint orbits of elements of X. Then Y and Z can be used to define equivalence relations σ and τ on S as follows.

(1) σ is defined to be equality on G.

(2) For $a, b \in N$, define

$$a \equiv b(\sigma) \quad \text{if} \quad \begin{cases} a, b \in Y \cup 0, & \text{or} \\ a = x_{i_1} \cdots x_{i_r},\ b = x_{j_1} \cdots x_{j_r},\ 1 < r < h, & \\ \quad \text{where } x_{i_1}, x_{j_1} \in Y \text{ and } x_{i_\alpha} = x_{j_\alpha},\ \alpha = 2, \cdots, r, & \text{or} \\ a = b. & \end{cases}$$

Similarly define the relation τ on S by replacing Y by Z in (1) and (2) above. It is a matter of direct calculation to show that σ and τ are nonequality congruences on S whose intersection is equality. This contradicts the subdirect irreducibility of S. Therefore, the orbits of any two elements of X intersect, and G is a transitive cyclic group of permutations on X of order p^n. Let $a \in G$ be a generator of G. Since G is transitive, the decomposition of the permutation a into disjoint cycles yields a single cycle which consists of precisely the elements of X. Furthermore, since G has order p^n, it follows that $|X| = p^n$. Any two transitive cyclic permutation groups of order p^n defined on a set of p^n elements are isomorphic; therefore G is isomorphic to $\mathfrak{G}(X)$. From Property 4.6 and the description of $\phi(G)$ given in the proof of Property 4.7, it follows that ϕ is the isomorphism of Theorem 3.2, whence $\mathfrak{R} \subseteq R$ and S is isomorphic to the permutation extension of N. This completes the proof of Property 4.8.

We may now summarize the results of the foregoing properties in this manner: any subdirectly irreducible semigroup of type (iii) whose group is nontrivial is up to isomorphism the permutation extension of a nilpotent semigroup. Therefore, the problem central to this paper shall have been solved when we know which nilpotent semigroups have subdirectly irreducible permutation extensions. The author has proved the next theorem in [6]:

Theorem 4.9. *If $N = (X, R, h)$, $|X| = p^n$ and $h = 2$, then the permutation extension of N is subdirectly irreducible.*

Our final result settles the question for nilpotent semigroups of arbitrary height greater than 2.

Theorem 4.10. *Let $N = (X, R, h)$, $h > 2$, where $X = \{x_1, \cdots, x_{p^n}\}$ and $\mathfrak{R} \subseteq R$. The permutation extension $S = \mathfrak{G}(X) \cup N$ is subdirectly irreducible if and only if $\mathfrak{R} = R$.*

Proof. Necessity. Suppose S is subdirectly irreducible. By Property 3.5 we need only show that the elements of (1) are distinct in each nonzero layer of N. Suppose that for some r, $1 < r < h$, two of the elements of (1) are equal, and assume that r is the smallest such positive integer. Since $\mathfrak{G}(X)$ is transitive, we lose no generality by supposing that the assumed relation has the form

$$x_1^r = x_1^{r-1} x_i, \quad \text{some } i > 1. \tag{4}$$

Let $d = \gcd\{i - 1, p^n\}$. Notice that since $d - 1$ and p^n are relatively prime, g_d is a generator of $\mathfrak{G}(X)$. Now if we multiply both sides of (4) by each of the elements $g_d, g_d^2, \cdots$ in turn, the result will be the p^n layer r relations induced in N by the action of $\mathfrak{G}(X)$ on (4) (see Definition 3.7). By the definition of multiplication in S, these induced relations have the form

$$x_1^{r-1}(x_1 g_d^t) = x_1^{r-1}(x_i g_d^t), \qquad t = 1, \cdots, p^n,$$

where $x_i g_d^t$ is the image of x_i under the permutation g_d^t. One can verify, after the application of the permutations, that these relations can be described by

$$x_1^{r-1}x_j = x_1^{r-1}x_k \quad \text{if and only if } j \equiv k \pmod{d}.$$

Thus if we let $m = (p^n/d) - 1$, we may write a tabular representation of the relations induced by the action of $\mathfrak{G}(X)$ on (4) as follows:

$$\begin{aligned}
&x_1^r = x_1^{r-1}x_{1+d} = x_1^{r-1}x_{1+2d} = \cdots = x_1^{r-1}x_{1+md} \\
&x_1^{r-1}x_2 = x_1^{r-1}x_{2+d} = x_1^{r-1}x_{2+2d} = \cdots = x_1^{r-1}x_{2+md} \\
&\quad\vdots \\
&x_1^{r-1}x_d = x_1^{r-1}x_{d+d} = x_1^{r-1}x_{d+2d} = \cdots = x_1^{r-1}x_{d+md}.
\end{aligned} \tag{5}$$

Also Property 3.4 implies that the relations in layers L_s, $r < s < h$, induced by the relations (5) are obtained by replacing the integer r in (5) by s.

Now consider the following partition of L_{r-1}:

$$\begin{aligned}
C_1 &= \{x_1^{r-1}, x_1^{r-2}x_{1+d}, x_1^{r-2}x_{1+2d}, \cdots, x_1^{r-2}x_{1+md}\} \\
C_2 &= \{x_1^{r-2}x_2, x_1^{r-2}x_{2+d}, x_1^{r-2}x_{2+2d}, \cdots, x_1^{r-2}x_{2+md}\} \\
&\vdots \\
C_d &= \{x_1^{r-2}x_d, x_1^{r-2}x_{d+d}, x_1^{r-2}x_{d+2d}, \cdots, x_1^{r-2}x_{d+md}\},
\end{aligned}$$

and let σ be the equivalence relation on S which coincides with the above partition on L_{r-1}, and which is equality elsewhere in S. Since for each $g_j \in \mathfrak{G}(X)$ and each partition class C_i, $g_j C_i \subseteq C_i$, and since for each $a \in N$ the product aC_i results in one of the relations in (5) or a layer relation induced by a relation in (5), it follows that σ is a congruence. Furthermore, σ is not the equality congruence. For since $d > 1$, each C_i has at least two elements, and no two of these elements are equal by the minimality of r.

Next let τ denote the congruence on S whose only nonsingleton class is $L_{h-1} \cup \{0\}$. (Note $L_{h-1} \neq \{0\}$ because N has height h.) Recalling that $r - 1 < h - 1$, we see that the nonsingleton classes of σ do not intersect $L_{h-1} \cup \{0\}$. It follows that $\sigma \cap \tau$ is the equality congruence, and this contradiction to the subdirect irreducibility of S completes the proof of the necessity part of the theorem.

Sufficiency. Assume that $\mathfrak{R} = R$. By Property 3.5 this implies that the totality of elements in each layer L_r, $1 < r < h$, is given by the p^n distinct elements of the form (1).

Let g_0 be any element of $\mathfrak{G}(X)$ of minimal order p, and let $g_0 = C_1 C_2 \cdots C_{p^n-1}$ denote its disjoint cycle decomposition. We shall show that S is subdirectly irreducible by establishing the following claim.

Claim. If θ is any nonequality congruence on S, then θ does not divide the $(h-1)$st layer cycles, $C_1^{h-1}, C_2^{h-1}, \cdots$, of g_0, i.e. the elements in each of the sets C_i^{h-1} are related modulo θ (cf. Property 3.6).

Proof of the claim. If θ is a nonequality congruence on S, then there exist two distinct elements of S which are related modulo θ. The possibilities for these two elements are exhausted in the following four cases:

(a) $x_1^{r-1}x_i \equiv x_1^{r-1}x_j(\theta)$, $i \neq j$,

(b) $x_1^{r-1}x_i \equiv x_1^{s-1}x_j(\theta)$, $s > r$,

(c) $g_i \equiv x_1^{r-1}x_j(\theta)$,

(d) $g_i \equiv g_j(\theta)$, $i \neq j$,

where $1 \leq i, j \leq p^n$ and $1 \leq r, s \leq h$. We show that if relation (a) holds, then θ does not divide the $(h-1)$st layer cycles of g_0; then we indicate that a relation of the form (a) results from each of the relations (b) through (d).

Toward this end let us assume that (a) holds, and let C_i denote the cycle of g_0 which contains x_i. By the transitivity of $\mathfrak{G}(X)$ there is an element $g \in \mathfrak{G}(X)$ such that $x_i g = x_j$. Let m denote the order of g and let $g = B_1 B_2 \cdots$ be the disjoint cycle decomposition of g. Then x_i and x_j belong to the same cycle B_k of g, and the elements $x_i, x_i g, \cdots, x_i g^{m-1}$ constitute the totality of elements in B_k. From this it follows that $x_1^{r-1}x_i, x_1^{r-1}x_i g, \cdots, x_1^{r-1}x_i g^{m-1}$ constitute the totality of elements in B_k^r. Since $x_1^{r-1}x_i \equiv x_1^{r-1}x_j(\theta)$, we have $x_1^{r-1}x_i \equiv x_1^{r-1}x_i g(\theta)$, whence

$$x_1^{r-1}x_i \equiv x_1^{r-1}x_i g \equiv \cdots \equiv x_1^{r-1}x_i g^{m-1}(\theta),$$

which says that B_k^r is indivisible by θ. Since g_0 has minimal order, it can be shown that $C_i \subseteq B_k$ (use Theorem 7.5 of [11] and the well-known property that the subgroups of $\mathfrak{G}(X)$ form a chain). This implies that $C_i^r \subseteq B_k^r$, which proves that C_i^r is indivisible by θ. Now if each element of C_i^r is multiplied by the element x_1^{h-r-1}, one sees that C_i^{h-1} is indivisible by θ. (Note that since $\mathfrak{R} = R$, Property 3.6 assures that C_i^{h-1} consists of p distinct elements.)

If C_i is the only p-cycle of g_0, we are finished with case (a); hence assume that g_0 has a cycle C_t different from C_i and let x_t be an element in C_t. By the transitivity of $\mathfrak{G}(X)$ there is an element g in $\mathfrak{G}(X)$ such that $x_i g = x_t$. Let $x_u = x_j g$. Then applying g to both sides of relation (a) we have $x_1^{r-1}x_t \equiv x_1^{r-1}x_u(\theta)$, where $t \neq u$ since $i \neq j$. Now a proof exactly like the proof that C_i^{h-1} is indivisible by θ shows that C_t^{h-1} is likewise indivisible. We conclude that each of the $(h-1)$st layer cycles of g_0 is indivisible by θ.

Suppose that (b) holds, and let $g \in \mathfrak{G}(X)$ be such that $x_i g = x_1$. Then multiplying g on both sides of (b) yields

$$x_1^r \equiv x_1^{s-1}x_k(\theta) \quad \text{where } x_k = x_j g. \tag{6}$$

Now if both sides of (6) are multiplied by x_1^{b-r-1}, we obtain $x_1^{b-1} \equiv O(\theta)$; and if both sides of (6) are multiplied by $x_1^{b-r-2}x_2$ we obtain $x_1^{b-1}x_2 \equiv O(\theta)$. Consequently, we have obtained the relation $x_1^{b-1} \equiv x_1^{b-2}x_2(\theta)$, a relation of the form (a).

If (c) holds, then multiplying both sides of (c) by x_1^{b-1} and then by $x_1^{b-2}x_2$ yields the type (a) relation $x_1^{b-2}x_i \equiv x_1^{b-2}x_k(\theta)$, where $x_k = x_2 g$.

Finally if (d) holds, the type (a) relation $x_1^{r-1}x_i \equiv x_1^{r-1}x_j(\theta)$, $i \neq j$, results from multiplying both sides of the relation (d) by x_1^r for any r, $1 \leq r < b$. This completes the proof of the claim. The proof of the sufficiency part of Theorem 4.10 now follows from Property 4.2.

Corollary. *Let S be the semigroup of Theorem 4.10 with $\mathfrak{R} = R$, and let g_0 be any element of $\mathfrak{G}(X)$ of minimal order p. Then the unique minimum (nonequality) congruence θ_0 on S is given as follows: for $a, b \in S$, $a \equiv b(\theta_0)$ if and only if $a = b$ or a and b belong to the same $(h-1)$st layer cycle of g_0.*

Proof. This follows from the proof of the claim in Theorem 4.10 and the easily verified fact that θ_0 is a congruence relation.

REFERENCES

1. G. Birkhoff, *Subdirect unions in universal algebras*, Bull. Amer. Math. Soc. 50 (1944), 764–768. MR 6, 33.

2. ———, *Lattice theory*, 2nd rev. ed., Amer. Math Soc. Colloq. Publ., vol. 25, Amer. Math. Soc., Providence, R. I., 1948. MR 10, 673.

3. A. H. Clifford, *Extensions of semigroups*, Trans. Amer. Math. Soc. 68 (1950), 165–173. MR 11, 499.

4. A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*, Vol. I, Math. Surveys, no. 7, Amer. Math. Soc., Providence, R. I., 1961. MR 24 #A2627.

5. P. E. McNeil, *The structure of certain semigroups with two idempotents*, Ph. D. Dissertation, Pennsylvania State University, University Park, Pa., 1968.

6. ———, *Group extensions of null semigroups*, Duke Math. J. 38 (1971), 491–497.

7. B. M. Šaĭn (Schein), *Homomorphisms and subdirect decompositions of semigroups*, Pacific J. Math. 17 (1966), 529–547. MR 33 #5768.

8. J. T. Sedlock, *Certain decompositions of periodic semigroups and congruences on nilpotent semigroups*, Ph. D. Dissertation, Lehigh University, Bethlehem, Pa., 1966.

9. T. Tamura, *The theory of construction of finite semigroups. III. Finite unipotent semigroups*, Osaka Math. J. 10 (1958), 191–204. MR 21 #1351.

10. G. Thierrin, *Sur la structure des demi-groupes*, Publ. Sci. Univ. Alger. Sér. A. 3 (1956), 161–171. MR 20 #7071.

11. H. Wielandt, *Finite permutation groups*, Lectures, University of Tübingen, 1954/55; English transl., Academic Press, New York, 1964. MR 32 #1252.

12. R. Yoshida, *Ideal extensions of semigroups and compound semigroups*, Mem. Res. Inst. Sci. Eng. Ritumeikan Univ. Kyoto 13 (1965), 1–8.

13. D. Zitarelli, *Subdirectly irreducible finite inverse semigroups*, Ph. D. Dissertation, Pennsylvania State University, University Park, Pa., 1970.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CINCINNATI, CINCINNATI, OHIO 45221

THE INSTITUTE FOR SERVICES TO EDUCATION, 2001 S STREET N. W., WASHINGTON, D. C. 20009 (Current address)