

EXTENDING ALGEBRAS TO MODEL CONGRUENCE SCHEMES

J. BERMAN, G. GRÄTZER AND C. R. PLATT

1. Introduction. This paper is concerned with the description of principal congruence relations. Given elements a and b of a universal algebra \mathfrak{A} , let $\theta(a, b)$ denote the smallest congruence relation on \mathfrak{A} containing the pair $\langle a, b \rangle$. One of the earliest characterizations of $\theta(a, b)$ is Mal'cev's well-known result [5, Theorem 1.10.3], which says that $c \equiv d(\theta(a, b))$ if and only if there exists a sequence z_0, z_1, \dots, z_n of elements of \mathfrak{A} and a sequence f_1, f_2, \dots, f_n of unary algebraic functions such that $c = z_0, d = z_n$, and for each $i = 1, \dots, n$,

$$\{f_i(a), f_i(b)\} = \{z_i, z_{i-1}\}.$$

Although this describes $\theta(a, b)$ in terms of a set of unary algebraic functions, it is not possible to predict the number or complexity of the unary functions used independently of the choice of a, b, c and d . Several recent papers ([1], [2], [3], [4], [6]) investigate classes of algebras in which principal congruences are simpler.

By way of illustration, consider an algebra \mathfrak{A} such that $c \equiv d(\theta(a, b))$ in \mathfrak{A} if and only if

$$c = (a + a) + u, \quad (b + b) + u = v + b, \quad v + a = d$$

for some $u, v \in A$. This can be described by two polynomials,

$$\mathbf{p}_1 = (\mathbf{x} + \mathbf{x}) + \mathbf{y}_1 \quad \text{and} \quad \mathbf{p}_2 = \mathbf{y}_2 + \mathbf{x},$$

which produce the pairs of elements

$$\langle (a + a) + u, (b + b) + u \rangle \quad \text{and} \quad \langle v + a, v + b \rangle$$

together with a "switching sequence" to signify that the second pair is to be inverted (and so $c = p_1(a, u), p_1(b, u) = p_2(b, v), p_2(a, v) = d$). The general definition, taken from [2], involves an arbitrary sequence of polynomial symbols and a switching sequence.

Definition 1.1. A congruence scheme Σ consists of a sequence of pairs $\langle \mathbf{p}_1, t_1 \rangle, \dots, \langle \mathbf{p}_n, t_n \rangle$ where, for each i , \mathbf{p}_i is a polynomial symbol and t_i is 0 or 1. Furthermore, any two of the \mathbf{p}_i are assumed to have exactly one variable, \mathbf{x}_0 , in common.

Received January 25, 1980 and in revised form April 22, 1983. The work of the second and third authors was supported by the NSERC of Canada.

If all the polynomials occurring in Σ are defined in some algebra \mathfrak{A} (i.e., the type of \mathfrak{A} contains all the operation symbols occurring in Σ), then we say that \mathfrak{A} admits Σ , with a similar definition for classes of algebras.

Definition 1.2. If an algebra \mathfrak{A} admits Σ then we define a 4-ary relation $\Sigma_{\mathfrak{A}}$ on A as follows: Let x_0, x_1, \dots, x_k be all the variables occurring in all the p_i of Σ . Then we may write $p_i(x_0, x_1, \dots, x_k)$ (even though not all variables occur explicitly). For $a_0, a_1, b_0, b_1 \in A$, we define $\Sigma_{\mathfrak{A}}(a_0, a_1, b_0, b_1)$ to hold if and only if there exist elements $c_1, c_2, \dots, c_k \in A$ such that

- (i) $b_0 = p_1(a_{t_1}, c_1, \dots, c_k)$,
- (ii) $b_1 = p_n(a_{1-t_n}, c_1, \dots, c_k)$,
- (iii) for $i = 1, 2, \dots, n - 1$,

$$p_i(a_{1-t_i}, c_1, \dots, c_k) = p_{i+1}(a_{t_{i+1}}, c_1, \dots, c_k).$$

We will say in this case that $\Sigma_{\mathfrak{A}}(a_0, a_1, b_0, b_1)$ holds via c_1, \dots, c_k .

Clearly $\Sigma_{\mathfrak{A}}(a, b, c, d)$ implies that

$$c \equiv d(\theta(a, b)).$$

Mal'cev's Lemma states that, conversely, if $c \equiv d(\theta(a, b))$ then $\Sigma_{\mathfrak{A}}(a, b, c, d)$ holds for some congruence scheme Σ . If Σ is a congruence scheme and \mathfrak{A} a non-trivial algebra such that for all $a, b, c, d \in A$,

$$\Sigma_{\mathfrak{A}} = \{ \langle a, b, c, d \rangle \mid c \equiv d(\theta(a, b)) \},$$

then we say \mathfrak{A} represents Σ . Let Σ^* denote the class of all algebras which represent Σ .

In [2] the question of which congruence schemes can be represented was addressed. Because of certain technical difficulties, it is necessary to restrict our discussion to schemes Σ containing no constant symbols. Then the following is proved in [2].

REPRESENTATION THEOREM FOR CONGRUENCE SCHEMES. *If Σ contains no constants, then the following three conditions are equivalent:*

- (i) no p_i occurring in Σ is unary;
- (ii) Σ^* is nonempty;
- (iii) $\mathbf{K} \subseteq \Sigma^*$ for some nontrivial equational class \mathbf{K} .

In this paper we present two more results concerning congruence schemes and the algebras which can represent them. The first result considers whether an algebra \mathfrak{A} can be "enlarged" so as to represent a scheme Σ .

EMBEDDING THEOREM. *Let \mathfrak{A} be an algebra of a type τ without constants and having at least one non-unary operation. Then the following are equivalent:*

- (i) Every unary polynomial in \mathfrak{A} is one-to-one.
- (ii) For every representable congruence scheme Σ , of type contained in τ , there is an extension \mathfrak{B} of \mathfrak{A} which represents Σ .
- (iii) For every representable congruence scheme Σ , of type contained in τ , there is an equational class $\mathbf{K} \subseteq \Sigma^*$ such that the type of \mathbf{K} contains τ and \mathfrak{A} is a subalgebra of the τ -reduct of some $\mathfrak{B} \in \mathbf{K}$.

To illustrate the motivation for (i), consider the example of an algebra \mathfrak{A} having a unary polynomial q and a binary polynomial p . Let Σ be the congruence scheme $\langle \mathbf{p}(q(x_0), x_1), 0 \rangle$. If \mathfrak{A} were to represent Σ , then for any $a, b \in A$, since $a \equiv b(\theta(a, b))$, there would exist $u \in A$ with

$$a = p(q(a), u) \quad \text{and} \quad b = p(q(b), u).$$

Therefore, if $q(a) = q(b)$, then $a = b$.

The second result of this paper is the construction of a “testing algebra” for the quasi-ordering \subseteq_a introduced in [2] (see Section 6 for a definition).

EXISTENCE THEOREM FOR TESTING ALGEBRAS. *Let Σ be a congruence scheme containing no constants. Then there exists an algebra $\mathfrak{A}(\Sigma)$ and a, b, c, d elements of $\mathfrak{A}(\Sigma)$ with the following properties:*

- (i) $\mathfrak{A}(\Sigma) \in \Sigma^*$;
- (ii) $c \equiv d(\theta(a, b))$ in $\mathfrak{A}(\Sigma)$;
- (iii) For any congruence scheme Ω of type contained in the type of Σ , the relation $\Sigma^* \subseteq \Omega^*$ holds if and only if $\Omega(a, b, c, d)$ is in $\mathfrak{A}(\Sigma)$.

The reason for the name “testing algebra” should be clear from (iii). By definition, to verify $\Sigma^* \subseteq \Omega^*$ we have to establish that for all algebras \mathfrak{A} in Σ^* and for all $x, y, u, v \in A$ with $u = v(\theta(x, y))$, the relation $\Omega(x, y, u, v)$ holds. This theorem reduces the consideration of all $\mathfrak{A} \in \Sigma^*$ to just one algebra, $\mathfrak{A}(\Sigma)$, and within $\mathfrak{A}(\Sigma)$ the consideration of all quadruples x, y, u, v is reduced to one: a, b, c, d .

The paper is organized as follows. In Section 2 we clarify the notation and prove a number of technical lemmas, mostly about unary polynomials. In Section 3 we introduce the bridge construction which is used as an inductive step in the proof of the embedding theorem in Section 4. In Section 5 we show how to construct testing algebras, and in Section 6 we conclude with some examples and open problems.

2. Roots. In this section and the next, we work in a fixed similarity type τ with no constants. Let $\mathbf{P}(n)$ denote the set of all n -ary polynomial symbols. We let \mathbf{f} and \mathbf{g} denote fundamental operation symbols, while $\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s}, \mathbf{t}$ will denote arbitrary members of $\mathbf{P}(n)$. If \mathfrak{A} is a (partial) algebra, then $\mathbf{p} \in \mathbf{P}(n)$ induces in \mathfrak{A} a polynomial, $\mathbf{p}^{\mathfrak{A}}$, which is a (partial) function from A^n to A . We will usually write p instead of $\mathbf{p}^{\mathfrak{A}}$, and thus $p(x_1, \dots, x_n)$

instead of $\mathfrak{P}^{\mathfrak{A}}(x_1, \dots, x_n)$. Of particular interest will be the algebra of polynomial symbols $\mathfrak{P}(n)$, defined on the set $\mathbf{P}(n)$, where, if \mathbf{f} is a k -ary operation symbol and $\mathbf{q}_1, \mathbf{q}_2, \dots, \mathbf{q}_k \in \mathbf{P}(n)$, then

$$f(\mathbf{q}_1, \dots, \mathbf{q}_k) = \mathbf{f}(\mathbf{q}_1, \dots, \mathbf{q}_k) \text{ in } \mathfrak{P}(n).$$

Consequently, if \mathbf{p} is an n -ary polynomial symbol, then the polynomial p in $\mathfrak{P}(n)$ is described inductively by

$$p(\mathbf{q}_1, \dots, \mathbf{q}_n) = \mathbf{q}_i$$

if $\mathbf{p} = \mathbf{x}_i$ and

$$p(\mathbf{q}_1, \dots, \mathbf{q}_n) = \mathbf{f}(p_1(\mathbf{q}_1, \dots, \mathbf{q}_n), \dots, p_k(\mathbf{q}_1, \dots, \mathbf{q}_n))$$

if $\mathbf{p} = \mathbf{f}(\mathbf{p}_1, \dots, \mathbf{p}_k)$.

With $\mathbf{p} \in \mathbf{P}(n)$ we associate a partial algebra $\mathfrak{C}(\mathbf{p})$ (the component partial algebra of \mathbf{p}) as follows: If $\mathbf{p} = \mathbf{x}_i$, then

$$C(\mathbf{p}) = \{\mathbf{p}\}$$

and if $\mathbf{p} = \mathbf{f}(\mathbf{p}_1, \dots, \mathbf{p}_k)$, then

$$C(\mathbf{p}) = \{\mathbf{p}\} \cup C(\mathbf{p}_1) \cup \dots \cup C(\mathbf{p}_k).$$

Thus $C(\mathbf{p}) \subseteq \mathbf{P}(n)$ and $\mathfrak{C}(\mathbf{p})$ has the natural partial algebra structure as a relative subalgebra of $\mathfrak{P}(n)$. Members of $C(\mathbf{p})$ are called *components* of \mathbf{p} .

LEMMA 2.1. *If $\mathbf{p}, \mathbf{t}_1, \dots, \mathbf{t}_n \in \mathbf{P}(m)$, $\mathbf{q} \in \mathbf{P}(n)$, $\mathbf{p} = \mathbf{q}(\mathbf{t}_1, \dots, \mathbf{t}_n)$, and $\mathbf{s} \in C(\mathbf{p})$, then there exists a j , such that either $\mathbf{s} \in C(\mathbf{t}_j)$ or $\mathbf{t}_j \in C(\mathbf{s})$ holds. Moreover, \mathbf{p} cannot be a proper component of itself, that is, if $\mathbf{p} = \mathbf{f}(\mathbf{p}_1, \dots, \mathbf{p}_k)$, then $\mathbf{p} \notin C(\mathbf{p}_i)$ for any $i = 1, 2, \dots, k$.*

Proof. We use induction on the rank of \mathbf{p} . If $\mathbf{p} = \mathbf{x}_i$, then $\mathbf{q} = \mathbf{x}_j$, say, with $\mathbf{t}_j = \mathbf{x}_i$. The only choice for \mathbf{s} is \mathbf{x}_i and the conclusion follows. If

$$\mathbf{p} = \mathbf{f}(\mathbf{p}_1, \dots, \mathbf{p}_k) = \mathbf{q}(\mathbf{t}_1, \dots, \mathbf{t}_n),$$

then $\mathbf{q} = \mathbf{f}(\mathbf{q}_1, \dots, \mathbf{q}_k)$ for some $\mathbf{q}_1, \dots, \mathbf{q}_k \in \mathbf{P}(n)$. If $\mathbf{s} = \mathbf{p}$, then $\mathbf{t}_j \in C(\mathbf{p})$ for all j . If $\mathbf{s} \neq \mathbf{p}$, then

$$\mathbf{s} \in C(\mathbf{q}_i(\mathbf{t}_1, \dots, \mathbf{t}_n)) \text{ for some } i.$$

Thus, the induction hypothesis yields $\mathbf{s} \in C(\mathbf{t}_j)$ or $\mathbf{t}_j \in C(\mathbf{s})$ for some j . An equally straightforward argument proves the final statement of the lemma.

Definition 2.2. For a partial algebra \mathfrak{A} , $\mathbf{r} \in \mathbf{P}(1)$, and $u, v \in A$, if $r(u) = v$, then u is an \mathbf{r} -th root of v in \mathfrak{A} .

Definition 2.3. A partial algebra \mathfrak{A} is said to satisfy the *Unique Root Condition (URC)* if and only if for every $\mathbf{r} \in \mathbf{P}(1)$, each $v \in A$ has at most

one r -th root in \mathfrak{A} , that is, all unary polynomials on \mathfrak{A} are one-to-one.

Definition 2.4. A subset X of a partial algebra \mathfrak{A} is called *prime* if and only if $u_1, \dots, u_k \in A$ and $f(u_1, \dots, u_k) \in X$ imply that $u_1, \dots, u_k \in X$ for any partial operation f of \mathfrak{A} .

The next result easily follows by induction.

LEMMA 2.5. If X is prime in \mathfrak{A} , $\mathbf{q} \in \mathbf{P}(n)$, $u_1, \dots, u_n \in A$, $q(u_1, \dots, u_n) \in X$, and if x_j is a variable explicitly occurring in \mathbf{q} , (that is, $x_j \in C(\mathbf{q})$), then $u_j \in X$.

It will be necessary at certain stages to deal with an algebra rather than with a partial algebra. For a partial algebra \mathfrak{B} , let $\mathfrak{F}(\mathfrak{B})$ denote the algebra completely freely generated by \mathfrak{B} . It is known ([5], Theorem 14.4 and Corollary 2 to Theorem 28.1) that $\mathfrak{F}(\mathfrak{B})$ is characterized up to isomorphism by the following properties:

- (F1) B generates $\mathfrak{F}(\mathfrak{B})$;
- (F2) \mathfrak{B} is a relative subalgebra of $\mathfrak{F}(\mathfrak{B})$;
- (F3) B is prime in $\mathfrak{F}(\mathfrak{B})$;
- (F4) if $u_1, \dots, u_k, v_1, \dots, v_m \in F(\mathfrak{B})$ and \mathbf{f}, \mathbf{g} are operation symbols with

$$f(u_1, \dots, u_k) = g(v_1, \dots, v_m) \notin B,$$

then $\mathbf{f} = \mathbf{g}$, $k = m$ and $u_i = v_i$ for $i = 1, 2, \dots, k$.

LEMMA 2.6. If a partial algebra \mathfrak{B} satisfies (URC), then so does $\mathfrak{F}(\mathfrak{B})$.

Proof. Let $\mathbf{r} \in \mathbf{P}(1)$ and let $a, b \in F(\mathfrak{B})$ with $r(a) = r(b)$. We prove $a = b$ by induction on the rank of \mathbf{r} . If \mathbf{r} is a variable, then the conclusion is evident. Suppose that

$$\mathbf{r} = \mathbf{f}(\mathbf{r}_1, \dots, \mathbf{r}_k), \quad \text{with } \mathbf{r}_i \in \mathbf{P}(1).$$

If $r(a) \in B$, then (F3) and Lemma 2.5 give $a, b \in B$. Hence (F2) and (URC) for \mathfrak{B} imply $a = b$. If $r(a) \notin B$, then (F4) implies that $r_i(a) = r_i(b)$ for $i = 1, 2, \dots, k$, so $a = b$ by the induction hypothesis.

Definition 2.7. Let $\mathbf{r} \in \mathbf{P}(1)$; we call \mathbf{r} *irreducible* if and only if $\mathbf{p}, \mathbf{q} \in \mathbf{P}(1)$ and $\mathbf{r} = p(\mathbf{q})$ imply that $\mathbf{r} = \mathbf{q}$ or $\mathbf{r} = \mathbf{p}$.

Clearly, every unary polynomial can be built up from the irreducible ones. For example, if

$$\mathbf{r} = ((\mathbf{x}_1 + \mathbf{x}_1) + (\mathbf{x}_1 + \mathbf{x}_1)) + (\mathbf{x}_1 + \mathbf{x}_1),$$

then $\mathbf{r} = p(\mathbf{q})$ where

$$\mathbf{q} = \mathbf{x}_1 + \mathbf{x}_1 \quad \text{and} \quad \mathbf{p} = (\mathbf{x}_1 + \mathbf{x}_1) + \mathbf{x}_1.$$

In this case, \mathbf{r} is not irreducible, but \mathbf{p} and \mathbf{q} are.

Let $\mathbf{r} = p(\mathbf{q})$ and $b \in A$; let b be a \mathbf{p} -th root of c in \mathfrak{A} and let a be a \mathbf{q} -th root of b in \mathfrak{A} . Clearly, a is an \mathbf{r} -th root of c in \mathfrak{A} . This observation motivates the hypothesis of irreducibility in the next lemma and justifies its corollary.

LEMMA 2.8. *Let \mathfrak{A} be a partial algebra satisfying (URC), let $\mathbf{r} \in \mathbf{P}(1)$ be irreducible, and let $a \in A$. Then there is a partial algebra \mathfrak{A}' extending \mathfrak{A} and satisfying (URC) such that a has an \mathbf{r} -th root in \mathfrak{A}' .*

Proof. Assume that a has no \mathbf{r} -th root in \mathfrak{A} . Thus \mathbf{r} is not a variable, so

$$\mathbf{r} = \mathbf{f}(\mathbf{r}_1, \dots, \mathbf{r}_k), \quad \text{where } \mathbf{r}_i \in \mathbf{P}(1).$$

Let \mathfrak{B} be the partial algebra that is the disjoint union of \mathfrak{A} and $C(\mathbf{r}) - \{\mathbf{r}\}$. Then $\mathbf{f}^{\mathfrak{B}}(\mathbf{r}_1, \dots, \mathbf{r}_k)$ is undefined. Let \mathfrak{A}' be the partial algebra obtained from \mathfrak{B} by adding the definition

$$\mathbf{f}^{\mathfrak{A}'}(\mathbf{r}_1, \dots, \mathbf{r}_k) = a.$$

Clearly, $\mathbf{x}_1 \in C(\mathbf{r})$ is an \mathbf{r} -th root of a in \mathfrak{A}' ; so it remains to show that \mathfrak{A}' satisfies (URC). Obviously, \mathfrak{B} satisfies (URC), so if $u, v \in B$, $\mathbf{t} \in \mathbf{P}(1)$, $\mathbf{t}^{\mathfrak{A}'}(u) = \mathbf{t}^{\mathfrak{A}'}(v)$, and $\mathbf{t}^{\mathfrak{B}}(u)$ and $\mathbf{t}^{\mathfrak{B}}(v)$ are defined, then $u = v$. Thus the verification of (URC) for \mathfrak{A}' involves examination of when $\mathbf{t}^{\mathfrak{A}'}(u)$ is undefined. The following claim narrows this examination.

Claim. If $u \in B$, $\mathbf{t} \in \mathbf{P}(1)$, $\mathbf{t}^{\mathfrak{A}'}(u)$ is defined, and $\mathbf{t}^{\mathfrak{B}}(u)$ is undefined, then $u = \mathbf{x}_1$, $\mathbf{t}^{\mathfrak{A}'}(u) \in A$, and $\mathbf{t} = q(\mathbf{r})$ for some $\mathbf{q} \in \mathbf{P}(1)$.

To see this, first note that \mathbf{t} cannot be a variable, so let

$$\mathbf{t} = \mathbf{g}(\mathbf{t}_1, \dots, \mathbf{t}_m) \quad \text{with } \mathbf{t}_1, \dots, \mathbf{t}_m \in \mathbf{P}(1).$$

There are two possibilities:

Case 1. $\mathbf{t}_j^{\mathfrak{B}}(u)$ is defined for all $j = 1, 2, \dots, m$. Since $\mathbf{t}^{\mathfrak{B}}(u)$ is undefined, we must have $a = \mathbf{t}^{\mathfrak{A}'}(u) \in A$. So $\mathbf{g} = \mathbf{f}$ and $\mathbf{t}_j^{\mathfrak{B}}(u) = \mathbf{r}_j$. Since \mathbf{r} is irreducible, it follows that $u = \mathbf{x}_1$, so $\mathbf{t}_j = \mathbf{r}_j$, hence $\mathbf{t} = \mathbf{r}$.

Case 2. $\mathbf{t}_j^{\mathfrak{B}}(u)$ is undefined for some j . Then, since $\mathbf{t}_j^{\mathfrak{A}'}(u)$ is defined, Case 1 and an induction on the rank of \mathbf{t}_j give $u = \mathbf{x}_1$, $\mathbf{t}_j^{\mathfrak{A}'}(u) \in A$, and $\mathbf{t}_j = \mathbf{q}_j(\mathbf{r})$ for some $\mathbf{q}_j \in \mathbf{P}(1)$. Now observe that in \mathfrak{B} no operation is defined whose arguments include elements of both A and $B - A$, hence

$$\mathbf{t}_i^{\mathfrak{A}'}(u) \in A \quad \text{for all } i = 1, 2, \dots, m,$$

and none of the $\mathbf{t}_i^{\mathfrak{B}}(u)$ is defined. Thus, the induction hypothesis can be applied again to give $\mathbf{t}_i = \mathbf{q}_i(\mathbf{r})$ with $\mathbf{q}_i \in \mathbf{P}(1)$ for all i . So $\mathbf{t} = q(\mathbf{r})$ where

$$\mathbf{q} = \mathbf{g}(\mathbf{q}_1, \dots, \mathbf{q}_m).$$

Clearly, $\mathbf{t}^{\mathfrak{A}'}(u) \in A$ and the proof of the claim is complete.

Thus, if $t^{\mathfrak{A}'}(u) = t^{\mathfrak{A}'}(v)$ and neither $t^{\mathfrak{B}}(u)$ nor $t^{\mathfrak{B}}(v)$ is defined, then $u = v = x_1$. Finally, suppose that $t^{\mathfrak{B}}(u)$ is undefined and that $t^{\mathfrak{B}}(v)$ is defined. Then, by the Claim, $u = x_1$, $t = q(r)$, and $t^{\mathfrak{A}'}(u) \in A$. Since $t^{\mathfrak{B}}(v)$ is defined, $v \in A$. Thus

$$\begin{aligned} q^{\mathfrak{A}'}(r^{\mathfrak{A}'}(v)) &= t^{\mathfrak{B}}(v) = t^{\mathfrak{A}'}(v) = t^{\mathfrak{A}'}(u) \\ &= q^{\mathfrak{A}'}(r^{\mathfrak{A}'}(x_1)) = q^{\mathfrak{A}'}(a) = q^{\mathfrak{A}'}(a). \end{aligned}$$

But \mathfrak{A} has (URC), so $a = r^{\mathfrak{A}'}(v)$. This contradicts the assumption that a has no r -th root in \mathfrak{A} , completing the proof of the lemma.

By applying Lemmas 2.6 and 2.8 alternately, repeating this transfinitely, and using direct limit constructions when necessary, one obtains an algebra that proves the next result.

COROLLARY 2.9. *If \mathfrak{A} is a partial algebra satisfying (URC), then \mathfrak{A} can be embedded into an algebra \mathfrak{A}' satisfying (URC) such that for every $r \in \mathbf{P}(1)$, each $a \in A'$ has an r -th root in \mathfrak{A}' .*

For the remainder of this section, \mathfrak{A} is a fixed algebra and B is any set containing A . The partial algebra \mathfrak{B} on the set B will have only operations defined as on \mathfrak{A} , (that is, $f^{\mathfrak{B}} = f^{\mathfrak{A}}$ for any operation symbol f). We shall prove some technical results for $\mathfrak{F} = \mathfrak{F}(\mathfrak{B})$.

Note that properties (F2), (F3), and (F4) hold for \mathfrak{A} relative to $\mathfrak{F}(\mathfrak{B})$:

(F2') \mathfrak{A} is a relative subalgebra to $\mathfrak{F}(\mathfrak{B})$;

(F3') A is prime in $\mathfrak{F}(\mathfrak{B})$;

(F4') If $u_1, \dots, u_k, v_1, \dots, v_m \in F(\mathfrak{B})$, f and g are operation symbols, and

$$f(u_1, \dots, u_k) = g(v_1, \dots, v_m) \notin A,$$

then $f = g$, $k = m$, and $u_i = v_i$ for $i = 1, 2, \dots, k$.

Definition 2.10. For any $u \in F = F(\mathfrak{B})$, we define $\rho(u)$, the rank of u , and the set $C_F(u)$, the F -components of u , inductively as follows:

- (i) if $u \in B$, then $\rho(u) = 0$ and $C_F(u) = \{u\}$;
- (ii) if $u = f(u_1, \dots, u_k) \notin B$, then

$$\rho(u) = 1 + \sum (\rho(u_i) \mid i = 1, 2, \dots, k)$$

and

$$C_F(u) = \{u\} \cup \cup (C_F(u_i) \mid i = 1, 2, \dots, k).$$

In view of (F4'), it is clear that ρ and C_F are well defined. Observe that $u \in C_F(v)$ implies that $\rho(u) \leq \rho(v)$. Therefore we have immediately:

Remark 2.11. If $u \in F - A$, then u is not a proper F -component of itself, that is, if $u = f(v_1, \dots, v_k) \notin A$, then $u \notin C_F(v_i)$.

LEMMA 2.12. *If $\mathbf{p} \in \mathbf{P}(n)$, $u_1, \dots, u_n \in B$, $u = p(u_1, \dots, u_n)$ in $\mathfrak{F}(B)$, and $v \in C_F(u)$, then there exists a $\mathbf{q} \in C(\mathbf{p})$ such that*

$$v = q(u_1, \dots, u_n).$$

Proof. If $v = u$, then let $\mathbf{q} = \mathbf{p}$. If $v \neq u$, then $u \notin B$, so there exist an operation symbol \mathbf{f} and $\mathbf{p}_1, \dots, \mathbf{p}_k \in \mathbf{P}(n)$ for which

$$\mathbf{p} = \mathbf{f}(\mathbf{p}_1, \dots, \mathbf{p}_k).$$

So

$$v \in C_F(p_i(u_1, \dots, u_n)) \text{ for some } i.$$

By induction it follows that

$$v = q(u_1, \dots, u_n) \text{ for some } \mathbf{q} \in C(\mathbf{p}_i) \subseteq C(\mathbf{p}),$$

completing the proof.

It is clear that property (F4) is false if \mathbf{f} or \mathbf{g} are replaced by arbitrary polynomial symbols, but we do have the following very special case which will be needed in Section 3.

LEMMA 2.13. *Let $a_0, a_1 \in A$, $z_1, \dots, z_m \in B - A$, $\mathbf{p}, \mathbf{q} \in \mathbf{P}(m + 1)$ and $\mathbf{p} \in C(\mathbf{q})$. If*

$$p(a_0, z_1, \dots, z_m) = q(a_1, z_1, \dots, z_m) \notin A,$$

then $\mathbf{p} = \mathbf{q}$.

Proof. If \mathbf{p} is a variable, then we may assume

$$p(a_0, z_1, \dots, z_m) = z_j \notin A \text{ for some } j.$$

But then \mathbf{q} is also a variable so $\mathbf{p} = \mathbf{q}$.

Thus we may assume that $\mathbf{p} = \mathbf{f}(\mathbf{p}_1, \dots, \mathbf{p}_k)$ and therefore, by (F4'),

$$\mathbf{q} = \mathbf{f}(\mathbf{q}_1, \dots, \mathbf{q}_k) \text{ for some } \mathbf{p}_i, \mathbf{q}_i \in \mathbf{P}(m + 1), \text{ and}$$

$$p_i(a_0, z_1, \dots, z_m) = q_i(a_1, z_1, \dots, z_m) \text{ for } i = 1, 2, \dots, k.$$

Suppose that $\mathbf{p} \neq \mathbf{q}$. The hypothesis $\mathbf{p} \in C(\mathbf{q})$ then gives $\mathbf{p} \in C(\mathbf{q}_j)$ for some j . So $\mathbf{p}_j \in C(\mathbf{q}_j)$. If $q_j(a_1, z_1, \dots, z_m) \in A$, then by Lemma 2.5 and (F3'), \mathbf{q}_j and therefore \mathbf{p} cannot explicitly contain any of the variables x_1, \dots, x_m . But this would imply that

$$p(a_0, z_1, \dots, z_m) \in A,$$

contrary to hypothesis. Thus,

$$p_j(a_0, z_1, \dots, z_m) = q_j(a_1, z_1, \dots, z_m) \notin A,$$

so by the induction hypothesis $\mathbf{p}_j = \mathbf{q}_j$. But then

$$\mathbf{p} \in C(\mathbf{q}_j) = C(\mathbf{p}_j),$$

violating Lemma 2.1. This contradiction proves $\mathbf{p} = \mathbf{q}$.

We shall need one more fact about $\mathfrak{F}(\mathfrak{B})$.

LEMMA 2.14. *Let $\mathbf{p} \in \mathbf{P}(m)$, $v_1, \dots, v_m \in B$, $v = p(v_1, \dots, v_m) \notin A$, $u \in F$, $\mathbf{r} \in \mathbf{P}(1)$, and $r(u) = v$. Then there exist $n > 0$ and polynomial symbols $\mathbf{q} \in \mathbf{P}(n)$ and $\mathbf{t}_1, \dots, \mathbf{t}_n \in \mathbf{P}(m)$ such that*

- (i) $\mathbf{p} = q(\mathbf{t}_1, \dots, \mathbf{t}_n)$;
- (ii) $t_j(v_1, \dots, v_m) = u$ for all $j = 1, 2, \dots, n$;
- (iii) $\mathbf{r} = q(\mathbf{x}_1, \mathbf{x}_1, \dots, \mathbf{x}_1)$.

Proof. If \mathbf{r} is a variable, then let $n = 1$, $\mathbf{q} = \mathbf{x}_1$, and $\mathbf{t}_1 = \mathbf{p}$. Suppose

$$\mathbf{r} = \mathbf{f}(\mathbf{r}_1, \dots, \mathbf{r}_k), \mathbf{r}_i \in \mathbf{P}(1), i = 1, 2, \dots, k.$$

Since $v \notin A$, by (F4'),

$$\mathbf{p} = \mathbf{f}(\mathbf{p}_1, \dots, \mathbf{p}_k) \text{ for some } \mathbf{p}_i \in \mathbf{P}(m)$$

with

$$p_i(v_1, \dots, v_m) = r_i(u).$$

Since \mathfrak{A} is a subalgebra of \mathfrak{F} , $v \notin A$ implies $u \notin A$, so $r_i(u) \notin A$ by (F3') and Lemma 2.5. Thus, by induction, there exist $n_i > 0$, $\mathbf{q}_i \in \mathbf{P}(n_i)$, and $\mathbf{t}_j^i \in \mathbf{P}(m)$ such that

$$\begin{aligned} \mathbf{p}_i &= q_i(\mathbf{t}_1^i, \dots, \mathbf{t}_{n_i}^i), \quad t_j^i(v_1, \dots, v_m) = u, \text{ and} \\ \mathbf{r}_i &= q_i(\mathbf{x}_1, \mathbf{x}_1, \dots, \mathbf{x}_1) \end{aligned}$$

for all $i = 1, 2, \dots, k$ and $j = 1, 2, \dots, n_i$. Let \mathbf{x}_j^i , $i = 1, 2, \dots, k$, $j = 1, 2, \dots, n_i$ be distinct variable symbols. Let us put $n = n_1 + n_2 + \dots + n_k$ and let $\mathbf{t}_1, \mathbf{t}_2, \dots, \mathbf{t}_n$ denote the sequence $\mathbf{t}_1^1, \mathbf{t}_2^1, \dots, \mathbf{t}_1^2, \dots, \mathbf{t}_{n_k}^k$; define \mathbf{q} by

$$\mathbf{q} = \mathbf{f}(q_1(\mathbf{x}_1^1, \dots, \mathbf{x}_{n_1}^1), \dots, q_k(\mathbf{x}_1^k, \dots, \mathbf{x}_{n_k}^k)).$$

Then properties (i), (ii), (iii) of the lemma are evident.

3. Bridges. Let $\mathbf{p} \in \mathbf{P}(m + 1)$ be a polynomial symbol in which the variables $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_m$ explicitly occur. A partial algebra \mathfrak{A} with elements a_0, a_1, b_0, b_1 is said to contain a \mathbf{p} -bridge from $\langle a_0, a_1 \rangle$ to $\langle b_0, b_1 \rangle$ if and only if there exist elements c_1, \dots, c_m of A such that

$$p(a_i, c_1, \dots, c_m) = b_i \text{ for } i = 0, 1.$$

Let \mathfrak{A} be an algebra and let Σ be the congruence scheme $\langle \mathbf{p}_1, t_1 \rangle, \dots, \langle \mathbf{p}_n, t_n \rangle$. Then $\mathfrak{A} \in \Sigma^*$ is equivalent to the following condition: $c \equiv d(\theta(a, b))$ if and only if there exists a sequence

$$c = z_0, z_1, \dots, z_n = d$$

of elements of \mathfrak{A} such that there is a p_i -bridge from $\langle a, b \rangle$ to $\langle z_{i-1}, z_i \rangle$ (if $t_i = 0$) or $\langle z_i, z_{i-1} \rangle$ (if $t_i = 1$) for $i = 1, \dots, n$.

Thus to construct our extension \mathfrak{B} of an algebra \mathfrak{A} satisfying $\mathfrak{B} \in \Sigma^*$ it is sufficient to construct an extension in which some specified bridges exist. Hence the general problem of representing Σ is reduced to constructing bridges.

The purpose of this section is to prove the next theorem which shows that an extension can be built for a single bridge.

THEOREM 3.1. *Let \mathfrak{A} be a partial algebra satisfying the (URC). Let $\mathbf{p} \in \mathbf{P}(m + 1)$ explicitly contain the variables $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_m$, where $m > 0$. Let $a_0, a_1, b_0, b_1 \in A$ such that if $a_0 = a_1$, then $b_0 = b_1$. Then there exists an extension \mathfrak{A}' of \mathfrak{A} satisfying the (URC) and containing a \mathbf{p} -bridge from $\langle a_0, a_1 \rangle$ to $\langle b_0, b_1 \rangle$.*

By Corollary 2.9, we may assume that \mathfrak{A} is a (full) algebra satisfying the (URC) and, for any $a \in A$ and $\mathbf{r} \in \mathbf{P}(1)$, a has an \mathbf{r} -th root in \mathfrak{A} . These assumptions concerning \mathfrak{A} and the hypotheses of Theorem 3.1 will be in effect for the remainder of this section.

Let $\{z_1, \dots, z_m\}$ be an m -element set disjoint from A and let

$$B = A \cup \{z_1, \dots, z_m\}.$$

Let $\mathfrak{F} = \mathfrak{F}(\mathfrak{B})$ as in Section 2.

LEMMA 3.2. *Let $\mathbf{q} = \mathbf{q}(\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbf{P}(m + 1)$. If \mathbf{x}_0 occurs in \mathbf{q} and if*

$$\mathbf{q}^{\mathfrak{F}}(a_0, z_1, \dots, z_m) = \mathbf{q}^{\mathfrak{F}}(a_1, z_1, \dots, z_m),$$

then $a_0 = a_1$.

Proof. If $\mathbf{q} \in \mathbf{P}(1)$, then $a_0 = a_1$ since \mathfrak{A} satisfies the (URC). Thus we may assume that $\mathbf{q} = \mathbf{f}(\mathbf{q}_1, \dots, \mathbf{q}_k)$ for some operation symbol \mathbf{f} and some $\mathbf{q}_i \in \mathbf{P}(m + 1)$, $i = 1, 2, \dots, k$, $m > 0$. Moreover, for some $j > 0$, \mathbf{x}_j occurs in \mathbf{q} . Then by (F3') and Lemma 2.5,

$$q(a_0, z_1, \dots, z_m) \notin A.$$

Then by (F4'),

$$q_i(a_0, z_1, \dots, z_m) = q_i(a_1, z_1, \dots, z_m) \quad \text{for each } i.$$

Since \mathbf{x}_0 occurs in \mathbf{q} , it also occurs in some \mathbf{q}_j , so by induction hypothesis $a_0 = a_1$.

LEMMA 3.3. *Let $\mathbf{r} \in \mathbf{P}(1)$, $u \in F$, and $r(u) = p(a_0, z_1, \dots, z_m)$. If*

$$u \in C_F(p(a_1, z_1, \dots, z_m)),$$

then $a_0 = a_1$.

Proof. Let $Z = [z_1, \dots, z_m]$ be the subalgebra generated by $\{z_1, \dots, z_m\}$ in \mathfrak{F} . We claim that Z is prime in \mathfrak{F} . Indeed, let

$$u_1, \dots, u_k \in F \text{ and } f(u_1, \dots, u_k) \in Z.$$

There must exist $\mathbf{q} \in \mathbf{P}(m)$ such that

$$q(z_1, \dots, z_m) = f(u_1, \dots, u_k).$$

If \mathbf{q} were a variable then say

$$f(u_1, \dots, u_k) = z_j.$$

By (F3), $u_1, \dots, u_k \in B$, but then

$$\mathbf{f}^{\mathfrak{B}}(u_1, \dots, u_k) = z_j$$

contradicting our definition of \mathfrak{B} . Thus

$$\mathbf{q} = \mathbf{f}(\mathbf{q}_1, \dots, \mathbf{q}_k)$$

for some $\mathbf{q}_i \in \mathbf{P}(m)$ such that

$$q_i(z_1, \dots, z_m) = u_i.$$

Hence $u_i \in Z$. This proves our claim.

Next, observe that $u \in A$ implies that

$$p(a_0, z_1, \dots, z_m) \in A,$$

which by Lemma 2.5 and (F3') implies that $\mathbf{p} \in \mathbf{P}(1)$, contrary to the assumption that x_0, x_1, \dots, x_m explicitly occur in \mathbf{p} , $m > 0$. Thus $u \notin A$.

By Lemma 2.12, $u \in C_F(p(a_1, z_1, \dots, z_m))$ implies that

$$u = q(a_1, z_1, \dots, z_m) \text{ for some } \mathbf{q} \in C(\mathbf{p}).$$

Then x_0 must occur in \mathbf{q} , for otherwise u and therefore $p(a_0, z_1, \dots, z_m)$ would be in Z , which by Lemma 2.5 and the fact that Z is prime in \mathfrak{F} , would contradict our assumption that x_0 appears in \mathbf{p} . Thus by Lemma 2.14 there exist $n > 0$, $\mathbf{q}' \in \mathbf{P}(n)$ and $\mathbf{t}_1, \dots, \mathbf{t}_n \in \mathbf{P}(m + 1)$ such that

$$\mathbf{p} = \mathbf{q}'(\mathbf{t}_1, \dots, \mathbf{t}_n) \text{ and}$$

$$t_j(a_0, z_1, \dots, z_m) = u \text{ for } j = 1, 2, \dots, n.$$

By Lemma 2.1, for some j , either $\mathbf{t}_j \in C(\mathbf{q})$ or $\mathbf{q} \in C(\mathbf{t}_j)$. In any case, Lemma 2.13 then implies that $\mathbf{t}_j = \mathbf{q}$. Since x_0 occurs in \mathbf{q} , Lemma 3.2 implies that $a_0 = a_1$. This completes the proof.

For $i = 0, 1$, let w_i denote $p(a_i, z_1, \dots, z_m)$. In view of Lemma 2.14, each w_i has only finitely many roots in \mathfrak{F} , so we may choose *minimal roots*, that is, choose $u_i \in F$, $\mathbf{r}_i \in \mathbf{P}(1)$ such that $r_i(u_i) = w_i$, and if $\mathbf{q} \in \mathbf{P}(1)$, $v \in F$, and $q(v) = u_i$, then $v = u_i$. If it happens that $w_0 = w_1$, then we

choose $r_0 = r_1$ and $u_0 = u_1$. It can be shown that, in fact, w_i has a unique minimal root, so the choice is unnecessary. However, this stronger result will not be needed.

Let

$$B^* = A \cup C_F(u_0) \cup C_F(u_1)$$

and let \mathfrak{B}^* be the corresponding relative subalgebra of \mathfrak{F} . By hypothesis, every $a \in A$ has an r -th root for any $r \in \mathbf{P}(1)$. Let c_i be the r_i -th root of b_i in \mathfrak{A} , $i = 0, 1$. If $u_0 = u_1$, then $a_0 = a_1$ by Lemma 3.2, so $w_0 = w_1$ and $r_0 = r_1$. Also, if $a_0 = a_1$, then $b_0 = b_1$, and hence $c_0 = c_1$.

Define the equivalence relation Θ on B^* whose nontrivial equivalence classes are $\{c_0, u_0\}$ and $\{c_1, u_1\}$ provided that $c_0 \neq c_1$, and $\{c_0, u_0, u_1\}$ otherwise. It follows from the next lemma that Θ is a congruence relation of \mathfrak{B}^* .

LEMMA 3.4. *No operation on \mathfrak{B}^* is defined on u_0 or u_1 , that is, if $f(v_1, \dots, v_k)$ is defined in \mathfrak{B}^* , then $v_j \neq u_i$, for $j = 1, 2, \dots, k, i = 0, 1$.*

Proof. Suppose, for example, that

$$v_j = u_0 \quad \text{and} \quad f(v_1, \dots, v_k) = v \in B^*.$$

Since $u_i \notin A$, (F3') implies $v \notin A$, so

$$v \in C_F(u_0) \quad \text{or} \quad v \in C_F(u_1).$$

If $v \in C_F(u_1)$, then $u_0 \in C_F(w_1)$, so Lemma 3.3 implies that $a_0 = a_1$. Thus $v \in C_F(u_0)$ in any case. But this contradicts Remark 2.11. The case $v_j = u_1$ is similar.

COROLLARY 3.5. *The equivalence relation Θ is a congruence relation on \mathfrak{B}^* .*

Thus, we can form the partial algebra \mathfrak{B}^*/Θ . It is immediately clear that \mathfrak{A} is a subalgebra of \mathfrak{B}^*/Θ and that

$$p(a_i, z_1, \dots, z_m) = r_i^{\mathfrak{A}}(c_i) = b_i$$

in \mathfrak{B}^*/Θ for $i = 0, 1$. We next show that \mathfrak{B}^*/Θ satisfies the (URC).

Note that for an arbitrary congruence relation Ψ on some partial algebra \mathfrak{D} , if $U \in \mathfrak{D}/\Psi$, and if $r \in \mathbf{P}(1)$, then $r(U)$ may be defined while $r^{\mathfrak{D}}(u)$ is not defined in \mathfrak{D} for any $u \in U$. Fortunately, this is not the case for \mathfrak{B}^* and Θ

LEMMA 3.6. *If $r \in \mathbf{P}(1)$, $U \in \mathfrak{B}^*/\Theta$ and if $r(U)$ is defined in \mathfrak{B}^*/Θ , then there exists a $u \in U$ such that $r(u)$ is defined in \mathfrak{B}^* .*

Proof. If there exists a $u \in U \cap A$, then $r(u)$ is defined since \mathfrak{A} is a subalgebra of \mathfrak{B}^* . Suppose then that $U \cap A = \emptyset$, and hence $U = \{u\}$ for some $u \in B^* - A$. We argue inductively. If $r = x_1$, then the lemma is trivial, so let

$$\mathbf{r} = \mathbf{f}(r_1, \dots, r_k), \quad r_i \in \mathbf{P}(1).$$

Then $r_i(U)$ exists in \mathfrak{B}^*/Θ for each $i = 1, 2, \dots, k$, and there are elements $d_i \in r_i(U)$ such that $f(d_1, \dots, d_k)$ is defined in \mathfrak{B}^* . By induction, $r_i(u)$ is defined in \mathfrak{B}^* . But Θ is a congruence relation so

$$r_i(U) = [r_i(u)]\Theta,$$

so

$$d_i \equiv r_i(u)(\Theta), \quad \text{for } i = 1, 2, \dots, k.$$

Now if $r_i(u) = d_i$ for all i , then

$$r(u) = f(d_1, \dots, d_k)$$

and we are finished. If $r_j(u) \neq d_j$ for some j , then

$$[r_j(u)]\Theta = \{u_i, c_i\}$$

for some $j = 1, 2, \dots, k$ and some $i = 0, 1$. Since $u \notin A$, $r_j(u) \notin A$, so $r_j(u) = u_i$. By the minimality of u_i , this gives $u = u_i$, contrary to the hypothesis $U = \{u\}$.

COROLLARY 3.7. \mathfrak{B}^*/Θ satisfies (URC).

Proof. Let $U, V \in \mathfrak{B}^*/\Theta$ with $r(U) = r(V)$ for some $\mathbf{r} \in \mathbf{P}(1)$. Thus by Lemma 3.6, there exist $u \in U$ and $v \in V$ such that

$$r(u) \equiv r(v)(\Theta) \quad \text{in } \mathfrak{B}^*.$$

If $r(u) = r(v)$, then $u = v$ since \mathfrak{B}^* satisfies (URC) and so $U = V$. If $r(u) \neq r(v)$, then

$$\{r(u), r(v)\} = \{u_i, c_i\} \quad \text{for some } i = 0, 1.$$

Then, for instance, $r(u) = u_i$, which implies that $u = u_i$ by the minimality of u_i . Thus $\mathbf{r} = \mathbf{x}_1$, so again $U = V$.

We can now give the proof of Theorem 3.1. Clearly, \mathfrak{B}^*/Θ contains a \mathbf{p} -bridge from $\langle a_0, a_1 \rangle$ to $\langle b_0, b_1 \rangle$. Moreover, \mathfrak{B}^*/Θ satisfies (URC) by Corollary 3.7. Let $\mathfrak{A}' = \mathfrak{F}(\mathfrak{B}^*/\Theta)$. By Lemma 2.6, \mathfrak{A}' satisfies (URC). Thus, \mathfrak{A}' satisfies the requirements of Theorem 3.1.

4. The embedding theorem. Let τ be a fixed similarity type and let $(\mathbf{p}_i | i \in I)$ be a listing of $\mathbf{P}(\omega)$, the set of all polynomial symbols in the variables $\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \dots$. Let $\mathfrak{A}_0 = \mathfrak{A}$ be an algebra of type τ satisfying (URC). Form $\mathfrak{A}_{\gamma+1}$ from \mathfrak{A}_γ by direct limits formed by iterating the construction of Theorem 3.1 for each $\mathbf{p}_i, i \in I$, and each a_0, a_1, b_0, b_1 in A_γ for which $a_0 = a_1$ implies that $b_0 = b_1$. Thus, in $\mathfrak{A}_{\gamma+1}$ there is a \mathbf{p} -bridge from $\langle a_0, a_1 \rangle$ to $\langle b_0, b_1 \rangle$ for every polynomial symbol \mathbf{p} and all such a_0, a_1, b_0, b_1 in A_γ . Letting

$$\mathfrak{B} = \cup(\mathfrak{A}_\gamma | \gamma \in \omega),$$

we have the following:

THEOREM 4.1. *Let τ be any similarity type containing no constants and let \mathfrak{A} be an algebra of type τ satisfying the (URC). Then there is a simple algebra \mathfrak{B} of type τ containing \mathfrak{A} as a subalgebra, such that \mathfrak{B} has a \mathbf{p} -bridge from $\langle a_0, a_1 \rangle$ to $\langle b_0, b_1 \rangle$ for any polynomial symbol \mathbf{p} and all a_0, a_1, b_0, b_1 in B for which $a_0 = a_1$ implies that $b_0 = b_1$.*

COROLLARY 4.2. *Let τ be a similarity type containing no constants and let \mathfrak{A} be an algebra of type τ satisfying (URC). Then there is a simple algebra \mathfrak{B} of type τ containing \mathfrak{A} as a subalgebra, such that $\mathfrak{B} \in \Sigma^*$ for any congruence scheme Σ of type τ contained in τ .*

If Σ is a congruence scheme and if there exists a simple algebra $\mathfrak{B} \in \Sigma^*$, then there is a nontrivial equational class $\mathbf{K} \subseteq \Sigma^*$ such that the type of \mathfrak{B} is a reduct of the type of \mathbf{K} and \mathfrak{B} is embeddable in the τ -reduct of some algebra in \mathbf{K} (see [2], Theorem 8). We now apply this to Corollary 4.2 to give most of the Embedding Theorem.

THEOREM 4.3. *Let τ be a similarity type containing no constants. Let \mathfrak{A} be any algebra of type τ satisfying (URC) and let Σ be any congruence scheme such that the type of Σ is contained in τ . Then there exists an equational class \mathbf{K} such that $\mathbf{K} \subseteq \Sigma^*$ and \mathfrak{A} is isomorphic to a subalgebra of some τ -reduct of an algebra in \mathbf{K} .*

As observed in [2], the equational class \mathbf{K} enjoys a number of properties: \mathbf{K} is congruence distributive, semisimple, and has the Congruence Extension Property. Moreover, if C is any family of congruence schemes whose types are contained in τ , then the equational class \mathbf{K} can be constructed so that $\mathbf{K} \subseteq \Sigma^*$ for all $\Sigma \in C$.

Now we are ready to prove the Embedding Theorem. By Theorem 4.3, (i) implies (iii).

Let \mathfrak{B}_τ be the τ -reduct of the algebra \mathfrak{B} whose existence is claimed by (iii); then \mathfrak{B}_τ satisfies (ii), so (iii) implies (ii).

It remains to show that (ii) implies (i). By our assumption on the type τ , there is an n -ary operation symbol $\mathbf{f}(x_1, \dots, x_n)$ with $n > 1$. Let $\mathbf{r}(\mathbf{x}) \in \mathbf{P}(1)$ and consider the congruence scheme Σ consisting of $\langle \mathbf{f}(\mathbf{r}(\mathbf{x}), y_2, \dots, y_n), 0 \rangle$.

To verify (URC) for an algebra \mathfrak{A} satisfying (ii), let $a, b \in A$, $r(a) = r(b)$. Thus by (ii), \mathfrak{A} has an extension \mathfrak{B} satisfying $\mathfrak{B} \in \Sigma^*$. Since $a \equiv b(\Theta(a, b))$ in \mathfrak{B} , there exist $u_2, \dots, u_n \in B$ such that

$$a = f(r(a), u_2, \dots, u_n) \quad \text{and} \quad b = f(r(b), u_2, \dots, u_n).$$

By assumption $r(a) = r(b)$, hence $a = b$, verifying (URC) in \mathfrak{A} . This completes the proof of the Embedding Theorem.

5. A testing algebra. We start with a definition.

Definition 5.1. Let Σ be a congruence scheme of type τ . Let \mathfrak{A} be an algebra of type τ and $a, b, c, d \in A$. The algebra \mathfrak{A} is said to be $\langle a, b, c, d \rangle$ Σ -free if and only if for any algebra \mathfrak{B} of type τ satisfying $\mathfrak{B} \in \Sigma^*$ and for any $\bar{a}, \bar{b}, \bar{c}, \bar{d} \in B$ with $\Sigma(\bar{a}, \bar{b}, \bar{c}, \bar{d})$ in \mathfrak{B} , there exists a homomorphism $h: \mathfrak{A} \rightarrow \mathfrak{B}$ such that

$$h(a) = \bar{a}, h(b) = \bar{b}, h(c) = \bar{c}, \text{ and } h(d) = \bar{d}.$$

We note that if \mathfrak{A} is of type τ and \mathfrak{A} is $\langle a, b, c, d \rangle$ Σ -free, and if \mathfrak{B} is any algebra, not necessarily of type τ , with $\mathfrak{B} \in \Sigma^*$ and for which $\Sigma(\bar{a}, \bar{b}, \bar{c}, \bar{d})$ for some $\bar{a}, \bar{b}, \bar{c}, \bar{d} \in B$, then there is a homomorphism h of \mathfrak{A} to the $(\tau \cap (\text{type of } \mathfrak{B}))$ -reduct of \mathfrak{B} such that

$$h(a) = \bar{a}, h(b) = \bar{b}, h(c) = \bar{c}, \text{ and } h(d) = \bar{d}$$

In this section we shall prove the following.

THEOREM 5.2. *For any congruence scheme Σ of type τ containing no constants there exists an algebra $\mathfrak{A}(\Sigma)$ and elements $a, b, c, d \in \mathfrak{A}(\Sigma)$ such that the following three conditions hold:*

- (i) $\mathfrak{A}(\Sigma) \in \Sigma^*$
- (ii) $c \equiv d(\Theta(a, b))$;
- (iii) $\mathfrak{A}(\Sigma)$ is $\langle a, b, c, d \rangle$ Σ -free.

We call $\mathfrak{A}(\Sigma)$ a *testing algebra* for Σ . It tests several things. First of all, a scheme Σ has a nontrivial representation if and only if $\mathfrak{A}(\Sigma)$ is nontrivial. Secondly, if $\mathfrak{B} \in \Sigma^*$ then for any $\bar{c} \equiv \bar{d}(\Theta(\bar{a}, \bar{b}))$ in \mathfrak{B} , there must be a homomorphism h from $\mathfrak{A}(\Sigma)$ to the $(\tau \cap (\text{type of } \mathfrak{B}))$ -reduct of \mathfrak{B} , for which

$$h(a) = \bar{a}, h(b) = \bar{b}, h(c) = \bar{c}, \text{ and } h(d) = \bar{d}.$$

The validity of these two tests involving $\mathfrak{A}(\Sigma)$ follow immediately from the definition. A third use of $\mathfrak{A}(\Sigma)$ is contained in the next lemma.

LEMMA 5.3. *Let \mathfrak{A} be any algebra satisfying the three conditions of Theorem 5.2 for some $a, b, c, d \in A$. Let Ω be any congruence scheme. Then $\Sigma^* \subseteq \Omega^*$ if and only if $\Omega_{\mathfrak{A}}(a, b, c, d)$.*

Proof. One direction is immediate, so assume that $\Omega_{\mathfrak{A}}(a, b, c, d)$ holds. We wish to show that if \mathfrak{B} is any algebra, and if $\mathfrak{B} \in \Sigma^*$ then $\mathfrak{B} \in \Omega^*$. Let

$$\bar{c} \equiv \bar{d}(\Theta(\bar{a}, \bar{b})) \text{ in } \mathfrak{B}.$$

Then $\Sigma_{\mathfrak{B}}(\bar{a}, \bar{b}, \bar{c}, \bar{d})$. Let h be the homomorphism of \mathfrak{A} into the $(\tau \cap (\text{type of } \mathfrak{B}))$ -reduct of \mathfrak{B} , where τ is the type of \mathfrak{A} . Since $\Omega_{\mathfrak{A}}(a, b, c, d)$, therefore,

$$\Omega_{\mathfrak{B}}(h(a), h(b), h(c), h(d))$$

holds. Since

$$h(a) = \bar{a}, h(b) = \bar{b}, h(c) = \bar{c}, h(d) = \bar{d},$$

the proof is complete.

The proof of Theorem 5.2 will proceed by first constructing an $\langle a, b, c, d \rangle \Sigma$ -free algebra and then by extending it so as to represent Σ still preserving freeness.

LEMMA 5.4. *Let Σ be any congruence scheme. Then there exists an algebra \mathfrak{A} with $a, b, c, d \in A$, such that \mathfrak{A} is $\langle a, b, c, d \rangle \Sigma$ -free. Moreover, $\Sigma_{\mathfrak{A}}(a, b, c, d)$ holds.*

Proof. Let Σ be as described in Definitions 1.1 and 1.2. Let τ be the type of Σ and let $\mathbf{K}(\tau)$ be the class of all algebras of type τ . Let \mathfrak{F} be the free algebra in $\mathbf{K}(\tau)$ on free generators

$$\{a_0, a_1, b_0, b_1\} \cup \{x_i | 0 \leq i \leq k\}.$$

Define the congruence relation θ on \mathfrak{F} by

$$\begin{aligned} \theta = & \theta(b_0, p_1(a_{t_1}, x_1, \dots, x_k)) \vee \theta(b_1, p_n(a_{t_n}, x_1, \dots, x_k)) \\ & \vee \vee (\theta(p_i(a_{1-t_i}, x_1, \dots, x_k), p_{i+1}(a_{t_{i+1}}, x_1, \dots, x_k)) \\ & | 1 \leq i < n). \end{aligned}$$

Let $\mathfrak{A} = \mathfrak{F}/\theta$ and let $f: \mathfrak{F} \rightarrow \mathfrak{A}$ have kernel θ . Then clearly

$$\Sigma_{\mathfrak{A}}(f(a_0), f(a_1), f(b_0), f(b_1))$$

holds.

Let $\mathfrak{B} \in \Sigma^*$ and suppose for some $\bar{a}_0, \bar{a}_1, \bar{b}_0, \bar{b}_1$ in B that $\Sigma_{\mathfrak{B}}(\bar{a}_0, \bar{a}_1, \bar{b}_0, \bar{b}_1)$ holds via elements $\bar{x}_1, \dots, \bar{x}_k$. Let $g: \mathfrak{F} \rightarrow \mathfrak{B}$ be the unique homomorphism sending x to \bar{x} for each free generator x of \mathfrak{F} . The kernel of f is clearly contained in the kernel of g , so there exists a homomorphism $h: \mathfrak{A} \rightarrow \mathfrak{B}$ with $hf = g$. Thus \mathfrak{A} is $\langle f(a_0), f(a_1), f(b_0), f(b_1) \rangle \Sigma$ -free.

LEMMA 5.5. *Let Σ be a congruence scheme which contains no constants. Let \mathfrak{A} be $\langle a, b, c, d \rangle \Sigma$ -free. Let*

$$b_0 \equiv b_1(\Theta(a_0, a_1)) \text{ for some } a_0, a_1, b_0, b_1 \in A.$$

Then there exists an algebra \mathfrak{A}' , of the same type as \mathfrak{A} , such that:

- (i) *there is a homomorphism $f: \mathfrak{A} \rightarrow \mathfrak{A}'$;*
- (ii) *if \mathfrak{B} is any algebra in Σ^* and if h is any homomorphism of \mathfrak{A} to \mathfrak{B} , then there is a homomorphism $h': \mathfrak{A}' \rightarrow \mathfrak{B}$ such that $h'f = h$;*
- (iii) $\Sigma_{\mathfrak{A}'}(f(a_0), f(a_1), f(b_0), f(b_1))$;
- (iv) \mathfrak{A}' is $\langle f(a), f(b), f(c), f(d) \rangle \Sigma$ -free.

Proof. Let \mathfrak{A} and Σ be of type τ with Σ as above. Let \mathfrak{F} be the free $K(\tau)$ algebra on free generators x_1, \dots, x_k . Note that free products exist in $K(\tau)$ since τ contains no constants. Let $\mathfrak{A} * \mathfrak{F}$ be the free product of \mathfrak{A} and \mathfrak{F} in $K(\tau)$. We shall consider \mathfrak{A} and \mathfrak{F} as subalgebras of $\mathfrak{A} * \mathfrak{F}$. Let Θ be the congruence relation defined in the proof of Lemma 5.4. Forming $\mathfrak{A}' = (\mathfrak{A} * \mathfrak{F})/\Theta$ with $k:\mathfrak{A} * \mathfrak{F} \rightarrow \mathfrak{A}'$ having kernel Θ , we let f be the restriction of k to \mathfrak{A} ; thus $f:\mathfrak{A} \rightarrow \mathfrak{A}'$. Moreover

$$\Sigma_{\mathfrak{A}'}(f(a_0), f(a_1), f(b_0), f(b_1))$$

holds, so (i) and (ii) are satisfied. Let $\mathfrak{B} \in \Sigma^*$ and let h be an arbitrary homomorphism of \mathfrak{A} into \mathfrak{B} . Since

$$\begin{aligned} b_0 &\equiv b_1(\Theta(a_0, a_1)) \text{ in } \mathfrak{A}, \\ h(b_0) &\equiv h(b_1)(\Theta(h(a_0), h(a_1))) \text{ in } \mathfrak{B}, \end{aligned}$$

and thus

$$\Sigma_{\mathfrak{B}}(h(a_0), h(a_1), h(b_0), h(b_1))$$

holds. Let

$$\Sigma_{\mathfrak{B}}(h(a_0), h(a_1), h(b_0), h(b_1))$$

hold via $\bar{x}_1, \dots, \bar{x}_k$ and let $h^*:\mathfrak{F} \rightarrow \mathfrak{B}$ be the homomorphism sending x_i to \bar{x}_i , $i = 1, 2, \dots, k$. Now $h:\mathfrak{A} \rightarrow \mathfrak{B}$ and $h^*:\mathfrak{F} \rightarrow \mathfrak{B}$, so there exists a homomorphism $g:\mathfrak{A} * \mathfrak{F} \rightarrow \mathfrak{B}$ which extends both h and h^* . As in the proof of Lemma 5.4, Θ is contained in the kernel of g . Hence, there exists a map $h':\mathfrak{A}' \rightarrow \mathfrak{B}$ with $h'f = h$, and this proves (iii). To prove (iv), we observe that (ii) together with the fact that \mathfrak{A} is $\langle a, b, c, d \rangle$ Σ -free guarantees that h' is the desired homomorphism. This completes the proof of the lemma.

We now prove Theorem 5.2. Let \mathfrak{A}_0 be any $\langle a_0, b_0, c_0, d_0 \rangle$ Σ -free algebra, constructed as in Lemma 5.4. Note that \mathfrak{A}_0 is countable. For each $c \equiv d(\Theta(a, b))$ in \mathfrak{A}_0 , apply Lemma 5.5. The resulting family of algebras and homomorphisms gives a countable direct limit system. Let \mathfrak{A}_1 be the direct limit. By Lemma 5.4 (iii) and the properties of direct limits, the algebra \mathfrak{A}_1 is $\langle a_1, b_1, c_1, d_1 \rangle$ Σ -free, where $a_1, b_1, c_1, d_1 \in A_1$ are the canonical images of $a_0, b_0, c_0, d_0 \in A_0$. Continuing in this way we obtain $\mathfrak{A}_2, \mathfrak{A}_3, \dots$. Finally, let \mathfrak{A} be the direct limit of the \mathfrak{A}_i , $i = 0, 1, \dots$. Again \mathfrak{A} is $\langle a, b, c, d \rangle$ Σ -free where a, b, c, d are the images of a_0, b_0, c_0, d_0 . Thus $\Sigma_{\mathfrak{A}}(a, b, c, d)$ holds, so $c \equiv d(\Theta(a, b))$. It remains to show that $\mathfrak{A} \in \Sigma^*$. Let

$$u \equiv v(\Theta(x, y)) \text{ in } \mathfrak{A}.$$

Thus, there exist unary algebraic functions q_0, q_1, \dots, q_{m-1} such that the sets $\{q_i(x), q_i(y)\}$ form a chain from u to v . Let Z be the set of all elements of A used as arguments in these unary algebraic functions. Let

the integer k be chosen so that for each $z \in Z$ there exists $z_k \in A_k$ with $g_{k,\infty}(z_k) = z$, where $g_{k,\infty}$ is the canonical homomorphism from \mathfrak{A}_k to \mathfrak{A} . Since Z is finite, such a k exists, so

$$u_k \equiv v_k(\Theta(x_k, y_k)) \text{ in } \mathfrak{A}_k.$$

Hence

$$\Sigma_{\mathfrak{A}_{k+1}}(x_k, y_k, u_k, v_k).$$

Thus $\Sigma_{\mathfrak{A}}(x, y, u, v)$ holds as desired. This completes the proof of the theorem.

6. Problems and examples. Let Σ be a congruence scheme and let \mathfrak{A} be an algebra in Σ^* . If a, b , and c are arbitrary elements of \mathfrak{A} , then

$$\Sigma_{\mathfrak{A}}(a, b, a, b), \Sigma_{\mathfrak{A}}(a, b, b, a), \text{ and } \Sigma_{\mathfrak{A}}(a, b, c, c)$$

must hold. These particular instances of $\Sigma_{\mathfrak{A}}$ are useful for finding schemes derivable from Σ and for investigating varieties $\mathbf{K} \subseteq \Sigma^*$.

In particular, if Σ is a scheme we call a scheme Σ' a *reduction* of Σ if $\Sigma^* = \Sigma'^*$, and the sum of the ranks of the polynomial symbols in Σ' is less than the sum of the ranks of the polynomial symbols in Σ .

For example, if

$$\Sigma = \{ \langle x + (y_1 + y_2), 0 \rangle \} \text{ and } \Sigma' = \{ \langle x + y_3, 0 \rangle \},$$

then clearly $\Sigma^* \subseteq \Sigma'^*$ and the rank of the polynomial in Σ' is less than the rank of the polynomial in Σ . Also, $\Sigma'^* \subseteq \Sigma^*$, since if $\mathfrak{A} \in \Sigma'^*$ and $c \equiv d(\Theta(a, b))$ in \mathfrak{A} , then there exists $e \in A$ such that $c = a + e$ and $d = b + e$. But

$$e \equiv e(\Theta(e, e)),$$

so there is an element $e' \in A$ such that $e = e + e'$; thus,

$$c = a + (e + e') \text{ and } d = b + (e + e').$$

So $\Sigma_{\mathfrak{A}}(a, b, c, d)$ holds and Σ' is a reduction of Σ .

Similarly, the scheme

$$\Sigma = \{ \langle (x + (y_1 + y_2)) + (x + y_3), x + ((y_4 + y_5) + y_6), 0 \rangle \}$$

has a reduction

$$\Omega = \{ \langle (x + (y_1 + y_2)) + (x + y_3), x + y_5, 0 \rangle \}.$$

A general description of this method of forming reductions is the following.

Example 6.1. Let Σ be a congruence scheme and suppose that \mathbf{p}_i is a polynomial symbol of Σ such that

$$p_i = r(r_1, \dots, r_m)$$

for some polynomial symbols r, r_1, \dots, r_m , where at least one of the r_i is not a variable. Suppose also that there exists some p_j of Σ such that

$$r(y_1^j, \dots, y_m^j) \in C(p_j)$$

and the variables $y_l^j, 1 \leq l \leq m$, occur only in $r(y_1^j, \dots, y_m^j)$. Let Ω be the congruence scheme obtained from Σ by replacing the polynomial symbol $r(y_1^j, \dots, y_m^j)$ in p_j by a new auxiliary variable y . Then Ω is a reduction of Σ .

Proof. Clearly, $\Sigma^* \subseteq \Omega^*$ and Ω has rank less than that of Σ . Suppose that $\mathfrak{A} \in \Omega^*$ and $c \equiv d(\Theta(a, b))$ in \mathfrak{A} . Let e be the value of y in \mathfrak{A} used to establish $\Omega_{\mathfrak{A}}(a, b, c, d)$. $\Omega_{\mathfrak{A}}(e, e, e, e)$ holds, so by virtue of $p_j \in \Sigma$,

$$e = r(e_1, \dots, e_m) \quad \text{for some } e_1, \dots, e_m \text{ in } \mathfrak{A}.$$

Then $\Sigma_{\mathfrak{A}}(a, b, c, d)$ holds using e_l as the value $y_l^j, 1 \leq l \leq m$, and all other auxiliary variables as those used to establish $\Omega_{\mathfrak{A}}(a, b, c, d)$.

Problem 1. Given an arbitrary scheme Σ find all reductions of Σ . In particular, find all Σ which have no reductions.

We recall here the three order relations on congruence schemes that were defined in [2]. If Σ and Ω are congruence schemes, then

$\Sigma \subseteq_i \Omega$ means that for all algebras $\mathfrak{A}, \Sigma_{\mathfrak{A}} \subseteq \Omega_{\mathfrak{A}}$;

$\Sigma \subseteq_a \Omega$ means that $\Sigma^* \subseteq \Omega^*$;

$\Sigma \subseteq_e \Omega$ means that for every equational class K ,

$$K \subseteq \Sigma^* \text{ implies } K \subseteq \Omega^*.$$

It is clear that if Σ and Ω are schemes and $\Sigma \subseteq_i \Omega$, then $\Sigma \subseteq_a \Omega$, and if $\Sigma \subseteq_a \Omega$, then $\Sigma \subseteq_e \Omega$.

Example 6.2. There exist congruence schemes Σ and Ω such that $\Sigma \subseteq_a \Omega$ but $\Sigma \not\subseteq_i \Omega$.

Proof. Let Σ have only one polynomial symbol $x + y_0^0$ with $t_0 = 0$. Let Ω have exactly two polynomial symbols, $x + y_0^0$ and $x + y_0^1$ with $t_0 = t_1 = 0$. If \mathfrak{A} is any algebra in Σ^* with $c \equiv d(\Theta(a, b))$, then there exists an $e \in A$ with $c = a + e$ and $d = b + e$. Moreover, $\Sigma_{\mathfrak{A}}(a, b, d, d)$ holds, so there exists $e' \in A$ satisfying $d = a + e'$ and $d = b + e'$. Hence $\Omega_{\mathfrak{A}}(a, b, c, d)$ holds. To show that $\Sigma \not\subseteq_i \Omega$, consider the completely free algebra \mathfrak{F} of type $+$, having two generators x and y . Note that

$$\Sigma_{\mathfrak{F}}(x, y, x + x, y + x)$$

holds. If

$$\Omega_{\mathfrak{F}}(x, y, x + x, y + x)$$

were to hold, then there would exist $\mathbf{q}_1, \mathbf{q}_2$ in \mathfrak{F} with $\mathbf{y} + \mathbf{q}_1 = \mathbf{x} + \mathbf{q}_2$. Then (F4) would imply $\mathbf{x} = \mathbf{y}$ which is not the case.

Problem 2. Does $\Sigma \subseteq_e \Sigma'$ imply $\Sigma \subseteq_a \Sigma'$?

In any equational class, the free algebra on a given number of generators is unique up to isomorphism.

Problem 3. Does any $\langle a, b, c, d \rangle$ Σ -free algebra contain as a subalgebra an algebra isomorphic to the algebra constructed in Theorem 5.2?

If an algebra \mathfrak{A} represents the congruence scheme Σ , then \mathfrak{A} and its subalgebras will satisfy the (URC) with respect to all those unary polynomial symbols \mathbf{r} for which there is a polynomial symbol \mathbf{p} in Σ which can be represented in the form $q(\mathbf{r}(\mathbf{x}), \mathbf{y}_1, \dots, \mathbf{y}_n)$.

Problem 4. Is the above condition necessary and sufficient for an algebra \mathfrak{A} to have an extension to represent a given congruence scheme?

Similarly, the requirement that τ have no constants was used to avoid complications with free completions and free products, and to guarantee that the scheme Σ has a nontrivial representation.

Problem 5. Find a version of the Embedding Theorem in which τ and Σ can have constants.

REFERENCES

1. J. T. Baldwin and J. Berman, *Definable principal congruence relations: kith and kin*, Acta Math. Sci. Szeged 44 (1982), 255-270.
2. J. Berman and G. Grätzer, *Uniform representations of congruence schemes*, Pacific J. Math 76 (1978), 301-311.
3. W. J. Blok and D. Pigozzi, *On the structure of varieties with equationally definable principal congruences. I*, Algebra Universalis 15 (1982), 195-227.
4. E. Fried, G. Grätzer, and R. W. Quackenbush, *Uniform congruence schemes*, Algebra Universalis 10 (1980), 176-188.
5. G. Grätzer, *Universal algebra*, Second Edition (Springer Verlag, New York, Heidelberg, Berlin, 1979).
6. P. Köhler and D. Pigozzi, *Varieties with equationally defined principal congruences*, Algebra Universalis 11 (1980), 213-219.

*University of Illinois at Chicago,
Chicago, Illinois;
University of Manitoba,
Winnipeg, Manitoba*