DEFINABLE PRINCIPAL SUBCONGRUENCES

KIRBY A. BAKER AND JU WANG

ABSTRACT. For varieties of algebras, we present the property of having "definable principal subcongruences" (DPSC), generalizing the concept of having definable principal congruences. It is shown that if a locally finite variety V of finite type has DPSC, then V has a finite equational basis if and only if its class of subdirectly irreducible members is finitely axiomatizable. As an application, we prove that if A is a finite algebra of finite type whose variety $V(A)$ is congruence distributive, then $V(A)$ has DPSC. Thus we obtain a new proof of the finite basis theorem for such varieties. In contrast, it is shown that the group variety $V(S_3)$ does not have DPSC.

1. INTRODUCTION

We consider only varieties of finite type. Following Baldwin and Berman [3] and McKenzie [10], let us say that a first-order formula $\Gamma(u, v, x, y)$ is a *congruence formula* if it is positive existential and $\Gamma(u, v, x, x) \to u \approx v$ holds in all algebras of the relevant type. It follows that $\Gamma(u, v, x, y)$ implies $\langle u, v\rangle \in \mathrm{Cg}(x, y)$ (the principal congruence relation generated by identifying x and y) in any algebra of the type. A typical congruence formula expresses the assertion that $\langle u, v\rangle$ can be reached from $\langle x, y\rangle$ by using one of finitely many Mal'tsev congruence schemes [7].

For some congruence formulas Γ and instances of x, y in an algebra, it is the case that $\Gamma(\_, \_, x, y)$ *is* $\mathrm{Cg}(x, y)$. A useful observation [10] is that this case can be described by a first-order formula $\Pi_\Gamma(x, y)$; specifically, $\Pi_\Gamma(x, y)$ asserts that $\Gamma(\_, \_, x, y)$ is an equivalence relation compatible with the (finitely many) basic operations and also that $\Gamma(x, y, x, y)$ holds.

Date: May 7, 2000.

1991 *Mathematics Subject Classification.* Primary: 08B05; Secondary: 08B10, 08C10.

Key words and phrases. finite basis,congruence distributive,congruence formula, principal congruence.

Work of the second author supported by Chinese National Technology Project 97-3.

A variety V is said to have *definable principal congruences* (DPC) [3] if there is a first-order formula $\Gamma(u,v,x,y)$ such that in any $B \in V$, $\langle c,d\rangle \in \mathrm{Cg}(a,b)$ if and only if $B \models \Gamma(c,d,a,b)$. If V does have DPC, then Γ can be taken to be a congruence formula.

McKenzie [10] proves that if V is a variety of finite type with DPC and only finitely many subdirectly irreducible members up to isomorphism, all finite, then V is finitely based. We generalize this fact by defining the concept of having definable principal subcongruences (DPSC) and showing (Theorem 1) that if V is a locally finite variety of finite type with DPSC for which the class of subdirectly irreducible members is definable (finitely axiomatizable), then V is finitely based. An application is to congruence distributive varieties generated by a finite algebra A of finite type, which are shown to have DPSC (Theorem 2). The resulting proof of the finite basis theorem [1, 9] for this congruence distributive case avoids dependence on computation with Jónsson terms [8]; cf. [1, 9, 2].

General references for varieties of algebras are [5] and [11].

2. Definable principal subcongruences

Definition. *A variety V has* **definable principal subcongruences** *(DPSC) if there are congruence formulas $\Gamma_1(u,v,x,y)$ and $\Gamma_2(u,v,x,y)$ such that given any algebra $B \in V$ and elements $a,b \in B$ with $a \neq b$ there exist elements $c,d \in B$ with $c \neq d$ for which $B \models \Gamma_1(c,d,a,b)$ and $B \models \Pi_{\Gamma_2}(c,d)$.*

In essence, the condition for DPC says that the variety has a finite list of congruence schemes [7] sufficient to compute any principal congruence, while the condition for DPSC says that the variety has a finite list of congruence schemes sufficient to reach a principal congruence that can be fully computed by a predetermined finite list of congruence schemes. Observe that DPC implies DPSC.

An instructive example is the variety $V(M_3)$, where M_3 is the five-element modular lattice with three atoms. By Theorem 2 below, $V(M_3)$ has DPSC, but McKenzie [10] shows that $V(M_3)$ does not have DPC. McKenzie observes that $V(M_3)$ contains lattices P_n for $n = 1, 2, \ldots$, of which P_4 is shown in Figure 1. The computation $\langle b,1\rangle \in \mathrm{Cg}^{P_n}(a,b)$ requires a sequence of transitivities of length at least n, so there cannot be a single formula for principal congruences and DPC fails. On the other hand, the condition for DPSC is satisfied; for example, in P_4 with a,b as indicated, one can choose c,d as shown and then a typical pair $\langle r,s\rangle \in \mathrm{Cg}(c,d)$ is reached via a computation whose complexity has a bound depending only on the variety. See also [4].

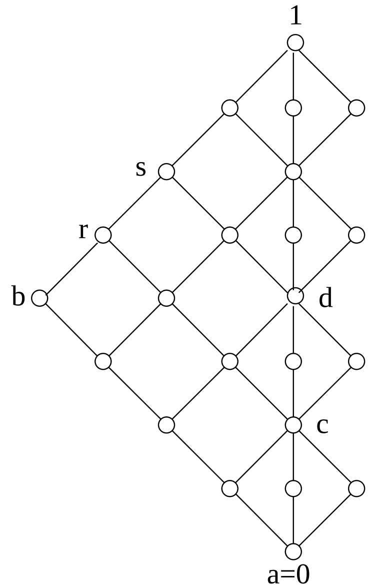

FIGURE 1. The lattice P_4 of McKenzie

A class of similar algebras is said to be *finitely axiomatizable* (or *strictly elementary* or *definable*) if it is the class of models of some first-order sentence. By the compactness theorem, the finitely axiomatizable varieties are simply those that are finitely based.

As mentioned, McKenzie [10] showed that a variety of finite type with DPC and with only finitely many subdirectly irreducible members, all finite, is finitely based. The following fact is a generalization. For any class $\mathcal{K}$ of similar algebras, let $\mathcal{K}_{\mathrm{SI}}$ denote the class of subdirectly irreducible members of $\mathcal{K}$.

Theorem 1. *A variety V with definable principal subcongruences is finitely based if and only if V_{SI} is finitely axiomatizable.*

The proof depends on the following lemma. For convenience, let us say that a class $\mathcal{K}$ of similar algebras has a property "doubly" if both $\mathcal{K}$ and $\mathcal{K}_{\mathrm{SI}}$ have the property.

Lemma. *If a variety V is contained in a doubly finitely axiomatizable class $\mathcal{K}$, then V is either doubly finitely axiomatizable or doubly not finitely axiomatizable.*

Proof (after Jònsson [9]): First suppose that V is not finitely axiomatizable. Then there exists an index set I, algebras $A_i \notin V, i \in I$, and an ultrafilter $\mathcal{U}$ on I such that the resulting ultraproduct A^* is in V, by [6] Theorem 4.1.12, or by taking $I = \omega$ and for each i choosing

A_i to satisfy all i-variable laws of V but not all laws. If we replace each A_i by one of its subdirectly irreducible subdirect factors not in V, then A^* is replaced by a homomorphic image, so without loss of generality we may assume that each A_i is subdirectly irreducible. Further, since $A^* \in \mathcal{K}$, which is finitely axiomatizable, we have $\{i \in I : A_i \in \mathcal{K}\} \in \mathcal{U}$, so without loss of generality we may assume $A_i \in \mathcal{K}$ for all i. Then $A_i \in \mathcal{K}_{\mathrm{SI}}$ for all i, and since $\mathcal{K}_{\mathrm{SI}}$ is axiomatizable, A^* is subdirectly irreducible. Thus $A_i \notin \mathcal{V}_{\mathrm{SI}}$ for all i but $A^* \in \mathcal{V}_{\mathrm{SI}}$. Therefore V_{SI} is not finitely axiomatizable.

Suppose on the other hand that V *is* finitely axiomatizable. Then so is $V_{\mathrm{SI}} = V \cap \mathcal{K}_{\mathrm{SI}}$. □

Proof of Theorem 1: Let Γ_1 and Γ_2 be congruence formulas witnessing DPSC for V and let $\mathcal{K}$ be the class of all algebras (of the type of V) for which Γ_1 and Γ_2 witness DPSC. Observe that $\mathcal{K}$ is the class of models of

$$\Phi \;\equiv\; (\forall a,b)[a \neq b \rightarrow (\exists c,d)[c \neq d \;\wedge\; \Gamma_1(c,d,a,b) \wedge \Pi_{\Gamma_2}(c,d)]],$$

while $\mathcal{K}_{\mathrm{SI}}$ is the class of models of $\Phi \wedge \Psi$ for

$$\Psi \equiv (\exists r,s)[r \neq s \wedge (\forall a,b)[(a \neq b \rightarrow (\exists c,d)[\Gamma_1(c,d,a,b) \wedge \Gamma_2(r,s,c,d))]].$$

Since $V \subseteq \mathcal{K}$, the Lemma applies. □

Remarks. *The same kind of argument would apply if it is the class of finitely subdirectly irreducible members of V that is finitely axiomatizable.*

3. Congruence-distributive varieties generated by a finite algebra

Theorem 2. *Let A be a finite algebra of finite type for which $V(A)$ is congruence distributive. Then $V(A)$ has definable principal subcongruences.*

The proof depends on this fact about embeddings in a product:

Observation. *In a congruence distributive variety, consider an embedding $C \hookrightarrow \prod_{i \in I} A_i$, where C is finite. Let $p,q,r,s \in C$. Then $\langle r,s\rangle \in \mathrm{Cg}^C(p,q)$ in C if and only if the same holds in the projected image of C in each factor, i.e., for each $i \in I$ we have $\langle \bar{r},\bar{s}\rangle \in \mathrm{Cg}^{\pi_i(C)}(\bar{p},\bar{q})$, where $\bar{r},\bar{s},\bar{p},\bar{q}$ are the images in A_i.*

Indeed, "only if" is automatic. For "if", observe that $\mathrm{Cg}^C(r,s) \leq \mathrm{Cg}^C(p,q) \vee \ker \pi_i$ for each i. Since C is finite there are only finitely many possible kernels, so that the distributive law applies: $\mathrm{Cg}^C(r,s) \leq$

$\cap_{i\in I}(\mathrm{Cg}^C(p,q) \vee \ker \pi_i) = \mathrm{Cg}^C(p,q) \vee (\cap_{i\in I} \ker \pi_i) = \mathrm{Cg}^C(p,q) \vee 0 = \mathrm{Cg}^C(p,q)$.

Proof of Theorem 2: By Jònsson's Lemma [8], $V(A)$ has up to isomorphism only finitely many subdirectly irreducible members, all finite. Let N be the maximum of their cardinalities. We proceed as follows. Given any algebra $B \in V(A)$ and $a \neq b$ in B, we shall construct a subalgebra D of B with at most N generators, including a and b, and designate $c \neq d$ in D with $\mathrm{Cg}^D(c,d) \leq \mathrm{Cg}^D(a,b)$. Next, given any $r,s \in B$ with $\mathrm{Cg}^B(r,s) \leq \mathrm{Cg}^B(c,d)$, we shall let C be the subalgebra of B generated by D and r,s and show that $\langle r,s\rangle \in \mathrm{Cg}^C(c,d)$. By local finiteness, $|D|$ and $|C|$ have finite bounds depending only on A. Therefore there are congruence formulas $\Gamma_1(u,v,x,y)$ and $\Gamma_2(u,v,x,y)$, depending only on A, with $\Gamma_1(c,d,a,b)$ holding in D and hence in B, and with $\Gamma_2(r,s,c,d)$ holding in C and hence in B, as required. Thus $V(A)$ has DPSC.

To construct D, let $B \hookrightarrow \prod_{i\in I} S_i$ be a subdirect representation of B, with coordinate maps $\pi_i : B \to S_i$, $i \in I$. Choose $j \in I$ so that $n(j) = |S_j|$ is as large as possible subject to $\pi_j(a) \neq \pi_j(b)$. Choose preimages $e_1, \ldots, e_{n(j)} \in B$ of the elements of S_j under π_j, with $e_1 = a$ and $e_2 = b$. Let D be the subalgebra of B generated by $e_1, \ldots, e_{n(j)}$. Thus $\pi_j(D) = S_j$. For convenience, write π_i^D for $\pi_i|_D$.

Since S_j is subdirectly irreducible, $\ker \pi_j^D$ is completely meet irreducible in $\mathrm{Con}(D)$. By the congruence distributivity of $V(A)$, the interval $[0, \ker \pi_j^D]$ in $\mathrm{Con}(D)$ is a prime ideal; therefore its complement is a dual ideal whose least element α is join-prime. In particular, α is the least congruence on D not under $\ker \pi_j^D$. Because $\mathrm{Cg}^D(a,b) \not\leq \ker \pi_j^D$ we have $\alpha \leq \mathrm{Cg}^D(a,b)$. Moreover, since α is join-prime and is a finite join of principal congruences, α is principal, say $\alpha = \mathrm{Cg}^D(c,d)$.

Let us say that say i *splits* $u, v \in B$ if $\pi_i(u) \neq \pi_i(v)$. Observe that if i splits c,d, then $\mathrm{Cg}^D(c,d) \not\leq \ker \pi_i^D$ and i also splits a,b, so by the minimality of $\alpha = \mathrm{Cg}^D(c,d)$ we have $\ker \pi_i^D \leq \ker \pi_j^D$. Then there is an induced map of $D/\ker \pi_i^D \cong \pi_i(D)$ onto $D/\ker \pi_j^D \cong \pi_j(D) = S_j$. By the choice of j, π_i maps D onto S_i.

Now let $r,s \in B$ be given with $\mathrm{Cg}^B(r,s) \leq \mathrm{Cg}^B(c,d)$. As mentioned, let C be the subalgebra of B generated by D and r,s. Again by the local finiteness of $V(A)$, C is finite. We apply the Observation to c,d,r,s and $C \hookrightarrow \prod_{i\in I} S_i$, as follows. If i splits c,d, then $\pi_i(C) = S_i = \pi_i(B)$, so $\langle \bar{r}, \bar{s}\rangle \in \mathrm{Cg}^{\pi_i(B)}(\bar{c},\bar{d}) = \mathrm{Cg}^{\pi_i(C)}(\bar{c},\bar{d})$, where $\bar{r},\bar{s},\bar{c},\bar{d}$ are images in S_i. If i does not split c,d, then neither does i split r,s, so again $\langle \bar{r}, \bar{s} \rangle \in \mathrm{Cg}^{\pi_i(C)}(\bar{c}, \bar{d}) = 0$. Then the Observation applies to show $\langle r, s \rangle \in \mathrm{Cg}^C(c, d)$. $\square$

Corollary ([1])**.** *If A is a finite algebra of finite type for which $V(A)$ is congruence distributive, then A is finitely based.*

4. A group variety without DPSC

Theorem 3. *The group variety $V(S_3)$ does not have DPSC.*

Proof: We start from the observation that a variety V with DPSC has "definable atomic congruences in finite members" in the sense that there is a congruence formula $\Gamma(u, v, x, y)$ for V such that in any finite member B of V, for each nontrivial congruence $\mathrm{Cg}^B(a, b)$ there is *some* atomic congruence $\mathrm{Cg}^B(r, s) \leq \mathrm{Cg}^B(a, b)$ for which $\Gamma(r, s, a, b)$ holds. Indeed, given a, b we can choose c, d as in the definition of DPSC and then an atomic congruence $\mathrm{Cg}^B(r, s)$ under $\mathrm{Cg}^B(c, d)$, so that $\Gamma(r, s, a, b)$ holds for $\Gamma(u, v, x, y) \equiv (\exists z, w)[\Gamma_1(z, w, x, y) \wedge \Gamma_2(u, v, z, w)]$, again a congruence formula.

If V is a group variety, then principal congruences correspond to principal normal subgroups. For $a \in B \in V$, the elements of the principal normal subgroup $N(a)$ generated by a are the products of conjugates of a and a^{-1}. Let V have finite exponent, so that mention of a^{-1} can be omitted. By compactness, V has definable atomic congruences in finite members when there is a bound M such that for any finite member B of V and $a \in B$ with $a \neq 1$ there exists a minimal normal subgroup of B generated by the product of at most M conjugates of a.

We shall show that $V(S_3)$ lacks such a bound. Write $S_3 = \{1, c, c^2, b, bc, bc^2\}$, where $c^3 = 1$, $b^2 = 1$ and $cb = bc^2$. For future reference, observe that a conjugate $c^v = v^{-1}cv$ of c for $v \in S_3$ depends only on the coset of v modulo $A_3 = \{1, c, c^2\}$. For each n let B_n be the subgroup of $S_3^{2^n}$ generated by $\mathbf{b}_1^{(n)}, \ldots, \mathbf{b}_n^{(n)}$, where $\mathbf{b}_1^{(n)} = \langle 1, b, 1, b, \ldots \rangle$, $\mathbf{b}_2^{(n)} = \langle 1, 1, b, b, 1, 1, b, b, \ldots \rangle$, and in general $\mathbf{b}_k^{(n)}$ has alternating runs of 1's and b's each of length 2^{k-1}. Let E_n be the larger subgroup of $S_3^{2^n}$ generated by $\mathbf{b}_1^{(n)}, \ldots, \mathbf{b}_n^{(n)}$ and $\mathbf{c} = \langle c, c, \ldots, c \rangle$.

First we show that the minimal normal subgroups of E_n are all of the form $\{1\} \times \cdots \times \{1\} \times A_3 \times \{1\} \times \cdots \{1\}$. To establish principles let us examine E_1, which is generated by $\langle 1, b \rangle$ and $\langle c, c \rangle$. If N is a nontrivial normal subgroup not of the stated form, then N has an element $\langle x, y \rangle$ in which neither of x, y is 1. In the case where $y \in A_3$, we have $[\langle x, y \rangle, \langle 1, b \rangle] = \langle 1, y \rangle$ and $\{1\} < N(\langle 1, y \rangle) < N$. In the case where $y \notin A_3$, since $x \in A_3$ we have $[\langle x, y \rangle, \langle c, c \rangle] = \langle 1, c \rangle$ and $\{1\} < N(\langle 1, c \rangle) < N$. For E_1, these are the only cases, so that N

is not minimal. More generally, if $N \lhd E_n$ is a nontrivial normal subgroup not of the stated form, then N has some element $\mathbf{x}$ with two entries x_i, x_j neither of which is 1. In the case where both $x_i, x_j \in A_3$, as with E_1 we take the commutator of $\mathbf{x}$ with a generator $\mathbf{b}_k^{(n)}$ whose i-th and j-th entries differ. In the case where one of x_i, x_j is in A_3 and the other is not, we take the commutator with $\mathbf{c}$. In the case where $x_i, x_j \notin A_3$ (a case that does not occur for E_1), the i-th and j-th entries of $[\mathbf{x}, \mathbf{c}] \in N$ are both c, so we have arrived back at the first case. In all cases, we find that N is not minimal, showing that minimal normal subgroups of E_n do have the stated form.

Now suppose that there is a bound M as above for V. Let $n = M+1$ and consider any $\mathbf{a} \in N(\mathbf{c}) \lhd E_n$ other than the identity. We shall show that $N(\mathbf{a})$ cannot be a minimal normal subgroup of E_n. By assumption $\mathbf{a}$ is the product of at most $M < n$ conjugates of $\mathbf{c}$, say $\mathbf{a} = \mathbf{c}^{\mathbf{v}^{(1)}} \cdots \mathbf{c}^{\mathbf{v}^{(k)}}$, where $k < n$. Each conjugate $\mathbf{c}^{\mathbf{v}^{(i)}}$ is determined by the A_3-cosets of the entries of $\mathbf{v}^{(i)}$; say $v_j^{(i)} \in h_j^{(i)} A_3$, where $h_j^{(i)} \in \{1, b\}$. If we set $\mathbf{h}^{(i)} = \langle h_1^{(i)}, \dots, h_{2^n}^{(i)} \rangle$, we see $\mathbf{h}^{(i)} \in B_n$. A claim: The set of 2^n coordinate indices can be partitioned into nonsingleton blocks in such a way that the entries of each $\mathbf{h}^{(i)}$ are constant on each block. From this claim it follows that the entries of $\mathbf{a}$ are constant on each block. Then each entry value occurs in at least two coordinates and so $\mathbf{a}$ is not in any minimal normal subgroup as characterized above. We conclude that $V(S_3)$ does not have definable atomic congruences in finite members.

To verify the claim, let H be the subgroup of B_n generated by $\mathbf{h}^{(1)}, \dots, \mathbf{h}^{(k)}$. Since B_n is an elementary 2-group with n independent generators and H has fewer than n generators, we have $H < B_n$. The corresponding subgroup H' of the dual group $\widehat{B_n}$ is nontrivial and consists of characters that have value 1 on H. Two characters are in the same coset of H' when they agree on H. Now observe that from the construction of B_n the coordinate projections $\pi_i : B_n \to \{1, b\}$ *are* the characters of B_n with $\{1, b\}$ playing the role of $\{-1, 1\}$. Thus the 2^n coordinate indices are partitioned into blocks of equal size (the cosets) such that each element of H has constant entries on each block. This is the partition to which the claim refers. □

The authors are grateful to George McNulty and Andrew Glass for a number of valuable suggestions.

References

[1] K. A. Baker, *Finite equational bases for finite algebras in a congruence-distributive equational class,* Advances in Math. **24** (1977), 207-273.

[2] K. A. Baker and J. Wang, *Approximate distributive laws and finite equational bases for finite algebras in congruence-distributive varieties,* (to appear).

[3] J. T. Baldwin and J. Berman, *On the number of subdirectly irreducible algebras in a variety,* Algebra Universalis **5** (1975), 378-389.

[4] S. Burris, *An example concerning definable principal congruences,* Algebra Universalis **7** (1977), 403-404.

[5] S. Burris and H. P. Sankappanavar, *A Course in Universal Algebra,* Springer-Verlag, New York, 1981.

[6] C. C. Chang and H. J. Keisler, *Model Theory,*, North-Holland Publ. Co., Amsterdam, 1973.

[7] E. Fried, G. Grätzer, and R. Quackenbush, *Uniform congruence schemes*, Algebra Universalis **10** (1980), 176-188.

[8] B. Jónsson, *Algebras whose congruence lattices are distributive,* Math. Scand., **21** (1967), 110-121.

[9] B. Jónsson, *On finitely based varieties of algebras*, Colloq. Math. **42** (1979), 255-261.

[10] R. McKenzie, *Para primal varieties: a study of finite axiomatizability and definable principal congruences in locally finite varieties*, Algebra Universalis **8** (1978), 336-348.

[11] R. McKenzie, G. McNulty and W. Taylor, *Algebras, Lattices, Varieties,* vol I, Wadsworth & Brooks/Cole

University of California, Box 951555, Los Angeles, CA 90095-1555, USA

E-mail address: baker@math.ucla.edu

Institute of Software, Academia Sinica, Beijing, 100080, China