WEAKLY DEFINABLE PRINCIPAL CONGRUENCES

KIRBY A. BAKER AND JU WANG

ABSTRACT. For varieties of algebras, we present the property of having "weakly definable principal congruences" (WDPC), generalizing the concept of having definable principal congruences. It is shown that if a locally finite variety V of finite type has WDPC and its class of subdirectly irreducible members is definable (finitely axiomatizable), then V has a finite equational basis. 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 WDPC. 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 WDPC.

1. INTRODUCTION

We consider only varieties of finite type. Following Baldwin and Berman [3] and McKenzie [9], 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 [6].

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 [9] 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: June 16, 1999.

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 [9] 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 weakly definable principal congruences (WDPC) and showing (Theorem 1) that if V is a locally finite variety of finite type for which the class of subdirectly irreducible members is definable (finitely axiomatizable, absolutely rather than relative to V), 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 WDPC (Theorem 2). The resulting proof of the finite basis theorem [1, 8] for this congruence distributive case avoids dependence on computation with Jónsson terms [7]; cf. [1, 8, 2].

General references for varieties of algebras are [5] and [10].

2. Weakly definable principal congruences

Definition 1. *A variety V has* **weakly definable principal congruences** *(WDPC) 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 [6] sufficient to compute any principal congruence, while the condition for WDPC 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 WDPC.

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 WDPC, but McKenzie [9] 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 WDPC 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].

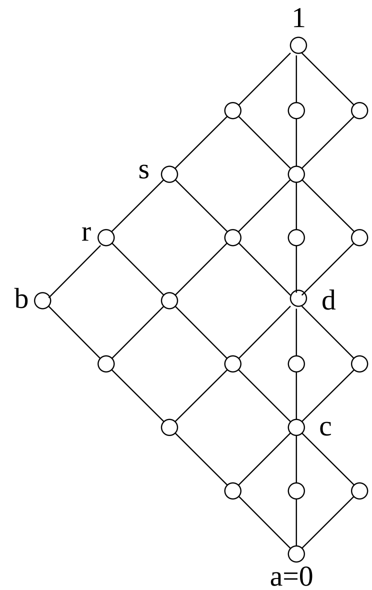

FIGURE 1. The lattice P_4 of McKenzie

Let us say that the class of subdirectly irreducible members of a variety V is *definable* (finitely axiomatizable, strictly elementary) if there is a first-order sentence Ψ in the language of V whose models, among all algebras of the type, are precisely the subdirectly irreducible members of V.

As mentioned, McKenzie [9] 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.

Theorem 1. *If a locally finite variety V has weakly definable principal congruences and its class of subdirectly irreducible members is definable, then V is finitely based.*

Proof: Let Γ_1 and Γ_2 be congruence formulas witnessing WDPC for V. Let $\Phi \equiv (\forall a, b)[a \neq b \rightarrow (\exists c, d)[c \neq d \wedge \Gamma_1(c, d, a, b) \wedge \Pi_{\Gamma_2}(c, d)]]$, a sentence asserting that an individual algebra satisfies the condition for WDPC as witnessed by Γ_1 and Γ_2. By hypothesis, the models of Φ include at least the members of V. Since all laws of V together imply Φ, by compactness there is an integer m such that $V^{(m)} \models \Phi$, where $V^{(m)}$ is the variety determined by all laws of V in at most m variables. Thus $V^{(m)}$ has WDPC.

Also by hypothesis, there is a sentence Ψ whose models are the subdirectly irreducible members of V. Within $V^{(m)}$, subdirectly irreducible algebras, in V or not, can also be characterized by the sentence

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

Thus $V \models \Psi' \rightarrow \Psi$. Again by compactness, there is an integer n such that $V^{(n)} \models \Psi' \rightarrow \Psi$; we may take $n \geq m$. Then $V^{(n)}$ and V have the same subdirectly irreducible members and so are equal. But the laws in at most n variables of a locally finite variety of finite type are finitely based, since a basis can be obtained from the operation tables of the free algebra $F_V(n)$. In other words, V is finitely based. □

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 weakly definable principal congruences.*

The proof depends on this fact about algebras embedded in a product:

Observation 1. *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 [7], $V(A)$ 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 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 $\Gamma_1(c,d,a,b)$ in D and hence in B, and with $\Gamma_2(r,s,c,d)$ in C and hence in B, as required. Thus $V(A)$ has WDPC.

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 additional elements $e_3, \dots, e_{n(j)} \in B$ so that $\pi_j(e_1), \dots, \pi_j(e_{n(j)})$ generate S_j. Let D be the subalgebra of B generated by $a, b, e_3, \dots, e_{n(j)}$. Thus $\pi_j(D) = S_j$.

Since S_j is subdirectly irreducible, $\ker \pi_j$ is completely meet irreducible in $\mathrm{Con}(D)$. By the congruence distributivity of $V(A)$, the interval $[0, \ker \pi_j]$ 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 $\ker \pi_j$. Because $\mathrm{Cg}^D(a, b) \not\leq \ker \pi_j$ 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 $\mathrm{Cg}^D(c, d) \not\leq \ker \pi_i$ and i also splits a, b, so by the minimality of $\mathrm{Cg}^D(c, d)$ we have $\ker \pi_i \leq \ker \pi_j$. Then there is an induced map of $D/\ker \pi_i$ onto $D/\ker \pi_j \cong S_j$. 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 Observation 1 to c, d, r, s and $C \hookrightarrow \prod_{i\in I} S_i$, as follows. If i splits c, d, then $\pi_i(C) = \pi_i(B) = S_i$, 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 $\langle \bar{r}, \bar{s} \rangle \in \mathrm{Cg}^{\pi_i(C)}(\bar{p}, \bar{q}) = 0$. Then Observation 1 applies to show $\langle r, s \rangle \in \mathrm{Cg}^C(c, d)$. $\square$

Note: In the preceding proof, one could economize on generators of D by using only enough elements to generate S_j. Then D and C have respectively at most $g + 2$ and $g + 4$ generators, where g is the maximum of the minimum numbers of generators needed for the various subdirectly irreducible members of $V(A)$.

Corollary 1 ([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 WDPC

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

Proof: We start from the observation that a variety V with WDPC 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 $\mathrm{Cg}^B(r,s) \le \mathrm{Cg}^B(a,b)$ for which $\Gamma(r,s,a,b)$ holds. Indeed, given a, b we can choose c, d as in the definition of WDPC and then an atomic congruence $\mathrm{Cg}(r,s)$ under $\mathrm{Cg}(c,d)$, so that $\Gamma(r,s,c,d)$ 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.

We shall show that $V(S_3)$ does not have definable atomic congruences in finite members. Write $S_3 = \{\iota, c, c^2, b, bc, bc^2\}$, where $c^3 = \iota$, $b^2 = \iota$ and $b^{-1}cb = c^2$. S_3 is the semidirect product of $A_3 = \{\iota, c, c^2\} \lhd S_3$ and $H = \{\iota, b\}$. Let $\langle k \times x\rangle$ mean the concatenated tuple $\langle x, \dots, x\rangle$ (k times), whether x is an element or a tuple itself.

Define groups E_0, E_1, $\dots$ recursively as follows, with $E_n \in S_3^{2^n}$ for each n. Let $E_0 = A_3$. For any $n > 0$, let E_n be the subgroup of $S_3^{2^n}$ generated by the set $\{(\mathbf{e}, \mathbf{e}) \mid \mathbf{e} \in E_n\}$ and the element $\bar{b}_n = \langle 2^{n-1} \times \iota, 2^{n-1} \times b\rangle$. Equivalently, E_n is generated by $\langle 2^n \times c\rangle$ and the n elements $\bar{b}_{n,k} = \langle 2^{n-k} \times b_k\rangle$ for $k = 1, \dots, n$.

The normal subgroup $N(\langle 2^n \times c\rangle)$ of E_n generated by $\langle 2^n \times c\rangle$ is $A_3^{2^n}$, as can be verified by induction using the commutator calculation $\langle 2^{n-1} \times \iota, 2^{n-1} \times c\rangle = [\langle 2^n \times c\rangle, \bar{b}_n] \in N(\langle 2^n \times c\rangle)$. Further, it can be shown that all atomic normal subgroups of E_n are of the form $\{\langle \iota, \dots, \iota, x, \iota, \dots, \iota\rangle \mid x \in A_3\}$. In terms of congruences, we have $\mathrm{Cg}(\langle \iota, \dots, \iota, c, \iota, \dots, \iota\rangle, \langle 2^n \times \iota\rangle) \le \mathrm{Cg}(\langle 2^n \times c\rangle, \langle 2^n \times \iota\rangle)$, but only by a computation involving all generators $\bar{b}_{n,k}$ of E_n; with fewer there will be pairs of coordinates that cannot be distinguished. It follows that there is no suitable congruence formula Γ valid for all E_n simultaneously.

References

[1] K. A. Baker, *Finite equational bases for finite algebras in a congruence-distributive equational class,* Advances in Math. **24** (1997), 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] E. Fried, G. Grätzer, and R. Quackenbush, *Uniform congruence schemes*, Algebra Universalis **10** (1980), 176-188.

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

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

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

[10] 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