Contents lists available at ScienceDirect

Annals of Pure and Applied Logic

journal homepage: www.elsevier.com/locate/apal

Definable principal congruences and solvability

Paweł M. Idziak [a], Keith A. Kearnes [b], Emil W. Kiss [c], Matthew A. Valeriote [d,*]

[a] Theoretical Computer Science Department, Jagiellonian University, ul. Gronostajowa 3, 30-387 Kraków, Poland
[b] Department of Mathematical Sciences, University of Colorado at Boulder, Boulder, CO, 80309-0395, USA
[c] Eötvös University, Department of Algebra and Number Theory, 1117 Budapest, Pázmány Péter sétány 1/c, Hungary
[d] Department of Mathematics and Statistics, McMaster University, Hamilton, Ontario, L8S 4K1, Canada

ARTICLE INFO

Article history:
Received 7 February 2006
Received in revised form 10 September 2008
Accepted 15 September 2008
Available online 25 October 2008
Communicated by A.J. Wilkie

MSC:
08B26
03C40

Keywords:
Definable principal congruences
Tame congruence theory
Twin group
Right- and strongly nilpotent congruence
Abelian variety

ABSTRACT

We prove that in a locally finite variety that has definable principal congruences (DPC), solvable congruences are nilpotent, and strongly solvable congruences are strongly abelian. As a corollary of the arguments we obtain that in a congruence modular variety with DPC, every solvable algebra can be decomposed as a direct product of nilpotent algebras of prime power size.

1. Introduction

A variety $\mathcal{V}$ is said to have Definable Principal Congruences (DPC) if there is a first order formula that defines the principal congruences in all members of $\mathcal{V}$. That is, a formula $\varphi(x, y, u, v)$ exists such that for every $a, b, c, d \in \mathbf{A} \in \mathcal{V}$, we have $c \equiv d\ Cg^{\mathbf{A}}(a, b)$ if and only if, $\varphi(a, b, c, d)$ holds in $\mathbf{A}$. This property ensures that the class of subdirectly irreducible algebras is first order definable in $\mathcal{V}$. Thus, in a variety with DPC either the size of the subdirectly irreducibles can be bounded by a natural number, or there is no cardinal bound at all. The investigation of DPC and residual smallness seems to be related also at the level of the tools used in the arguments ([2] is an early reference). The concept is also related to the question of finite axiomatizability, as shown by McKenzie in [14].

In [14] McKenzie proves that a variety of lattices has DPC if and only if, it is distributive and in [10] Kiss generalizes this by providing a characterization of the finitely generated congruence distributive DPC varieties. Finite groups generating a DPC variety were first studied by Burris and Lawrence [3,4], and were completely described later by Baker in [1]. These varieties all happen to be nilpotent of class at most three. The variety of commutative rings is an important example of a DPC variety. The collection of rings $\mathbb{Z}_{2^n}$ for $n > 0$ in this variety shows that, in general, we cannot restrict the nilpotence degree of congruences under the hypothesis of DPC (as was done for groups), not even in congruence permutable varieties.

[*] Corresponding author.
E-mail addresses: idziak@tcs.uj.edu.pl (P.M. Idziak), kearnes@euclid.colorado.edu (K.A. Kearnes), ewkiss@cs.elte.hu (E.W. Kiss), matt@math.mcmaster.ca (M.A. Valeriote).

0168-0072/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.apal.2008.09.019

A further study of ring varieties with DPC can be found in [3,4,15–18]. These results demonstrate that the property of having DPC is quite restrictive.

In this paper, we investigate solvable congruences and algebras in a DPC variety. We shall see that DPC imposes stronger centrality conditions such as nilpotence, or strong abelianness; this can be considered as a generalization of some of the results mentioned above. The limit of how far such arguments can reach is given by a result in [13], Corollary 4.1, which says that every locally finite abelian variety has DPC. In particular, everything that we prove in this paper holds for locally finite abelian varieties, too, and some of the results are new even in this special case. We summarize our results in the following theorem, so as to make references easier.

Theorem 1.1. *Let* $\mathbf{A}$ *be a finite algebra in a DPC variety.*

(1) *If* β *is a solvable congruence of* $\mathbf{A}$*, then* β *is left and right nilpotent, moreover,* β *centralizes every prime quotient of* $\mathbf{A}$ *below* β *on both sides.*
(2) *If* β *is a strongly solvable congruence of* $\mathbf{A}$*, then* β *is strongly abelian.*
(3) *If* $\mathsf{V}(\mathbf{A})$ *is congruence modular and* $\mathbf{A}$ *is solvable, then* $\mathbf{A}$ *can be decomposed as a direct product of nilpotent algebras of prime power size.*

This result is a summary of Theorems 6.3 and 6.6 and Corollary 9.5. Most of the arguments in the paper serve the proof of these statements, but Example 3.12 may be of independent interest. In the last section, we pose some problems that may show possible directions of further investigations concerning DPC.

The authors wish to acknowledge the hospitable environment of the Fields Institute in Toronto, Canada, where all of them were invited in the fall of 1996, and where the first important steps toward proving the results of the paper were taken.

2. Some machinery

In this section we give references for some tools used in the paper. First of all, the reader is assumed to be fluent in tame congruence theory, and also familiar with the theory of nilpotent algebras. The main references are [5,12,6]. We shall also use the elementary properties of strong and rectangular centrality and strong nilpotence, introduced in [8]. We single out two results that we shall refer to.

Lemma 2.1 (*cf.* [5]*, Lemma 4.27*)**.** *Let* $0 \prec \mu$ *be a minimal congruence of type* **2** *on a finite algebra* $\mathbf{A}$*, and* U *a* $\langle 0, \mu\rangle$*-minimal set. If* β *is a solvable congruence of* $\mathbf{A}$*, then there is no* $(b, t) \in \beta$ *such that* b *is in the body and* t *is in the tail of* U*.*

Theorem 2.2 ([6]*, Theorem 3.5*)**.** *On a finite algebra, every right nilpotent congruence is left nilpotent.*

Next, we define the *characteristic* of a type **2** prime quotient $\langle \alpha, \beta\rangle$ of a finite algebra $\mathbf{A}$. Choose an $\langle \alpha, \beta\rangle$-minimal set U, and an $\langle \alpha, \beta\rangle$-trace N of U. Then, $N/\alpha|_N$ is polynomially equivalent to a vector space over a finite field. Let p denote the characteristic of this field. Since all traces are polynomially isomorphic, p is independent of the trace (and of the minimal set) chosen. This prime number p will be called the characteristic of $\langle \alpha, \beta\rangle$.

Lemma 2.3. *Perspective type* **2** *prime quotients have the same characteristic.*

Proof. It is shown in [5] that perspective quotients have the same minimal sets and the same type. As this type is **2**, Theorem 5.2 of [12] shows that the bodies of these minimal sets are also the same for these quotients. By the results of Section 4 of [5], this body is an E-minimal algebra of type **2**. Thus the structure theorem on E-minimal algebras in [5], Theorem 13.9 (or the fact that the body has an induced Maltsev-operation) implies that the two characteristics are the same. □

The theorem below is not explicitly mentioned in [7], but it can be put together easily, using the arguments there.

Theorem 2.4. *Let* $\mathcal{V}$ *be a congruence modular variety. Suppose that for every finite, nilpotent subdirectly irreducible algebra* $\mathbf{S} \in \mathcal{V}$*, every prime quotient of* $\mathbf{S}$ *has the same characteristic (depending on* $\mathbf{S}$*). Then every finite nilpotent algebra in* $\mathcal{V}$ *is a direct product of nilpotent algebras of prime power size.*

Proof. Let $\mathbf{S} \in \mathcal{V}$ be a finite nilpotent subdirectly irreducible algebra, and denote by p the common characteristic of the prime quotients of $\mathbf{S}$. Lemma 3.1 of [7] and the remarks preceding it show that the cardinality of $\mathbf{S}$ is a power of p. Since in a congruence modular variety, factors of nilpotent algebras are nilpotent, we see that every finite nilpotent algebra in $\mathcal{V}$ is a subdirect product of nilpotent subdirectly irreducible algebras of prime power size. Now, the appropriately modified proof of Theorem 3.11 of [7] gives the statement of the theorem. □

Our final weapon is a translation of DPC to a more algebraic concept, one introduced by Alan Day, and which can be found in Lemma 3 of [10].

Lemma 2.5. *A locally finite variety* $\mathcal{V}$ *satisfies DPC if and only if, there exists a number* K*, depending only on the variety, with the following property: whenever* $a, b, c, d \in \mathbf{A} \in \mathcal{V}$ *and* $c \equiv d\ \mathrm{Cg}^{\mathbf{A}}(a, b)$*, there exists a subalgebra* $\mathbf{B}$ *of* $\mathbf{A}$ *of at most* K *elements that contains* a, b, c, d*, and satisfies that* $c \equiv d\ \mathrm{Cg}^{\mathbf{B}}(a, b)$*.*

We call the smallest such K the *DPC-number* of the variety $\mathcal{V}$. Now let us extend this result to the case of finitely generated congruences. If $\mathbf{a} = (a_1, \ldots, a_m)$ and $\mathbf{b} = (b_1, \ldots, b_m)$, then we shall denote by $Cg(\mathbf{a}, \mathbf{b})$ the congruence generated by all pairs $(a_1, b_1), \ldots, (a_m, b_m)$.

Lemma 2.6. *If a locally finite variety $\mathcal{V}$ has DPC, then for every natural number m there exists an integer K_m such that for every algebra $\mathbf{A} \in \mathcal{V}$, elements $c, d \in A$, and vectors $\mathbf{a}, \mathbf{b} \in A^m$, if $c \equiv d\ Cg^{\mathbf{A}}(\mathbf{a}, \mathbf{b})$, then $\mathbf{A}$ has an at most K_m-element subalgebra $\mathbf{B}$ containing c, d, and all components of $\mathbf{a}$ and $\mathbf{b}$ such that $c \equiv d\ Cg^{\mathbf{B}}(\mathbf{a}, \mathbf{b})$.*

Proof. We induct on m, the case $m = 1$ is established by the previous lemma. So, suppose that the statement is true for $m-1$. Let $\theta = Cg^{\mathbf{A}}(a_m, b_m)$. Then, there exists a subalgebra $\mathbf{C}$ of $\mathbf{A}/\theta$ of at most K_{m-1} elements such that c/θ is congruent to d/θ modulo $Cg^{\mathbf{C}}\{(a_1/\theta, b_1/\theta), \ldots, (a_{m-1}/\theta, b_{m-1}/\theta)\}$.

Consider a Maltsev chain demonstrating this. We can assume that its elements are pairwise different, so there are at most $K_{m-1} - 1$ links in the chain. Pull the constants used in the polynomials in this chain back to $\mathbf{A}$, making sure that we are picking at most one representative from any θ-class. Pull back the Maltsev chain also, using these representatives in the polynomials. Where we had an equality in the chain in $\mathbf{A}/\theta$, we now get a θ-related pair in $\mathbf{A}$. Thus, we get at most K_{m-1} pairs in θ, and these pairs, together with the pairs pulled back from the Maltsev chain, connect c to d. By the previous lemma, to each such θ-related pair (u, v) we can find a subalgebra of at most K_1 elements, where $u \equiv v\ Cg(a_m, b_m)$. Consider the elements of all these subalgebras, the pulled-back constants above, $c, d, a_1, \ldots, a_m$ and $b_1, \ldots, b_m$, and generate a subalgebra $\mathbf{B}$ with all these. Then $c \equiv d\ Cg^{\mathbf{B}}(\mathbf{a}, \mathbf{b})$. The number of generators of $\mathbf{B}$ is at most $K_{m-1}K_1 + K_{m-1} + 2m + 2$, and therefore the size of B is limited by the size of the free algebra in the variety generated by this many elements. The size K_m of this free algebra clearly depends only on the variety $\mathcal{V}$ and the number m, by the induction hypothesis, and we have demonstrated that K_m satisfies the conditions. □

Finally a word about the notation used in the paper. It is mainly standard, that is, the same as in the works cited above. Boldface lowercase letters usually denote vectors (sequences of elements), whose length is determined by the context, and b_i is always the ith component of $\mathbf{b}$ (we have already seen an example of this convention above). If b is some element of a set A, then $\hat{b}$ denotes the constant vector $(b, \ldots, b)$ of appropriate length. Similarly, if p is a function on A, then $\hat{p}$ denotes the function on (sub)powers of A acting componentwise as p. If β is a congruence on an algebra $\mathbf{A}$, then $\beta^{[n]}$ denotes the subalgebra of $\mathbf{A}^n$ consisting of all vectors that run in a β-class, that is, whose components are pairwise β-related.

3. Twin groups

An essential tool of the proofs is the so-called twin group on the traces of the algebras. The scope of this paper does not allow us to give a full introductory treatment. We only give the main definitions, and prove those technical statements that we shall use later in the proofs. The reader is encouraged to browse Section 2 of [9] before reading this paper, which gives an introduction to the concept of the twin group, and reviews the concepts of rectangular and strong centrality as well.

Definition 3.1. Let R be a reflexive, symmetric binary relation of an algebra $\mathbf{A}$, and $\mathbf{c}\ R\ \mathbf{d}$ (this means that the vectors $\mathbf{c}$ and $\mathbf{d}$ of $\mathbf{A}$ are R-related componentwise). If p is a polynomial of $\mathbf{A}$, then the polynomials $f(\mathbf{x}) = p(\mathbf{x}, \mathbf{c})$ and $g(\mathbf{x}) = p(\mathbf{x}, \mathbf{d})$ are called *R-twins.* If the vectors $\mathbf{c}$ and $\mathbf{d}$ are of length 1, then f and g are called *binary* R-twins.

The twin relation is useful in describing polynomials on subpowers of an algebra. In the statements below, $\mathbf{A}$ is always an algebra, E is a nonempty subset of A, and R is a reflexive, symmetric binary relation of A.

Definition 3.2. We denote by $\mathbf{G}(E)$ the group of all unary polynomials of $\mathbf{A}|_E$ that are permutations of E, and by $Tw(E, R)$ the set of all elements of $\mathbf{G}(E)$ that are R-twins of the identity map of E. This is a group under composition, which is called the *R-twin group* on E.

Claim 3.3. *The R-twin relation is a tolerance both on the group $\mathbf{G}(E)$ and on the semigroup $Pol_1(\mathbf{A}|_E)$. The twin group $Tw(E, R)$ is a normal subgroup in $\mathbf{G}(E)$.*

The last statement of the previous claim follows from the fact that every reflexive, compatible relation on a Maltsev algebra (in particular, on a group) is a congruence. The twin group is the normal subgroup obtained form the twin relation this way.

Remark. The set of binary twins of the identity map is not even a subgroup of $\mathbf{G}(E)$, in general. The reader may wonder why, since here we also have compatibility in the following sense. Let $\sim$ denote the binary R-twin relation on $\mathbf{G}(E)$. Then clearly, if $f \sim g$, then $hf \sim hg$ and $fh \sim gh$ for every $h \in \mathbf{G}(E)$. However, to prove that $\sim$ is a tolerance one needs to show that $f \sim g$ and $h \sim k$ imply $fh \sim gk$. This follows from the previous observation only if we assume that $\sim$ is transitive (which is not necessarily the case). On the other hand, the normal R-twin relation (using polynomials of arbitrary arity) is obviously a tolerance, and then we also get transitivity using the Maltsev operation of the group $\mathbf{G}(E)$.

Even though the binary twins do not normally form a subgroup, they do generate the twin group in important cases.

Lemma 3.4. *Let R be a reflexive, symmetric, binary relation on a finite algebra $\mathbf{A}$, and $E = e(A)$, where e is an idempotent unary polynomial of $\mathbf{A}$. Suppose that every binary R-twin of a permutation of E that maps E to E is also a permutation of E. If β is the congruence of $\mathbf{A}$ generated by R, then every β-twin of a permutation of E that maps E to E is also a permutation of E and $Tw(E, R) = Tw(E, \beta)$. Furthermore, the set of binary R-twins of the identity on E that map E to E generates the group $Tw(E, R)$.*

Proof. Suppose that $r(x, \mathbf{c})$ and $r(x, \mathbf{d})$ are polynomials that map E to E such that $\mathbf{c}\ \beta\ \mathbf{d}$ and $r(x, \mathbf{c})$ is the identity map on E. Replacing r by er implies that $r(x, \mathbf{y})$ maps E to E for every $\mathbf{y}\ \beta\ \mathbf{c}$.

We shall prepare a long chain of binary R-twin polynomials that connect $r(x, \mathbf{c})$ and $r(x, \mathbf{d})$. First, change the components of the vector $\mathbf{c}$ to the components of $\mathbf{d}$ one by one. Every such move leads to a pair of binary β-twins. Next, as $(c_i, d_i) \in \beta$, we can connect c_i to d_i by a chain of pairs that are images of pairs in R under a unary polynomial. Substitute this unary polynomial into r at the appropriate coordinate to get a new polynomial. We finally get a chain of binary R-twins between $r(x, \mathbf{c})$ and $r(x, \mathbf{d})$. By our assumption, these are all permutations of E and in particular, $r(x, \mathbf{d})$ is.

Clearly, if two permutations f and g are binary twins, then either of their quotients $g^{-1}f$ and gf^{-1} in the group of permutations is a binary twin of the identity map. Hence, we have shown that every element of $Tw(E, \beta)$ is a product of binary R-twins of the identity map. These binary twins are elements of $Tw(E, R)$, and therefore so is their product, since this is a subgroup. Thus $Tw(E, R) \supseteq Tw(E, \beta)$. The other inclusion is obvious, and so the lemma is proved. □

Of particular interest will be the twin group $Tw(N, R)$, where N is a trace for a minimal congruence. As indicated by the previous lemma, the question will frequently arise: is an R-twin of a permutation a permutation? This question is related to centrality and nilpotence (see Lemma 3.6). We prove an elementary statement first.

Lemma 3.5. *Let U be an $\langle\alpha, \beta\rangle$-minimal set for some congruences $\alpha \prec \beta$ of a finite algebra $\mathbf{A}$, and $N \subseteq U$ an $\langle\alpha, \beta\rangle$-trace.*

(1) *If every R-twin of every element of $\mathbf{G}(U)$ that maps U to U is also a permutation of U, then the analogous statement holds for N.*
(2) *The elements of $Tw(N, R)$ are exactly the restrictions of those elements of $Tw(U, R)$ to N that map N to N.*

Sketch of proof. Let $f(x) = p(x, \mathbf{c})$ and $g(x) = p(x, \mathbf{d})$ be twin unary polynomials of $\mathbf{A}$ such that $f(N) = N$. Replace p by ep for some idempotent unary polynomial e of $\mathbf{A}$ whose range is U, thus ensuring that f and g map A to U. Then $f(\beta)$ is not contained in α, and therefore f is a permutation of U by the minimality of U. The reader can easily infer (1) from this.

Now, suppose in addition that f is the identity map on N and $g(N) = N$. Let h be a polynomial inverse of f on U, and replace p by hp. This does not change the action of f and g on N, but makes sure that the new f is the identity map on U. □

Next, we borrow some ideas from [6] to clear up the relationship between centrality conditions and the behavior of twins and twin groups. To fix terminology, we shall say that a permutation group is *semiregular,* if the stabilizer of every point is trivial. It is *regular* if it is semiregular and transitive. It has been observed in [6] that if β is a right nilpotent congruence on a finite algebra, then the β-twin groups on traces for minimal congruences must be semiregular.

Lemma 3.6. *Suppose that $0 \prec \mu \leq \beta$ are congruences of a finite algebra $\mathbf{A}$. Then exactly one of the following two possibilities hold.*

(1) *For every symmetric, reflexive binary relation R that generates the congruence β, and for every $\langle 0, \mu\rangle$-trace N, the identity map on N has a binary R-twin g that is constant on N. In this case β is not left nilpotent, and if β/μ is left nilpotent, then $g(N) \subseteq N$, and the centralities $\mathbf{C}(\mu, \beta; 0)$, $\mathbf{C}(\beta, \mu; 0)$ (in fact $\mathbf{W}(\mu, \beta; 0)$) fail.*
(2) *For every $\langle 0, \mu\rangle$-minimal set U, every β-twin of every permutation of U mapping U to U is a permutation of U. If we are in this case, then the type of $\langle 0, \mu\rangle$ is $\mathbf{1}$ or $\mathbf{2}$, and the centrality $\mathbf{C}(\mu, \beta; 0)$ fails if and only if $Tw(N, \beta)$ is not semiregular for some (equivalently: every) $\langle 0, \mu\rangle$-trace N. When this non-semiregularity happens, the type of $\langle 0, \mu\rangle$ must be $\mathbf{1}$.*

Proof. Let U be a fixed $\langle 0, \mu\rangle$-minimal set. Suppose that we are not in Case (2) and let R be a binary relation as in Case (1). Then by Lemma 3.4, there is a binary polynomial $p(x, y)$ and $(c, d) \in R$ such that $p(x, c)$ is the identity map on U and $p(x, d)$ is collapsing on U. Note that as all $\langle 0, \mu\rangle$-minimal sets are polynomially isomorphic, then this situation will arise for every such U. This will take us to Case (1).

Since U is the range of an idempotent polynomial, we can assume that the range of p is contained in U. Iterate p in its first variable to obtain a new polynomial, also denoted by $p(x, y)$, that is idempotent for every choice of y, is still the identity map for $y = c$, and is still collapsing for $y = d$. The polynomial $g(x) = p(x, d)$ is then a binary R-twin of the identity map on U and is constant on every $\langle 0, \mu\rangle$-trace contained in U.

We show by induction on n that $p(x, d)\ (\beta]^n\ x$ for every $x \in U$. For $n = 1$ this is true, since $p(x, d)\ \beta\ p(x, c) = x$. Suppose that $p(x, d)\ (\beta]^n\ x$ holds. Then

$$p(p(x, d), d) = p(x, d)$$

implies (by moving d to c) that

$$p(x, d) = p(p(x, d), c)\ [\beta, (\beta]^n]\ p(x, c) = x.$$

Thus, the induction is complete.

If β is left nilpotent, then $(\beta]^n = 0$ for some n, and so the above statement yields that $p(x, d) = x$ for every $x \in U$, which is a contradiction, since $p(x, d)$ is collapsing on U. If β/μ is left nilpotent, we have $(\beta]^n \subseteq \mu$ for some n. Then $p(x, d)\ \mu\ x$, hence $p(N, d) \subseteq N$ for every trace $N \subseteq U$. In this case, let $u \in N$ be the constant value that $p(x, d)$ takes on N and choose some $v \in N$, which is different from u. Then $u = p(u, c) = p(u, d) = p(v, d)$, but $p(v, c) = v \neq u$. Thus all the centralities mentioned above fail, and so we have proved all the statements in Case (1).

Now, assume that we are in Case (2), that is, that every β-twin of every permutation of U that maps U to U is also a permutation of U. First, notice that by the properties of a pseudo-meet operation, the type of $\langle 0, \mu\rangle$ can only be **1** or **2**.

As all $\langle 0, \mu\rangle$-traces are polynomially isomorphic, the fact that $Tw(N, \beta)$ is semiregular or not does not depend on the trace chosen. Suppose that $Tw(N, \beta)$ is not semiregular for some trace N, that is, the identity map $p(x, \mathbf{c})$ of N has a non-identity β-twin $p(x, \mathbf{d})$ that maps N to N and fixes some $a \in N$. Let $b \in N$ be an element that is not fixed by $p(x, \mathbf{d})$. Then $p(a, \mathbf{c}) = a = p(a, \mathbf{d})$, but $b = p(b, \mathbf{c}) \neq p(b, \mathbf{d})$, which is a failure of $\mathbf{C}(\mu, \beta; 0)$. Suppose further that the type of $\langle 0, \mu\rangle$ is **2**. Let $-$ denote the subtraction polynomial operation on N (with respect to some $0 \in N$), and consider the polynomial $p(x, \mathbf{d}) - p(x, \mathbf{c})$. It is a β-twin of the constant zero map $p(x, \mathbf{c}) - p(x, \mathbf{c})$, and as we are in Case (2), $p(x, \mathbf{d}) - p(x, \mathbf{c})$ is also constant on N. Substituting $x = a$ we get that this constant value is zero, hence $p(x, \mathbf{d}) = p(x, \mathbf{c})$ on N, which is a contradiction. Thus, the type of $\langle 0, \mu\rangle$ must be **1**.

To prove the last remaining statement, suppose that $\mathbf{C}(\mu, \beta; 0)$ fails (and we are still in Case (2)). Then there exists a polynomial $p(x, \mathbf{y})$ such that $p(a, \mathbf{c}) = p(a, \mathbf{d})$ but $p(b, \mathbf{c}) \neq p(b, \mathbf{d})$ for some $a \ \mu \ b$ and $\mathbf{c} \ \beta \ \mathbf{d}$. By connecting a to b with a chain of traces we may assume that a and b are contained in a $\langle 0, \mu\rangle$-trace N. Since $p(b, \mathbf{c}) \ \mu - 0 \ p(b, \mathbf{d})$ by the transitivity of μ, we can map this pair nontrivially to N. Let U be the $\langle 0, \mu\rangle$-minimal set containing N. By prefixing p with a suitable idempotent polynomial we can assume that the range of $p(x, \mathbf{y})$ is contained in U. Thus $p(a, \mathbf{c}) = p(a, \mathbf{d}) \in N$, and either $p(a, \mathbf{c}) \neq p(b, \mathbf{c})$ or $p(a, \mathbf{d}) \neq p(b, \mathbf{d})$ (or both); we may assume that the former holds by symmetry. Then $p(x, \mathbf{c})$ is a permutation of U, and by prefixing it with its inverse we may assume that it is the identity map of U. Thus the failure of $\mathbf{C}(\mu, \beta; 0)$ allowed us to construct a β-twin of the identity map on U that has a fixed point $a \in N$ (and which, therefore maps N to N), but which is not the identity map on N. Since we are in Case (2), this is a permutation of U. Therefore $Tw(N, \beta)$ is not semiregular, and the lemma is proved. □

We shall need the following characterization of strongly nilpotent congruences. Contrary to "normal" nilpotence, it makes no difference whether we use strong centrality on the left, or on the right in their definition. For strongly nilpotent congruences, the twin groups are not just semiregular: they are trivial.

Lemma 3.7 *([8], Lemma 3.4). Let β be a congruence of a finite algebra* **A***. Then the following are equivalent.*

(1) *β is strongly nilpotent.*
(2) *For any prime quotient $\langle \delta, \theta\rangle$, any two β-twin polynomials of* **A** *mapping any product $C = C_1 \times \cdots \times C_k$ of θ-classes into U have the property that either they are equal modulo δ on C, or both collapse C into a δ-class.*
(3) *β strongly centralizes every prime quotient of* **A** *on both sides.*
(4) *For every prime quotient $\langle \delta, \theta\rangle$ and each $\langle \delta, \theta\rangle$-trace N, the congruence β weakly centralizes N^2 modulo δ and the β-twin group on N/δ is trivial.*

In particular, homomorphic images of strongly nilpotent congruences are also strongly nilpotent. (This property fails for left and for right nilpotence in general, see [6].) It suffices to check the conditions in parts (2), (3), *and* (4) *for prime quotients below β.*

Now we delve deeper into the group-theoretic aspects of twin groups on traces.

Lemma 3.8 *(cf. [9], Corollary 2.3). Let N be a trace for a minimal congruence on a finite algebra* **A***. Then $\mathbf{G}(N)$, as a permutation group on N, is either primitive, or trivial. If R is a symmetric binary relation on N, then $Tw(N, R)$ is either transitive or trivial.*

Lemma 3.9. *Let* **E** *be an E-minimal algebra of type* **2***. Then, the size of E is a power of some prime p, and the* 1*-twin group on E is a p-group.*

Proof. This statement follows from the structure theorem of E-minimal algebras ([5], Theorem 13.9), or from the proof of Corollary 3.5 in [7]. □

Lemma 3.10. *Let* **G** *be a primitive permutation group on a set N that has a minimal abelian normal subgroup* **K***. Then the order of* **K** *equals p^n for some prime p, and* **K** *acts regularly on N, hence $|N| = p^n$. If* **L** *is a normal p-subgroup of* **G***, then* **L** = **K** *or $|L| = 1$.*

Proof. It is a well-known, elementary fact that a minimal abelian normal subgroup of a finite group is elementary abelian, hence **K** has order p^n. As **G** is primitive, **K** is transitive, and as it is abelian, it is also regular. Hence, the size of N is also p^n.

Next, we recall the well-known fact that the centralizer of **K** in **G** is **K** itself. We prove this for the sake of completeness. Clearly, the centralizer $C_{\mathbf{G}}(\mathbf{K})$ is a normal subgroup of **G** containing **K**. Let **H** be the stabilizer of an $x \in N$, then $\mathbf{G} = \mathbf{HK}$ (as **K** is transitive), and therefore $C_{\mathbf{G}}(\mathbf{K}) = (\mathbf{H} \cap C_{\mathbf{G}}(\mathbf{K}))\mathbf{K}$ by modularity. Let $g \in \mathbf{H} \cap C_{\mathbf{G}}(\mathbf{K})$, then $gk(x) = kg(x) = k(x)$ for every $k \in \mathbf{K}$, so the transitivity of **K** implies that g is the identity map, proving $C_{\mathbf{G}}(\mathbf{K}) = \mathbf{K}$.

Now, suppose that **L** is a nontrivial normal p-subgroup of **G**. The center $Z(\mathbf{L})$ of **L** is characteristic in **L**, hence it is normal in **G**. By the minimality of **K** we have that $Z(\mathbf{L}) \cap \mathbf{K}$ is either **K** or trivial. In both cases, we see that $Z(\mathbf{L})$ centralizes **K**. Then $Z(\mathbf{L}) \leq C_{\mathbf{G}}(\mathbf{K}) = \mathbf{K}$, so the minimality of **K** implies that $Z(\mathbf{L}) = \mathbf{K}$ (since $Z(\mathbf{L})$ is nontrivial). But, **L** centralizes $Z(\mathbf{L}) = \mathbf{K}$, so by $C_{\mathbf{G}}(\mathbf{K}) = \mathbf{K}$ again we get $\mathbf{L} = \mathbf{K}$. □

We take a brief digression by presenting an example of independent interest.

Lemma 3.11 (*cf.* [6], *Theorem 4.20*). *Let R be an abelian reflexive and symmetric binary relation of* $\mathbf{A}$, *and E a finite subset of* $\mathbf{A}$. *Then the R-twin group on E is also abelian.*

Proof. Let $r(x, \mathbf{b})$ and $s(x, \mathbf{d})$ be elements of $Tw(E, R)$ such that $r(x, \mathbf{a})$ and $s(x, \mathbf{c})$ are both the identity map on E for some tuples $\mathbf{a}$ and $\mathbf{c}$ from A with $\mathbf{a}R\mathbf{b}$ and $\mathbf{c}R\mathbf{d}$. Write $r_{\mathbf{y}}$ for the permutation $r(x, \mathbf{y})$, and use a similar notation for s. Consider the group-theoretic commutator $[r_{\mathbf{b}}, s_{\mathbf{d}}]$. This is a polynomial, since the inverse of a permutation on a finite set can be expressed as a power of the permutation. We have

$$[r_{\mathbf{a}}, s_{\mathbf{c}}] = x = [r_{\mathbf{a}}, s_{\mathbf{d}}].$$

Move the parameters $\mathbf{a}$ to $\mathbf{b}$ to obtain

$$x = [r_{\mathbf{b}}, s_{\mathbf{c}}]\ [R, R]\ [r_{\mathbf{b}}, s_{\mathbf{d}}].$$

As R is abelian, we have equality, proving that $r_{\mathbf{b}}s_{\mathbf{d}} = s_{\mathbf{d}}r_{\mathbf{b}}$. □

We show that it is not possible to generalize the above lemma to get that the twin group for a solvable congruence is solvable. The following example presents a two-step right nilpotent finite algebra, where the 1-twin group is a nonabelian simple group, even on a trace for a minimal congruence.

Example 3.12. Let $\mathbf{G}$ be a nonabelian finite simple group and $u \neq v$ some symbols. We define an algebra $\mathbf{A}$ whose underlying set consists of all the pairs (g, u) and (h, v), where $g \in G$ and $1 \neq h \in G$. The algebra has one binary operation $*$, and $|G|$ unary operations. For every $k \in G$ the unary operation f_k maps (g, u) to $(k^{-1}gk, u)$, and maps (h, v) to itself. The binary operation $*$ satisfies that $x * y = x$ with the exception that $(g, u) * (h, v) = (gh, u)$.

It is easy to see that $\mathbf{A}$ is an E-minimal algebra of type $\mathbf{1}$ (see [12], Theorem 4.4). Let μ be the congruence whose only non-singleton block is $N = \{(g, u) \mid g \in G\}$. Then μ is a minimal congruence, and N is a $\langle 0, \mu\rangle$-trace, on which the 1-twin group is isomorphic to $\mathbf{G}$ (the twin permutations of the identity are the right translations of $\mathbf{G}$ given by the polynomials $x * (h, v)$). Note that the size of N is not a prime power. To see that the algebra is right nilpotent, one has to check the centrality $\mathbf{C}(\mu, 1; 0)$. This follows by looking at the congruence Δ on $\mathbf{A}^2$ consisting of the pairs $((a, b), (a, b))$ plus the pairs $(((g, u), (h, u)), ((k, u), (\ell, u)))$ where $gh^{-1} = k\ell^{-1}$.

In a congruence modular variety, the twin group is better behaved, as shown in [7].

4. Two DPC constructions

In this section, starting with a finite algebra $\mathbf{A}$ we present a "DPC" construction. Given a finite algebra $\mathbf{A}$ in a DPC variety we will construct a large subdirect power of $\mathbf{A}$, and then apply the DPC-number of the variety to this subdirect power to derive certain properties of $\mathbf{A}$.

Lemma 4.1. *Let* $\mathbf{A}$ *be a finite algebra,* $\langle\alpha, \beta\rangle$ *a type* $\mathbf{1}$ *prime quotient of* $\mathbf{A}$, *and M an $\langle\alpha, \beta\rangle$-trace. Let n be a natural number and* $\mathbf{B}$ *a subalgebra of* $\mathbf{A}^{n+1}$ *generated by the constant elements of A^{n+1} and some collection of $n + 1$-tuples of the form $(u, \ldots, u, v, u, \ldots, u)$, for some $u, v \in M$ with the v occurring anywhere but the last component.*

Let $L = \log_2(|A|)$ and let $\mathbf{C}$ *be a subalgebra of* $\mathbf{B}$ *of size strictly less than n/L. Then, for some $i < n+1$ we have that $(c_i, c_{n+1}) \in \alpha$ for all $\mathbf{c} \in C$.*

Proof. For $\mathbf{b} \in B$ we have that $\mathbf{b} = \hat{q}(\mathbf{b}^1, \ldots, \mathbf{b}^k)$, for some k-ary polynomial $q(x_1, \ldots, x_k)$ of $\mathbf{A}$ and some non-constant generators $\mathbf{b}^i$, $i \leq k$. Since the type of $\langle\alpha, \beta\rangle$ is $\mathbf{1}$ then the induced algebra on $W = M/\alpha|_M$ is essentially unary and modulo α, q will depend on at most L variables on any product of β-blocks. In particular, $q|_{M^k}$ depends on at most L variables.

By replacing in $\hat{q}$ those $\mathbf{b}^i$ for which $q|_{M^k}$ does not depend on x_i modulo α by some constant from M we obtain an element $\mathbf{b}'$ that, componentwise, is α-related to $\mathbf{b}$. Furthermore, since the generators $\mathbf{b}^i$ are constant except at one coordinate, the element $\mathbf{b}'$ will be constant outside of a set of coordinates $I(\mathbf{b})$ of size at most L and this constant value will be equal to the $n + 1^{\text{st}}$ component of $\mathbf{b}'$. In terms of $\mathbf{b}$ we have that if $i \notin I(\mathbf{b})$ then $(b_i, b_{n+1}) \in \alpha$.

Setting $I = \bigcup\{I(\mathbf{b}) : \mathbf{b} \in C\}$ we have that $|I| \leq |C|L < n$ and so there is some $i < n + 1$ with $i \notin I$. Then, for all $\mathbf{c} \in C$, $(c_i, c_{n+1}) \in \alpha$. □

Corollary 4.2. *Let* $\mathbf{A}$ *be a finite algebra in a DPC variety, and $\alpha \prec \beta$ congruences of* $\mathbf{A}$ *such that the type of $\langle\alpha, \beta\rangle$ is* $\mathbf{1}$. *Suppose that we have a subset U of A, a binary polynomial $r(x, y)$ of* $\mathbf{A}$, *and elements c, d in an $\langle\alpha, \beta\rangle$-trace M such that $r(x, c) = x$ and $s(x) := r(x, d) \in U$ for every $x \in U$. Then the congruence*

$$(u, s(u)) \equiv (v, s(v)) \quad Cg^{\alpha}((u, u), (v, v))$$

holds in the subalgebra of $\mathbf{A}^2$ *with universe α, for any $u, v \in U$.*

Proof. Let K be the DPC number of the variety generated by $\mathbf{A}$ and choose an integer $n > K\log_2(|A|)$. Let $\mathbf{B}$ be the subalgebra of A^{n+1} generated by the constant elements of A^{n+1} along with the elements $\mathbf{b}^i = (c, \ldots, c, d, c, \ldots, c) \in \mathbf{A}^{n+1}$ for $1 \leq i \leq n$, where d occurs at the ith component. When substituting $\mathbf{b}^i$ for y_i, and $\hat{u}$ for x into the polynomial

$$t(x, \mathbf{y}) = r(\ldots r(r(x, y_1), y_2), \ldots, y_n).$$

it is clear that the result will be the element

$$(s(u), s(u), \ldots, s(u), u).$$

Therefore, $(s(u), s(u), \ldots, s(u), u)$ and $(s(v), s(v), \ldots, s(v), v)$ are congruent modulo the principal congruence $Cg^{\mathbf{B}}(\hat{u}, \hat{v})$. By DPC, this congruence relation holds in a subalgebra $\mathbf{C}$ of $\mathbf{B}$ of size at most K. By Lemma 4.1 there is some $i \leq n$ such that the projection of $\mathbf{C}$ down to the pair of coordinates $(i, n+1)$ is contained in the congruence α. The result follows from this. □

Corollary 4.3. *Let $\mathbf{A}$ be a finite algebra in a DPC variety, and $\alpha \prec \beta$ congruences of $\mathbf{A}$ such that the type of $\langle \alpha, \beta \rangle$ is $\mathbf{1}$. Suppose that we have a subset U of A, a ternary polynomial $r(x, y, z)$ of $\mathbf{A}$, elements $a, b \in A$ and c, d in an $\langle \alpha, \beta \rangle$-trace M such that $r(x, c, a) = r(x, d, a) = r(x, c, b) = x$ and $s(x) := r(x, d, b) \in U$ for every $x \in U$. Then the congruence*

$$(u, u) \equiv (u, s(u)) \quad Cg^{\alpha}((a, a), (b, b))$$

holds in the subalgebra of $\mathbf{A}^2$ with universe α, for any $u \in U$.

Proof. The proof of this corollary is a variation of the proof of the previous corollary and so we will only point out the main differences. Consider instead, the polynomial

$$t(x, \mathbf{y}, z) = r(\ldots r(r(x, y_1, z), y_2, z), \ldots, y_n, z)$$

and elements

$$t(\hat{u}, \mathbf{b}^1, \ldots, \mathbf{b}^n, \hat{a}) = (u, u, \ldots, u)$$
$$t(\hat{u}, \mathbf{b}^1, \ldots, \mathbf{b}^n, \hat{b}) = (s(u), s(u), \ldots, u)$$

of $\mathbf{B}$. Note that these two elements are congruent modulo the principal congruence of $\mathbf{B}$ generated by the pair $(\hat{a}, \hat{b})$.

Applying Lemma 4.1 and making use of the DPC number as in the previous proof establishes the result. □

We shall now modify the above arguments to work in the case when the type of $\langle \alpha, \beta \rangle$ is $\mathbf{2}$. Our conclusions will be similar, with the exception that we have to use s^p instead of s, where p is the characteristic of $\langle \alpha, \beta \rangle$.

For the rest of this section, let $\mathbf{A}$ be a finite algebra, $\langle \alpha, \beta \rangle$ a prime quotient of $\mathbf{A}$ of type $\mathbf{2}$, and M an $\langle \alpha, \beta \rangle$-trace. Then, $M/\alpha|_M$ is polynomially equivalent to a one-dimensional vector space $\mathbf{W}$ over a finite field $\mathbf{F}$, no matter how we choose the zero element of $\mathbf{W}$. Let $0, +, -$, and p denote the zero element, addition, the subtraction, and the characteristic of $\mathbf{W}$, respectively.

Fix an integer n, and denote by I the set of all linear maps from $\mathbf{W}^n$ to $\mathbf{W}$. We shall also denote by 0 the constant zero map in I. This I will be our index set, and we shall construct a subalgebra $\mathbf{B} \leq \mathbf{A}^I$. Let $w \in W^n$, and denote by B_w the set of all functions $\mathbf{b} : I \to M$ such that for every $f \in I$ we have $b_f/\alpha = f(w)$ (here, as usual, we denote the fth component of $\mathbf{b}$ as b_f rather than $\mathbf{b}(f)$). Let $\mathbf{B}$ be the subalgebra of $\mathbf{A}^I$ generated by the diagonal, and by the elements from the B_w, where w runs over the entire W^n. Clearly, every non-constant generator of $\mathbf{B}$ is in M^I, and therefore every element of $\mathbf{B}$ runs in a β-class.

The following lemma establishes a property of "small" subalgebras of $\mathbf{B}/\alpha^I$. Note that by regarding $\mathbf{B}/\alpha^I$ as a subalgebra of $(\mathbf{A}/\alpha)^I$ we can regard elements of this algebra as functions from I to $\mathbf{A}/\alpha$.

Lemma 4.4. *Let $\mathbf{C}$ be a subalgebra of $\mathbf{B}/\alpha^I$. Then there exists a subgroup $\mathbf{G}$ of $I = Hom(\mathbf{W}^n, \mathbf{W})$ of index at most $|A|^{|C|}$ such that the partition of I given by the cosets of $\mathbf{G}$ is contained in the kernel of every $\mathbf{c} \in C$, considered as a function from I to $\mathbf{A}/\alpha$.*

Proof. Each set B_w collapses to a single element $\mathbf{b}^w$ in $\mathbf{B}/\alpha^I$, and this element, as a function from I to W is additive, because $\mathbf{b}^w_{f+g} = (f+g)(w) = \mathbf{b}^w_f + \mathbf{b}^w_g$. For $\mathbf{c} \in C$ there is some polynomial $s(x_1, \ldots, x_m)$ of $\mathbf{A}/\alpha$ and tuples $w_i \in W^n$ for $i \leq m$ such that $\mathbf{c} = \hat{s}(\mathbf{b}^{w_1}, \ldots, \mathbf{b}^{w_m})$. So, for $f \in I$ we have that $\mathbf{c}_f = s(f(w_1), \ldots, f(w_m))$.

Since β/α is abelian it follows that

$$\mathbf{c}_{f+g} = s(\ldots, f(w_i) + g(w_i), \ldots) = s(\ldots, f(w_i) + 0, \ldots) = \mathbf{c}_f$$

if and only if,

$$\mathbf{c}_g = s(\ldots, 0 + g(w_i), \ldots) = s(\ldots, 0 + 0, \ldots) = \mathbf{c}_0.$$

That is, the kernel of $\mathbf{c}$ is a coset decomposition modulo some subgroup of I, whose index of course is at most $|A|$. The intersection of these subgroups for all elements of $\mathbf{C}$ then has index at most $|A|^{|C|}$ in I, so we have established the property of the algebra $\mathbf{C}$ stated above. □

Our proofs of the analogs of Corollaries 4.2 and 4.3 hinge partly on the following observation.

Lemma 4.5. *Let p be a prime and $\mathbf{W}$ an elementary abelian p-group. Fix an element $w \in W$. Suppose that $\mathbf{G}$ is a subgroup of $\mathbf{W}^n$ that contains none of the $\binom{n}{p}$ vectors that have p components equal to w, and all other components equal to zero. Then, the index of $\mathbf{G}$ in $\mathbf{W}^n$ is at least $n/(p-1)$.*

Proof. Let e_i be the element of $\mathbf{W}^n$ whose ith component is w, and all other components are zero. If the index of $\mathbf{G}$ is less than $n/(p-1)$, then there must exist a coset modulo $\mathbf{G}$ that contains at least p different elements from $e_1, \ldots, e_n$. The sum of p such elements is in $\mathbf{G}$, because $\mathbf{W}^n/\mathbf{G}$ has exponent p. On the other hand, this sum is a forbidden element of $\mathbf{G}$, proving our assertion. □

Corollary 4.6. *Let $\mathbf{A}$ be a finite algebra in a DPC variety, and $\alpha \prec \beta$ congruences of $\mathbf{A}$ such that the type of $\langle \alpha, \beta \rangle$ is $\mathbf{2}$, and its characteristic is p. Suppose that we have a subset U of A, a binary polynomial $r(x, y)$ of $\mathbf{A}$, and elements c, d in an $\langle \alpha, \beta \rangle$-trace M such that $r(x, c) = x$ and $s(x) := r(x, d) \in U$ for every $x \in U$. Then the congruence*

$$(u, s^p(u)) \equiv (v, s^p(v)) \quad Cg^{\alpha}((u, u), (v, v))$$

holds in the subalgebra of $\mathbf{A}^2$ with universe α, for any $u, v \in U$.

Proof. We may assume that c and d are not α-related (for otherwise s^p is an α-twin of the identity, and the statement is trivial). Let K be the DPC number of the variety generated by $\mathbf{A}$ and let $n > (p-1)|A|^K$. Setting the zero element of the vector space $\mathbf{W}$ induced on $M/\alpha|_M$ by $\mathbf{A}$ to be the element $0 = c/\alpha$, let $\mathbf{B}$ be the subalgebra of $\mathbf{A}^I$ described prior to Lemma 4.4. Let $w = d/\alpha$ and for $i \le n$, let $e_i = (0, \ldots, 0, w, 0, \ldots, 0) \in W^n$, where the w occurs at the ith component. Note that the e_i's form a basis of the vector space $\mathbf{W}^n$ and that the map $f \mapsto (f(e_1), \ldots, f(e_n))$ is a vector space isomorphism between $I = Hom(\mathbf{W}^n, \mathbf{W})$ and $\mathbf{W}^n$.

For each $i \le n$, define $\mathbf{b}^i \in B_{e_i}$ to be any element satisfying that $\mathbf{b}^i_f = d$ whenever $f(e_i) = w = d/\alpha$, and $\mathbf{b}^i_f = c$ whenever $f(e_i) = 0 = c/\alpha$. We are interested in the values of $t(\hat{x}, \mathbf{b}^1, \ldots, \mathbf{b}^n)$ at those coordinates $f \in I$ for which $f(e_i) \in \{w, 0\}$ for every i, where

$$t(x, \mathbf{y}) = r(\ldots r(r(x, y_1), y_2), \ldots, y_n).$$

For such an f, we see that by the definition of $\mathbf{b}^i$ if $f(e_i) = 0$, then $\mathbf{b}^i_f = c$, while if $f(e_i) = w$, then $\mathbf{b}^i_f = d$. As $r(x, c)$ is the identity map, and $r(x, d) = s(x)$ it follows that the fth coordinate of $t(\hat{x}, \mathbf{b}^1, \ldots, \mathbf{b}^n)$ is equal to $s^k(x)$, where k is the number of those i for which $f(e_i) = w$.

In the algebra $\mathbf{B}$, we have that

$$t(\hat{u}, \mathbf{b}^1, \ldots, \mathbf{b}^n) \equiv t(\hat{v}, \mathbf{b}^1, \ldots, \mathbf{b}^n) \quad Cg^{\mathbf{B}}(\hat{u}, \hat{v}).$$

Hence by DPC, we have this congruence in a subalgebra $\mathbf{C}$ of size at most K. By Lemma 4.4 there is a subgroup $\mathbf{G}$ of $I \cong \mathbf{W}^n$ of index at most $|A|^K$ such that all elements of $\mathbf{C}$ are α-constant on the cosets of $\mathbf{G}$. Lemma 4.5 then shows that since $n/(p-1) > |A|^K$ then there is an $f \in \mathbf{G}$ such that f is of the form investigated above, with the number k of nonzero components in f being equal to p. Projecting down our algebra to the index-set $\{f, 0\} \subseteq I$ we get the desired conclusion. □

Corollary 4.7. *Let $\mathbf{A}$ be a finite algebra in a DPC variety, and $\alpha \prec \beta$ congruences of $\mathbf{A}$ such that the type of $\langle \alpha, \beta \rangle$ is $\mathbf{2}$, and its characteristic is p. Suppose that we have a subset U of A, a ternary polynomial $r(x, y, z)$ of $\mathbf{A}$, elements $a, b \in A$ and c, d in an $\langle \alpha, \beta \rangle$-trace M such that $r(x, c, a) = r(x, d, a) = r(x, c, b) = x$ and $s(x) := r(x, d, b) \in U$ for every $x \in U$. Then the congruence*

$$(u, u) \equiv (u, s^p(u)) \quad Cg^{\alpha}((a, a), (b, b))$$

holds in the subalgebra of $\mathbf{A}^2$ with universe α, for any $u \in U$.

Proof. The proof of this corollary is a variation of the proof of the previous corollary and so we will only point out the main differences. Consider instead the polynomial

$$t(x, \mathbf{y}, z) = r(\ldots r(r(x, y_1, z), y_2, z), \ldots, y_n, z)$$

and elements $t(\hat{u}, \mathbf{b}^1, \ldots, \mathbf{b}^n, \hat{a})$ and $t(\hat{u}, \mathbf{b}^1, \ldots, \mathbf{b}^n, \hat{b})$ of $\mathbf{B}$. Note that these two elements are congruent modulo the principal congruence of $\mathbf{B}$ generated by the pair $(\hat{a}, \hat{b})$. Also, for $f \in I$ with $f(e_i) \in \{w, 0\}$ for every $i \le n$ we have that these elements take on values u and $s^k(u)$ respectively at the coordinate f. Applying Lemmas 4.4 and 4.5 as in the previous proof establishes the result. □

5. Homogeneous characteristic

In order to prove in the next section that solvable congruences are right nilpotent in a DPC variety, we show in Lemma 5.2 that certain prime quotients of their algebras must have the same characteristic. First we translate a special case of the conclusions of Corollaries 4.3 and 4.7 in terms of the existence of certain binary twins.

Lemma 5.1. *Suppose that* $\mathbf{A}$ *is a finite algebra,* μ *is a minimal congruence of type* **2***, and* U *is a* $\langle 0, \mu\rangle$*-minimal set whose body is* B*. Let* $a, b \in A$ *such that* $Cg^{\mathbf{A}}(a, b)$ *is solvable, and* θ *a solvable congruence of* $\mathbf{A}$ *generated by a reflexive, symmetric binary relation* R*. Then there exist* $u \neq v \in B$ *such that*

$$(u, u) \equiv (u, v) \quad Cg((a, a), (b, b))$$

holds in the subalgebra of $\mathbf{A}^2$ *whose universe consists of all* θ*-related pairs if and only if there exists a binary polynomial* r *and a pair* $(c, d) \in R$ *such that*

$$u' := r(a, c) = r(a, d) = r(b, c) \neq r(b, d) =: v',$$

and $u', v' \in B$*.*

Proof. Let $\mathbf{C}$ denote the subalgebra of $\mathbf{A}^2$ whose universe consists of all θ-related pairs. If r, c and d above exist, then

$$(u', u') \equiv (u', v') \quad Cg^{\mathbf{C}}((a, a), (b, b))$$

clearly holds. To prove the converse, consider a Maltsev chain between (u, u) and (u, v) given by $Cg^{\mathbf{C}}((a, a), (b, b))$. By prefixing its polynomials with an idempotent polynomial whose range is U, we may assume that the chain goes inside $U \times U$. As the congruence $\beta = Cg^{\mathbf{A}}(a, b)$ is solvable, Lemma 2.1 shows that no β-related pair can cross from the body B to the tail of U. Therefore, the chain is actually in $B \times B$.

A typical link of this chain is a pair

$$((p(a, \mathbf{c}), p(a, \mathbf{d})), (p(b, \mathbf{c}), p(b, \mathbf{d}))),$$

where $\mathbf{c}\ \theta\ \mathbf{d}$. Let $\mathbf{D}$ be the subalgebra of $\mathbf{C}^2$ generated by the diagonal, and the pair $((a, a), (b, b))$. The pair above is a typical element of D. We show that the subset $D \cap B^4$, considered as a binary relation of $\mathbf{C}$, is symmetric and transitive.

Let d be a pseudo-Maltsev operation of U; we know that it is Maltsev on B. Hence, if $(x, y) \in D \cap B^4$ (where $x, y \in C$), then

$$(y, x) = d((x, x), (x, y), (y, y)) \in D \cap B^4,$$

proving symmetry. Similarly, if $(x, y), (y, z) \in D \cap B^4$, then

$$(x, z) = d((x, y), (y, y), (y, z)) \in D \cap B^4,$$

proving transitivity.

Each link in the Maltsev chain above can be considered an element of $D \cap B^4$. Since this relation is symmetric and transitive, the starting point and the endpoint of the chain is also contained in $D \cap B^4$, that is, $((u, u), (u, v)) \in D \cap B^4$. By changing notation we therefore have an appropriate p and $\mathbf{c}\ \theta\ \mathbf{d}$ such that

$$(p(a, \mathbf{c}), p(a, \mathbf{d})) = (u, u) \quad \text{and} \quad (p(b, \mathbf{c}), p(b, \mathbf{d})) = (u, v).$$

Write this as

$$(p(a, \mathbf{c}), p(b, \mathbf{c})) = (u, u) \quad \text{and} \quad (p(a, \mathbf{d}), p(b, \mathbf{d})) = (u, v).$$

Move the components of $\mathbf{c}$ to $\mathbf{d}$ one by one, and for every i connect c_i to d_i by a chain demonstrating that c_i is related to d_i by the congruence generated by R. By linking all these chains together we get a long chain of pairs (not necessarily in $\mathbf{C}$) from (u, u) to (u, v), such that each link in this chain has the form

$$((q(a, c), q(b, c)), (q(a, d), q(b, d))),$$

where q is a binary polynomial, and $(c, d) \in R$. The solvability of θ ensures that this chain is also contained in $B \times B$. Hence, there exists a step when we move out of the diagonal, that is, $q(a, c) = q(b, c)$ but $q(a, d) \neq q(b, d)$. To finish the proof, we use another classical method (described for example in Lemma 2.8 of [12]). Define the binary polynomial

$$r(x, y) = d(q(x, y), q(a, y), q(a, c)).$$

Then $r(a, c) = q(a, c)$, $r(b, c) = q(b, c) = q(a, c)$, and $r(a, d) = q(a, c)$, so we have to prove that $r(b, d)$ is different from these three elements. If not, then

$$d(q(b, d), q(a, d), q(a, c)) = r(b, d) = r(a, d) = d(q(a, d), q(a, d), q(a, c)),$$

and $q(a, d) \neq q(b, d)$ implies that $d(x, q(a, d), q(a, c))$ is not a permutation in x, which contradicts the properties of a pseudo-Maltsev polynomial. □

Lemma 5.2. *Let* $\mathbf{A}$ *be a finite algebra in a DPC variety, and* $0 \prec \mu \leq \alpha \prec \beta$ *congruences of* $\mathbf{A}$ *such that both* $\langle \alpha, \beta \rangle$ *and* $\langle 0, \mu \rangle$ *have type* **2**. *Suppose that* 0 *is meet-irreducible in the interval* $I[0, \beta]$ *and that* β *centralizes every prime quotient below it on the left. Then* $\langle \alpha, \beta \rangle$ *and* $\langle 0, \mu \rangle$ *have the same characteristic.*

Proof. Suppose not, and choose a counterexample that has the interval $I[0, \beta]$ as small as possible. Let p' be the characteristic of $\langle 0, \mu \rangle$ and $p \neq p'$ be the characteristic of $\langle \alpha, \beta \rangle$. We first establish two properties of the interval $I[0, \beta]$: β is join irreducible, and all intervening prime quotients between μ and α have type **1**.

Let β' be a minimal congruence in the interval $I[0, \beta]$ that is not below α. Then β' is a join-irreducible congruence, and thus it has a unique lower cover α'. Clearly, $\langle \alpha', \beta' \rangle$ and $\langle \alpha, \beta \rangle$ are perspective quotients, hence they have the same type and characteristic by Lemma 2.3. As 0 is meet-irreducible below β and the characteristic of $\langle 0, \mu \rangle$ is p' then $\beta' \neq \mu$ and so by the minimality of $I[0, \beta]$ it follows that $\beta' = \beta$ and so β is join irreducible.

Next suppose that there is an intervening prime quotient $\mu \leq \rho \prec \tau \leq \alpha$ of type **2** and choose such a prime quotient with ρ maximal. Note that the maximality of ρ ensures that it is meet irreducible in the interval $I[\rho, \beta]$. The minimality of $I[0, \beta]$ implies that the characteristic of $\langle \rho, \tau \rangle$ is p' and so factoring $\mathbf{A}$ by ρ produces a smaller counterexample. Thus there can be no intervening type **2** prime quotients.

So now we can assume that every prime quotient between μ and α has type **1**. Let U be a $\langle 0, \mu \rangle$-minimal set whose body is B. Let $\mathcal{C}$ be the set of all congruences $\theta \leq \beta$ that satisfy the following property: there exists $(a, b) \in \beta$ and $u \neq v \in B$ such that

$$(u, u) \equiv (u, v) \quad Cg((a, a), (b, b))$$

holds in the subalgebra of $\mathbf{A}^2$ whose universe consists of all θ-related pairs. Since β centralizes all prime quotients below it on the left, we have the centrality $\mathbf{C}(\beta, \mu; 0)$, which shows that $\mu \notin \mathcal{C}$.

Claim 5.3. $\beta \in \mathcal{C}$.

Proof. Let $(a, b) \in \beta - \alpha$ be elements of an $\langle \alpha, \beta \rangle$-trace K. As 0 is meet-irreducible below β, we get that $\mu \leq Cg(a, b)$. Hence, we can connect any two elements in a μ-trace with a Maltsev chain originating from (a, b). Pull this chain into U by an idempotent polynomial. As β is solvable, this chain stays within B by Lemma 2.1. Thus, there is a unary polynomial f such that $f(a)$ and $f(b)$ are different elements of B.

Let m be a pseudo-Maltsev operation on K, and d a pseudo-Maltsev operation on U. Then $f(K) \subseteq B$, hence $r_y(x) := d(x, f(a), f(y))$ is a permutation of B for every $y \in K$. Define $y + z = m(y, a, z)$ on K, and set

$$q(y, z) = r_{y+z} r_z^{-1} r_y^{-1}.$$

This is a polynomial in x that is a permutation of B. Then $q(c, a) = q(a, d) = q(a, a)$ are the identity map on B, whenever $c, d \in K$. So if $c = kb = b + b + \ldots b$ (k summands, the association does not matter), and $d = \ell b = b + \cdots + b$ (ℓ summands), then (a, c) and (a, d) are in $Cg^{\mathbf{A}}(a, b) \leq \beta$. Hence,

$$(q(a, a)(x), q(c, a)(x)) \equiv (q(a, d)(x), q(c, d)(x)) \quad Cg((a, a), (b, b))$$

holds in the subalgebra β of $\mathbf{A}^2$ for every $x \in B$. By evaluating we get for every $x \in B$ that

$$(x, x) \equiv (x, q(c, d)(x)) \quad Cg((a, a), (b, b)).$$

So if $\beta \notin \mathcal{C}$, then we have that $r_{c+d} = r_c r_d$ on B for every such c and d.

Recall that p' denotes the characteristic of $\langle 0, \mu \rangle$, and p denotes the characteristic of $\langle \alpha, \beta \rangle$. The induced algebra on the body of a type **2** minimal set is E-minimal, so Lemma 3.9 shows that $kb = a$, for k some power of p (since $x+b$ is a $K \times K$-twin of the identity map $x + a$ on K). Therefore, r_b raised to the same power is the identity. However, using Lemma 3.9 again we see that the order of r_b is a power of p' (since r_b is a $B \times B$-twin of the identity map r_a on B). Therefore, our assumption that $p \neq p'$ yields that r_b itself is the identity map. That is, $d(x, f(a), f(b)) = x$ for every $x \in U$. This is impossible, since this permutation takes $f(a)$ to $f(b)$. This finishes the proof of the claim. □

Claim 5.4. *Suppose that* $\mu \leq \delta \prec \theta \leq \beta$, *and* $\theta \in \mathcal{C}$. *Then* $\delta \in \mathcal{C}$.

Proof. Let M be a $\langle \delta, \theta \rangle$-trace, and choose the relation R to be $M^2 \cup \delta$. Since $\theta \in \mathcal{C}$ then Lemma 5.1 implies that there exists a binary polynomial q and a pair $(c, d) \in R$ such that

$$u' = q(a, c) = q(a, d) = q(b, c) \neq q(b, d) = v',$$

and $u', v' \in B$. If $(c, d) \in \delta$, then Lemma 5.1 shows that $\delta \in \mathcal{C}$. So we can assume that $c, d \in M$. Let d be a pseudo-Maltsev operation on U, and define

$$r(x, y, z) = d(x, q(z, y), u').$$

Then $r(x, c, a) = r(x, d, a) = r(x, c, b) = x$ holds for every element $x \in U$. Apply either Corollary 4.3 or Corollary 4.7, depending on the type of $\langle \delta, \theta \rangle$, for this quotient. In the type **1** case we get that for every $u \in B$,

$$(u, u) \equiv (u, s(u)) \quad Cg((a, a), (b, b))$$

in the subalgebra δ of $\mathbf{A}^2$, where $s(x) = r(x, d, b) = d(x, q(b, d), u')$. Hence $\delta \in \mathcal{C}$ unless $s(u) = u$ for every $u \in B$. However,

$$s(v') = d(v', q(b, d), u') = d(v', v', u') = u' \neq v'.$$

Hence, $\delta \in \mathcal{C}$ in this case, and so the claim is proved if the type of $\langle \delta, \theta \rangle$ is **1**.

If the type of this quotient is **2**, then of course $\langle \delta, \theta \rangle = \langle \alpha, \beta \rangle$, which has characteristic p. From Corollary 4.7 we get that for every $u \in B$,

$$(u, u) \equiv (u, s^p(u)) \quad Cg((a, a), (b, b))$$

in the subalgebra $\delta = \alpha$ of $\mathbf{A}^2$. Again if $\delta \notin \mathcal{C}$, then s^p is the identity map on B. The fact that $s(v') \neq v'$ shows that s is not the identity map on B, and so s has order p. But s is a $B \times B$-twin of the identity in $\mathbf{A}|_B$, and the twin-group here is a p'-group by Lemma 3.9, so we have $p = p'$, which is a contradiction proving the claim. □

To finish the proof of Lemma 5.2, consider a maximal chain of congruences between μ and α, and use the claim just proved to move down this chain. From $\beta \in \mathcal{C}$ we get that $\mu \in \mathcal{C}$. This final contradiction proves the statement. □

6. Solvability implies right nilpotence

To prove Theorem 6.3, we need two auxiliary lemmas. First we translate the behavior of certain congruences in the square of an algebra to the existence of various twin polynomials.

Lemma 6.1. *Let $0 \prec \mu$ be a congruence of a finite algebra $\mathbf{A}$, and N a $\langle 0, \mu \rangle$-trace. Suppose that $\alpha \geq \mu$ is a congruence of $\mathbf{A}$ such that every α-twin of the identity map on N that maps N to N is also a permutation on N. Let $\mathbf{B}$ be the subalgebra of $\mathbf{A}^2$ whose universe consists of all α-related pairs. Then the following hold.*

(1) *The non-constant unary polynomials of the induced algebra $\mathbf{B}|_{N \times N}$ are exactly pairs of α-twin unary polynomial permutations of N, acting componentwise.*

(2) *Suppose that $u \neq v$, u', v' are elements of N and*

$$(u, u') \equiv (v, v') \quad Cg^{\mathbf{B}}((u, u), (v, v)).$$

Then there exist $f, g \in Tw(N, \alpha)$ such that $f(u) = u'$ and $g(v) = v'$.

(3) *If in addition, $Tw(N, \alpha)$ is semiregular on N, then $f = g$ holds in* (2).

(4) *Let U be a $\langle 0, \mu \rangle$-minimal set and suppose that $u, v, u', v' \in U$ such that $u \ \mu - 0 \ v$ and*

$$(u, u') \equiv (v, v') \quad Cg^{\mathbf{B}}((u, u), (v, v)).$$

If $\mathbf{C}(\mu, \alpha; 0)$ holds, and every α-twin of a permutation on U that maps U to U is also a permutation on U, then there is an $f \in Tw(U, \alpha)$ such that $f(u) = u'$ and $f(v) = v'$.

Proof. The statement in (1) is an easy consequence of the fact that the polynomials of $\mathbf{B}$ are pairs of α-twin polynomials of $\mathbf{A}$ acting componentwise. As $N \times N$ is an E-trace in $\mathbf{B}$, any congruence of $\mathbf{B}$ generated by pairs in $N \times N$ restricts to $N \times N$ to be the same as the congruence generated in the induced algebra $\mathbf{B}|_{N \times N}$. The congruences on this induced algebra are determined by the non-constant unary polynomials, which are the permutations described in (1). Let $\mathbf{G} = \mathbf{G}(N \times N)$ denote this group of permutations of $N \times N$.

Assume the hypotheses of (2). If (u, u) and (v, v) are not in the same $\mathbf{G}$-orbit, then $\mathbf{G}(N)$ is trivial (since $\mathbf{G}(N)$ is either trivial, or transitive on N). In that case $\mathbf{G}$ is trivial, too, hence $u = u'$ and $v = v'$ must hold, and thus (2) and (3) are true in this case. Otherwise, the $\mathbf{G}$-orbit containing (u, u) and (v, v) must also contain (u, u') and (v, v') (since collapsing this orbit and leaving all other elements alone is a congruence of $\mathbf{B}|_{N \times N}$). Thus there is a pair $(f_1, f_2) \in \mathbf{G}$ such that $f_1(u) = u$ and $f_2(u) = u'$. Then $f = f_2 f_1^{-1} \in Tw(N, \alpha)$, which maps u to u', so (2) is proved.

Now assume that $Tw(N, \alpha)$ is semiregular. Then the stabilizer of (u, u) in $\mathbf{G}$ is trivial, hence $\mathbf{G}$ acts regularly on the orbit of (u, u). Let $h(u) = v$ for some $h \in \mathbf{G}(N)$, and let $\mathbf{H}$ be the subgroup of $\mathbf{G}$ generated by (h, h). The $\mathbf{G}$-orbit of (u, u) is in one-to-one correspondence with the elements of $\mathbf{G}$, and the left coset partition modulo $\mathbf{H}$ yields a congruence that collapses (u, u) to (v, v). Therefore, this congruence collapses $(u, u') = (u, f(u))$ to $(v, v') = (v, g(v))$, which means that $(id, f)^{-1}(id, g)$ is an element of H, that is, a power of (h, h). The first component shows that this power is the identity, so $f^{-1}g = id$, too, proving (3).

Finally, assume the conditions in (4). Note that the hypothesis on U implies the hypothesis on N stated at the beginning of this lemma. We show that there is a pair (f', g') of α-twin permutations of U that maps (u, u) to (u, u'). The unary polynomials of $\mathbf{B}|_{U \times U}$ are pairs of α-twin polynomials. Such a polynomial is either a permutation, or both components are collapsing by our assumption. The latter kind collapses (u, u) to (v, v), and is therefore useless in any Maltsev chain originating from this pair. Therefore there exists a pair of α-twin permutations mapping either (u, u) or (v, v) to (u, u'). In the first case we have found (f', g'). In the second case, when (v, v) is mapped to (u, u'), the first component shows that there is a $h \in \mathbf{G}(U)$ mapping v to u. Composing with (h, h) we obtain the desired pair (f', g').

The unary polynomial $f = g'f'^{-1}$ is in $Tw(U, \alpha)$, and $f(u) = u'$. Applying the unary polynomial (id, f^{-1}) to $(u, u') \equiv (v, v')$ we get that (u, u) and $(v, f^{-1}(v'))$ are also congruent modulo $Cg^{\mathbf{B}}((u, u), (v, v))$. The centrality $\mathbf{C}(\mu, \alpha; 0)$ implies that the diagonal of $\mathbf{B}$ is a union of $Cg^{\mathbf{B}}((u, u), (v, v))$-classes. Therefore $v = f^{-1}(v')$, proving the lemma. □

Next, we prove that the R-twin group on a trace cannot increase when we increase the relation R, except under special circumstances. Lemma 3.5 is used implicitly throughout the proof.

Lemma 6.2. *Let $\mathbf{A}$ be a finite algebra in a DPC variety, $0 \prec \mu \leq \alpha \prec \beta$ congruences of $\mathbf{A}$ such that β/α is solvable, and U a $\langle 0, \mu\rangle$-minimal set such that every β-twin of a permutation of U mapping U to U is also a permutation of U. Suppose that N is a $\langle 0, \mu\rangle$-trace in U such that $Tw(N, \alpha)$ is semiregular, and $Tw(N, \beta) \neq Tw(N, \alpha)$. Then the type of $\langle \alpha, \beta\rangle$ must be* **2***. Furthermore, if p denotes the characteristic of $\langle \alpha, \beta\rangle$, then $Tw(N, \alpha)$ cannot be a nontrivial p-group, and if $Tw(N, \alpha)$ is trivial, then $Tw(N, \beta)$ is a regular, elementary abelian p-group, and $|N|$ is a power of p.*

Proof. Let M be an $\langle \alpha, \beta\rangle$-trace, $(a, b) \in M^2 - \alpha$ and $R = \{(a, b), (b, a)\} \cup \alpha$. By Lemma 3.4, every β-twin of the identity map on U that maps U to U can be written as $q(x, b, a, \mathbf{d})$ while $q(x, a, b, \mathbf{c})$ is the identity map on U, for some $\mathbf{c}\ \alpha\ \mathbf{d}$. Let e be an idempotent unary polynomial of $\mathbf{A}$ with $e(A) = U$, and $s(x) = eq(x, b, a, \mathbf{d})$, $r(x) = eq(x, b, b, \mathbf{c})$, $t(x) = eq(x, b, b, \mathbf{d})$. Then, r and st^{-1} are binary R-twins of the identity map on U, witnessed by $(a, b) \in R$, while tr^{-1} is in $Tw(U, \alpha)$.

First, assume that the type of $\langle \alpha, \beta\rangle$ is **1** and apply Corollary 4.2 to this situation. We get that for every $u, v \in U$ the congruence

$$(u, r(u)) \equiv (v, r(v)) \quad Cg((u, u), (v, v))$$

holds in the subalgebra $\mathbf{B}$ of $\mathbf{A}^2$ with universe α. The semiregularity of $Tw(N, \alpha)$ implies $\mathbf{C}(\mu, \alpha; 0)$ by Lemma 3.6, and so if $u\ \mu - 0\ v$, then Lemma 6.1 (4) yields an $f \in Tw(U, \alpha)$ such that $f(u) = r(u)$ and $f(v) = r(v)$.

Now assume that $s(N) = N$, and repeat the above argument for $s(u)$ and $s(v)$ instead of u and v, and for ts^{-1} instead of r. We get a $g \in Tw(U, \alpha)$ such that $g(s(u)) = ts^{-1}(s(u))$ and $g(s(v)) = ts^{-1}(s(v))$. Thus

$$s(u) = g^{-1}t(u) = g^{-1}(tr^{-1})r(u) = g^{-1}(tr^{-1})f(u),$$

and similarly $s(v) = g^{-1}(tr^{-1})f(v)$. However, $h := g^{-1}(tr^{-1})f \in Tw(U, \alpha)$. What we have just shown can be summarized as follows: every $s \in Tw(N, \beta)$ can be interpolated at any two points $u, v \in N$ by an element $h \in Tw(N, \alpha)$.

If $s \in Tw(N, \beta)$ has a fixed point in N, but is not the identity on N, then the same holds for some $h \in Tw(N, \alpha)$ that interpolates s at these two points, which contradicts the semiregularity of $Tw(N, \alpha)$. Therefore $Tw(N, \beta)$ is semiregular on N. So if $s \in Tw(N, \beta)$ is arbitrary, and $u \in N$, then we have $s(u) = h(u)$ for some $h \in Tw(N, \alpha)$ by interpolation, and then semiregularity implies that $s = h$ on N. This gives that $Tw(N, \beta) = Tw(N, \alpha)$, which is a contradiction.

Now let us modify this argument to work in the case, when the type of $\langle \alpha, \beta\rangle$ is **2** of characteristic p. Note that $\mathbf{K} = Tw(U, \alpha)$ is a normal subgroup of $\mathbf{L} = Tw(U, \beta)$. We can decompose every $s \in L$ as a product $s = (st^{-1}r)(r^{-1}t) \in (st^{-1}r)K$. The polynomial $d(x) = st^{-1}r(x)$ is a binary R-twin of the identity map on U and we have that $s^p \in d^pK$ since K is a normal subgroup of L. Using the above argument, and Corollary 4.6 and Lemma 6.1 (4) we see that d^p can be interpolated and hence that s^p can be interpolated at any two μ-related points by an element of $\mathbf{K}$.

Thus if $Tw(N, \alpha)$ is trivial, then s^p must be the identity map on N. Therefore each element of $Tw(N, \beta)$ has order p or 1, and so this is indeed a p-group. Then it is solvable, and is a normal subgroup of $\mathbf{G} = \mathbf{G}(N)$. Therefore any minimal normal subgroup of $\mathbf{G}$ contained in $Tw(N, \beta)$ is an abelian p-group. Lemma 3.10 implies that $|N|$ is a power of p, and as $Tw(N, \beta)$ is a p-group, it equals this minimal, elementary abelian, normal subgroup by the same lemma, hence it is regular.

Now suppose that $Tw(N, \alpha)$ is a nontrivial p-group. By the same argument as in the previous paragraph, applied to $Tw(N, \alpha)$, we get that $|N|$ is a power of p, and $Tw(N, \alpha)$ is a regular, minimal normal subgroup of $\mathbf{G}(N)$. We show that $Tw(N, \beta)$ is a p-group. Indeed, if not, then it has an element s whose order is a prime different from p. Then s^p has the same order, and as $|N|$ is a power of p, this permutation must have a fixed point on N. But this contradicts the two-interpolation property, since $Tw(N, \alpha)$ is semiregular. Thus Lemma 3.10 implies that $Tw(N, \beta) = Tw(N, \alpha)$, again a contradiction. □

Theorem 6.3. *Let $\mathbf{A}$ be a finite algebra in a DPC variety and β a solvable congruence of $\mathbf{A}$. Then β is right nilpotent, moreover it centralizes each prime quotient below it on both sides.*

Proof. We shall prove that if β is solvable, then β centralizes all prime quotients below it on the right. (Every such congruence centralizes all prime quotients below it on the left, too, by Theorem 2.2.) Choose a failure of this property such that the size of the interval $I[0, \beta]$ is minimal. This ensures that we have a finite algebra $\mathbf{A}$ in our variety, and a congruence β of $\mathbf{A}$ having the following properties:

(1) For every congruence $\alpha < \beta$ we have that α centralizes all prime quotients below α on both sides;
(2) β centralizes all prime quotients below it on both sides, except, possibly, those at the bottom (because if not, we could move to a factor of $\mathbf{A}$);
(3) there exists a congruence $0 \prec \mu \leq \beta$ such that $\mathbf{C}(\mu, \beta; 0)$ fails.

Fix a $\langle 0, \mu\rangle$-minimal set U, and a $\langle 0, \mu\rangle$-trace $N \subseteq U$.

We show that we are in Case (2) of Lemma 3.6 for $0 \prec \mu \leq \beta$. Suppose not, and let α be any lower cover of β with $\mu \leq \alpha$ and M an $\langle \alpha, \beta\rangle$-trace. Define the binary relation R to be $M^2 \cup \alpha$. As we are in Case (1), there exists a binary polynomial r and a pair $(c, d) \in R$ such that $r(x, c)$ is the identity map on N, but $s(x) := r(x, d)$ is constant on N, with value $u \in N$. Then $(c, d) \notin \alpha$ since we have $\mathbf{C}(\mu, \alpha; 0)$ by our assumptions above. Therefore $c, d \in M$. Let v be an element of N that is not equal to u. Now apply Corollary 4.2 or Corollary 4.6, depending on the type of $\langle \alpha, \beta\rangle$. Since $s(x) = s^p(x) = u$ for $x \in N$, we get that

$$(u, u) \equiv (v, u) \quad Cg((u, u), (v, v))$$

in the subalgebra α of $\mathbf{A}^2$. This contradicts $\mathbf{C}(\mu, \alpha; 0)$.

Therefore Case (1) of Lemma 3.6 is excluded, and we see by the same lemma that the type of $\langle 0, \mu\rangle$ is **1**. By our assumption that $\mathbf{C}(\mu, \beta; 0)$ fails we get, by this lemma, that $Tw(N, \beta)$ is not semiregular. In particular, it is nontrivial.

Let $\mathcal{T}$ denote the set of all prime quotients $\langle \delta, \theta\rangle$ such that $Tw(N, \delta)$ is trivial, but $Tw(N, \theta)$ is not, where $\mu \le \delta \prec \theta \le \beta$. As the type of $\langle 0, \mu\rangle$ is **1**, the μ-twin group is trivial on N, but the β-twin group is not, and so the set $\mathcal{T}$ is nonempty. By Lemma 3.6 the conditions of Lemma 6.2 are satisfied for every such δ and θ in place of α and β. Lemma 6.2 therefore shows that every quotient in $\mathcal{T}$ has type **2**, and if the characteristic of such a quotient is p, then $|N|$ is a power of p. Since the size of N determines the prime p, we see that all elements of $\mathcal{T}$ have the same characteristic p, and the groups $Tw(N, \theta)$ are all p-groups, acting regularly on N.

We prove that for every $\mu \le \alpha \prec \beta$ the type of $\langle \alpha, \beta\rangle$ is **2** and its characteristic is different from p. Indeed, if there is no $\langle \delta, \theta\rangle \in \mathcal{T}$ such that $\theta \le \alpha$, then $Tw(N, \alpha)$ is trivial. Then Lemma 6.2 shows that $Tw(N, \beta)$ is regular, which is a contradiction. So there is some $\langle \delta, \theta\rangle \in \mathcal{T}$ such that $\theta \le \alpha$. Then $\mathbf{C}(\mu, \alpha; 0)$ implies that $Tw(N, \alpha)$ is semiregular, and as $Tw(N, \theta)$ is regular, these two groups are the same. Thus $Tw(N, \alpha)$ is a nontrivial p-group in this case. Lemma 6.2 implies that indeed the type of $\langle \alpha, \beta\rangle$ is **2** and its characteristic is different from p.

Choose a quotient $\langle \delta, \theta\rangle \in \mathcal{T}$, and push it as high as possible below β. That is, consider a congruence $\delta \le \rho \le \beta$ that is maximal for not being below θ. Then, ρ is meet-irreducible below β, and its unique upper cover τ below β satisfies that $\langle \delta, \theta\rangle$ and $\langle \rho, \tau\rangle$ are perspective, hence they have the same type and characteristic (namely p) by Lemma 2.3. Thus $\tau \ne \beta$ by the statement proved in the previous paragraph. Choose α so that $\tau \le \alpha \prec \beta$. Then $\langle \alpha, \beta\rangle$ has type **2**, and characteristic different from p by the result proved in the previous paragraph. We know that $\rho \ge \mu > 0$, hence β/ρ centralizes all prime quotients below it by our assumptions. Therefore Lemma 5.2 can be applied in the factor $\mathbf{A}/\rho$, and yields that the characteristic of $\langle \rho, \tau\rangle$ is the same as the characteristic of $\langle \alpha, \beta\rangle$. This contradiction proves the theorem. □

Corollary 6.4. *Let* **A** *be a finite algebra in a DPC variety, and* $0 \prec \mu \le \beta$ *congruences of* **A** *such that* β *is solvable. Then* $Tw(N, \beta)$ *is abelian for every* $\langle 0, \mu\rangle$*-trace* N*. If* β *is strongly solvable, then* $Tw(N, \beta)$ *is trivial.*

Proof. The previous theorem ensures that all factors of β are left and right nilpotent. Hence the conditions of Lemma 6.2 are guaranteed by Lemma 3.6. Consider a chain of prime quotients between μ and β, and apply Lemma 6.2 successively, starting at 0. The twin group cannot increase at all at type **1** quotients, and so if β is strongly solvable, then it remains trivial throughout the process. If there are type **2** quotients on the way, then the twin group may become nontrivial at some point. Lemma 6.2 says that in this case it becomes a regular, elementary abelian p-group for some prime p. But it stays regular, because even $Tw(N, \beta)$ is regular by Lemma 3.6. Therefore this twin group can never increase after such a step. □

Corollary 6.5. *Let* **A** *be a finite algebra in a DPC variety. Then every strongly solvable congruence of* **A** *is strongly nilpotent.*

Proof. Let β be a strongly solvable congruence of **A**. By Theorem 6.3, β centralizes each prime quotient below β, and by the previous corollary, the β-twin groups on the traces are trivial. Thus the statement follows from Lemma 3.7. □

Theorem 6.6. *Let* **A** *be a finite solvable algebra in a congruence modular DPC variety. Then* **A** *is nilpotent, and is a direct product of algebras of prime power cardinality.*

Proof. This is clear by Lemma 5.2, Theorems 2.4 and 6.3. □

7. Trivial twins

We shall now start proving that strongly solvable congruences are strongly abelian in a DPC variety. In this section, we discuss a concept that we need in the proof.

Definition 7.1. Let **A** be an algebra, U a subset of **A**, and β, μ congruences of **A**. We say that (U, β, μ) has the *trivial twin property*, if the following holds: any two β-twin polynomials of **A** mapping any product $C = C_1 \times \cdots \times C_k$ of μ-classes into U have the property that either they are equal on C, or both are constant on C.

Lemma 3.7 says that if β is strongly nilpotent and $0 \prec \mu$, then for every $\langle 0, \mu\rangle$-minimal set U the triple (U, β, μ) has the trivial twin property. This property may be lost when we move to a subpower of **A**, for the following reason. Take two β-twin unary polynomials f and g. Then, for every μ-class C, either these are equal on C, or they are both constant on C. This behavior is not necessarily uniform: it can happen that f and g are equal on some μ-class C, but on some other μ-class C' they are different constants. We need to rule out this non-uniform behavior to move up to subpowers.

Definition 7.2. Let **A** be a finite algebra, $0 \prec \mu \le \beta$ congruences of **A** and U a $\langle 0, \mu\rangle$-minimal set. We say that (U, β, μ) has the *strong trivial twin property*, if the following holds: whenever f and g are two binary β-twin unary polynomials mapping A to U that are both the identity map on the body of U, then f and g are equal on any β-class that intersects the body of U.

Lemma 7.3. *Let* **A** *be a finite algebra,* $0 \prec \mu \le \beta$ *congruences of* **A** *such that* β *is strongly nilpotent. Suppose that* (U, β, μ) *satisfies the strong trivial twin property for every* $\langle 0, \mu\rangle$*-minimal set* U*. Then in the subalgebra* $\mathbf{B} := \beta^{[n]} \le \mathbf{A}^n$ *the triple* $(U^n \cap B, \beta^n, \mu^n)$ *has the trivial twin property for every* $\langle 0, \mu\rangle$*-minimal set* U*.*

Proof. Any two β^n-twin polynomials on $\mathbf{B}$ can be written in the following way. Take a polynomial $p(\mathbf{x}, \mathbf{y})$ of $\mathbf{A}$, and $2n$ parameter sequences $\mathbf{u}^i$ and $\mathbf{v}^i$ for $i = 0, 1, \ldots, n$ such that any two of these are β-related componentwise. Then the two twin polynomials are

$$(p(\mathbf{x}, \mathbf{u}^1), \ldots, p(\mathbf{x}, \mathbf{u}^n)) \quad \text{and} \quad (p(\mathbf{x}, \mathbf{v}^1), \ldots, p(\mathbf{x}, \mathbf{v}^n))$$

acting componentwise on $\mathbf{B}$.

Suppose that these two β^n-twin polynomials map some product C' of μ^n-blocks into $U^n \cap B$, are not equal on C', and one of them, say the first one, is not constant on C'. Since U is a minimal set, we can assume that the range of p is contained in U. As these twins are not equal on C', they differ at some element $\mathbf{c}' \in C'$ in some coordinate, say the first coordinate. Let $\mathbf{c}$ denote the sequence of the first coordinates of the vector $\mathbf{c}'$, so

$$p(\mathbf{c}, \mathbf{u}^1) \neq p(\mathbf{c}, \mathbf{v}^1).$$

As the first of these twins is not constant on C', it takes different values on some $\mathbf{d}', \mathbf{e}' \in C'$. Suppose these values differ in the ith coordinate and let $\mathbf{d}$ and $\mathbf{e}$ denote the sequence of ith coordinates of $\mathbf{d}'$ and $\mathbf{e}'$, respectively. Then, $\mathbf{d} \ \mu \ \mathbf{e}$, and

$$p(\mathbf{d}, \mathbf{u}^i) \neq p(\mathbf{e}, \mathbf{u}^i).$$

The sequence of ith coordinates of $\mathbf{c}'$ is β-related to $\mathbf{c}$, because we are in $\beta^{[n]}$, and is μ-related to $\mathbf{d}$ because $\mathbf{c}', \mathbf{d}' \in C'$. Thus $\mu \leq \beta$ implies that $\mathbf{c} \ \beta \ \mathbf{d}$.

Let $C = C_1 \times \cdots \times C_k$ be the product of μ-blocks containing $\mathbf{c}$, and $D = D_1 \times \cdots \times D_k$ the product of μ-blocks containing $\mathbf{d}$ and $\mathbf{e}$. We know that for every j, the μ-classes C_j and D_j are contained in the same β-block and that the triple (U, β, μ) has the trivial twin property by Lemma 3.7. Applying this for the several pairs of twins here we get that $p(\mathbf{x}, \mathbf{u}^1)$ and $p(\mathbf{x}, \mathbf{v}^1)$ are constant on C (since they differ at $\mathbf{c}$), and $p(\mathbf{x}, \mathbf{u}^1)$, $p(\mathbf{x}, \mathbf{u}^i)$, $p(\mathbf{x}, \mathbf{v}^1)$ are equal on D (because $p(\mathbf{x}, \mathbf{u}^i)$ is not constant on D). In particular,

$$p(\mathbf{d}, \mathbf{u}^1) \neq p(\mathbf{e}, \mathbf{u}^1).$$

Moving the components of $\mathbf{d}$ to those of $\mathbf{e}$ one by one will change $p(\mathbf{x}, \mathbf{u}^1)$ at some point. By rearranging the order of the variables of p we may assume that this happens when we move the first component. Therefore, we can rewrite $p(\mathbf{x}, \mathbf{y})$ as $p(x, \mathbf{a}, \mathbf{y})$, where $\mathbf{a} \in D_2 \times \cdots \times D_k$ is fixed, such that $p(x, \mathbf{a}, \mathbf{u}^1)$ is not constant on D_1.

Now, let us see how this rewriting of p affects its behavior on C. Choose any vector $\mathbf{b} \in C_2 \times \cdots \times C_k$ such that $\mathbf{a} \ \beta \ \mathbf{b}$. (This can be done, since C_j and D_j are β-related.) Then the three polynomials

$$p(x, \mathbf{a}, \mathbf{u}^1), \quad p(x, \mathbf{b}, \mathbf{u}^1), \quad p(x, \mathbf{b}, \mathbf{v}^1),$$

are β-twins. The first of these is not constant on D_1 and so by the trivial twin property of (U, β, μ) we see that all three are equal on D_1 (and are not constant). On the other hand, $p(x, \mathbf{b}, \mathbf{u}^1)$ and $p(x, \mathbf{b}, \mathbf{v}^1)$ are different constants on C_1 (since if $x \in C_1$, then $(x, \mathbf{b}) \in C$). Modify p again by writing $p(x, \mathbf{y})$ instead of $p(x, \mathbf{b}, \mathbf{y})$. This new polynomial then satisfies that $p(x, \mathbf{u}^1)$ and $p(x, \mathbf{v}^1)$ are different constants on C_1, while the first one is not constant on D_1.

Since D_1 is connected up by traces, we can choose a $\langle 0, \mu \rangle$-trace M such that $p(x, \mathbf{u}^1)$ is not constant on M. Let V be a $\langle 0, \mu \rangle$-minimal set containing M. Then $p(x, \mathbf{u}^1)$ is a polynomial isomorphism from V to U and so it has a polynomial inverse q that maps U to V. Then, the polynomials $f'(x) = qp(x, \mathbf{u}^1)$ and $g'(x) = qp(x, \mathbf{v}^1)$ are β-twin unary polynomials mapping V to V and which differ at every $c \in C_1$. But C_1 and $M \subseteq D_1$ are in the same β-class and so f' and g' differ on a β-class that intersects the body of V. On the other hand, f' is the identity map on V by its construction.

To make these two β-twin polynomials binary twins, move the components of $\mathbf{u}^1$ to those of $\mathbf{v}^1$ one by one. At some point we must get different values at c. Let such a pair be f and g. But f and g are β-twins of f', which is the identity map on V. The fact that β is strongly nilpotent implies, using the trivial twin property, that f and g are also the identity map on the body of V. Therefore f and g exhibit a failure of the strong trivial twin condition, proving the statement of the lemma. □

Lemma 7.4. *Let $\mathbf{A}$ be a finite algebra, and $\mu \leq \beta$ congruences of $\mathbf{A}$. Suppose that U is the range of an idempotent polynomial of $\mathbf{A}$ such that (U, β, μ) has the trivial twin property. If $\delta \leq \mu$ is any congruence then $(U/\delta, \beta/\delta, \mu/\delta)$ also has the trivial twin property in $\mathbf{A}/\delta$.*

Proof. Consider two twin polynomials in the factor that are not equal on some C. Pull back the parameter sequences arbitrarily to $\mathbf{A}$, and apply an idempotent unary polynomial to make sure that these pulled-back twin polynomials map to U. Then these pulled-back twins cannot be equal on the coimage of C, hence both are constant on this coimage, so the original twins are both constant on C in the factor. □

8. Another DPC construction

The DPC construction used in Section 4 was sensitive to long compositions of polynomials, depending on many parameters. In this section, we present a new construction that has long Maltsev chains which are then reduced to short ones by DPC. We need the following ingredients.

(1) A finite algebra $\mathbf{A}$ in a DPC variety and a subalgebra $\mathbf{D} \leq \mathbf{A}$;
(2) Congruences β and γ of $\mathbf{A}$;
(3) A polynomial $r(\mathbf{x}, \mathbf{y})$ of $\mathbf{D}$ (that is, a term with parameters from D; we are allowed to substitute elements of A into r);
(4) Vectors $\mathbf{a}\ \gamma\ \mathbf{b}$ and $\mathbf{u}\ \beta\ \mathbf{v}\ \beta\ \mathbf{w}$ such that all components of $\mathbf{a}$, $\mathbf{b}$, $\mathbf{u}$ and $\mathbf{w}$ are in D, and $c := r(\mathbf{a}, \mathbf{u}) = r(\mathbf{a}, \mathbf{v})$ and $d := r(\mathbf{b}, \mathbf{v}) = r(\mathbf{b}, \mathbf{w})$ hold.

Notice that $c = r(\mathbf{a}, \mathbf{v})$ and $d = r(\mathbf{b}, \mathbf{v})$ are congruent modulo $Cg^{\mathbf{A}}(\mathbf{a}, \mathbf{b})$, but the parameter sequence $\mathbf{v}$ used to spread this congruence is not assumed to be in $\mathbf{D}$.

Next we shall build a subdirect power of $\mathbf{A}$. For any elements u, v, w consider the following vectors of length $n+2$ having index set $\{0, 1, \ldots, n+1\}$:

$$\begin{aligned}
(w, u, u, u, u, u, \ldots, u, u, u) &= \mathbf{z}^1(u, v, w)\\
(w, v, u, u, u, u, \ldots, u, u, u) &= \mathbf{z}^2(u, v, w)\\
(w, w, u, u, u, u, \ldots, u, u, u) &= \mathbf{z}^3(u, v, w)\\
(w, w, v, u, u, u, \ldots, u, u, u) &= \mathbf{z}^4(u, v, w)\\
(w, w, w, u, u, u, \ldots, u, u, u) &= \mathbf{z}^5(u, v, w)\\
&\cdots\\
(w, w, w, w, w, w, \ldots, w, u, u) &= \mathbf{z}^{2n-1}(u, v, w)\\
(w, w, w, w, w, w, \ldots, w, v, u) &= \mathbf{z}^{2n}(u, v, w)\\
(w, w, w, w, w, w, \ldots, w, w, u) &= \mathbf{z}^{2n+1}(u, v, w).
\end{aligned}$$

These vectors can be described as follows. The 0th component is always w, the $n+1$th component is always u. The components of $\mathbf{z}^{2i+1}$ (where $i = 0, 1, \ldots, n$) are w up to the ith coordinate, and after that they are u. The components of $\mathbf{z}^{2i}$ (where $i = 1, \ldots, n$) are w up to the $i-1$th coordinate, the ith coordinate is v, and after that the coordinates are u.

Let m denote the common length of the vectors $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{w}$ and define $\mathbf{B}$ to be the subalgebra of $\mathbf{A}^{n+2}$ generated by the diagonal of $\mathbf{D}$, and all $(2n+1)m$ elements $\mathbf{z}^i(u_j, v_j, w_j)$, where $i = 1, 2, \ldots, 2n+1$, and the u_j, v_j, w_j run over the components of $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{w}$, respectively. For $i = 1, 2, \ldots, 2n+1$ set

$$\mathbf{z}^i = (\mathbf{z}^i(u_1, v_1, w_1), \mathbf{z}^i(u_2, v_2, w_2), \ldots, \mathbf{z}^i(u_m, v_m, w_m)) \in \mathbf{B}^m$$

The equalities $r(\mathbf{a}, \mathbf{u}) = r(\mathbf{a}, \mathbf{v})$ and $r(\mathbf{b}, \mathbf{v}) = r(\mathbf{b}, \mathbf{w})$ then imply that

$$\hat{r}(\hat{\mathbf{a}}, \mathbf{z}^i) = \hat{r}(\hat{\mathbf{a}}, \mathbf{z}^{i+1})$$

when i is odd, and

$$\hat{r}(\hat{\mathbf{b}}, \mathbf{z}^i) = \hat{r}(\hat{\mathbf{b}}, \mathbf{z}^{i+1})$$

when i is even. (In the above formulas $\hat{\mathbf{a}}$ denotes the sequence whose components are $\hat{a}_i$, and $\hat{\mathbf{b}}$ is meant similarly). Therefore, $\hat{r}(\hat{\mathbf{a}}, \mathbf{z}^1)$ and $\hat{r}(\hat{\mathbf{b}}, \mathbf{z}^{2n+1})$ are congruent modulo $Cg(\hat{\mathbf{a}}, \hat{\mathbf{b}})$ in the algebra $\mathbf{B}$ by transitivity. Of course $\hat{r}(\hat{\mathbf{a}}, \mathbf{z}^1)$ is constant c, with the exception that its 0th coordinate is $r(\mathbf{a}, \mathbf{w})$, and $\hat{r}(\hat{\mathbf{b}}, \mathbf{z}^{2n+1})$ is constant d, with the exception that its $n+1$th coordinate is $r(\mathbf{b}, \mathbf{u})$.

By Lemma 2.6, this congruence holds in a "small" subalgebra $\mathbf{C}$ of $\mathbf{B}$. Note that the elements of $\mathbf{B}$ are of the form $\hat{s}(\ldots, \mathbf{z}^i(u_j, v_j, w_j), \ldots)$, where s is a $(2n+1)m$-ary polynomial of $\mathbf{D}$. Let B_j be the block of β containing u_j, v_j, w_j (for $j = 1, \ldots, m$). Then,

$$\hat{s}(\ldots, \mathbf{z}^i(u_j, v_j, w_j), \ldots)$$

runs in the β-block $s(\ldots, B_j, \ldots)$. We first show in the simplest case how these facts work together.

Corollary 8.1. *If β is strongly abelian, then $c \equiv d$ modulo $Cg(\mathbf{a}, \mathbf{b})$ in $\mathbf{D}$.*

Proof. Consider all the elements of the small subalgebra $\mathbf{C}$ above, and for each $c \in C$ fix a corresponding polynomial s_c as above. As β is strongly abelian, every such s_c depends on at most $L = \log_2(|A|)$ variables on any product of β-blocks. We claim that if n is large enough, then there exists an *even* number ℓ (between 2 and $2n$) such that for each of the polynomials s_c fixed above, s_c restricted to the specific product of β-blocks B_j mentioned above does not depend on any of the m variables where $\mathbf{z}^\ell(u_j, v_j, w_j)$ is written, $j = 1, \ldots, m$.

Indeed, suppose otherwise. Then for every even ℓ there is $c \in C$ such that s_c is "bad", that is, s_c depends on one of its m variables where $\mathbf{z}^i(u_j, v_j, w_j)$ is written (where j can be $1, 2, \ldots, m$). Thus there exists some s_c which must be used at least $n/|C|$ times, and this s_c then must depend on at least $n/|C|$ variables on the above product of β-blocks. Thus, $n \le |C|L$, a contradiction, since $|C|$ is bounded.

Fix such an even ℓ until the end of the argument and consider any element c of $\mathbf{C}$. Replacing $\mathbf{z}^\ell(u_j, v_j, w_j)$ by $\mathbf{z}^{\ell-1}(u_j, v_j, w_j)$ for every $j = 1, \ldots, m$ in the polynomial s_c fixed above does not change the value, c, of the polynomial. The coordinate $\ell/2$ of this element is therefore contained in the subalgebra $\mathbf{D}$, since the $\ell/2$th components of every $\mathbf{z}^i(u_j, v_j, w_j)$ are in D, except for $i = \ell$. Thus projecting down to the coordinate $\ell/2$ we get our assertion. □

The condition that β is strongly abelian is not always satisfied when we want to use this construction. We shall only have that β/μ is strongly abelian for some congruence $\mu \le \beta$. In this case, we shall need additional assumptions.

Corollary 8.2. *Suppose that β/μ is strongly abelian and $\mathbf{u}\ \mu\ \mathbf{w}$. Then*

$$(c, c) \equiv (d, r(b, \mathbf{u})) \quad Cg(\hat{\mathbf{a}}, \hat{\mathbf{b}})$$

holds in the subalgebra μ of $\mathbf{A}^2$ (here ˆ means pairs of course).

Proof. We apply the argument proving Corollary 8.1. We know only that β/μ is strongly abelian, so we have to work in the factor modulo μ. We obtain an even ℓ again, but when we replace $\mathbf{z}^\ell(u_j, v_j, w_j)$ by $\mathbf{z}^{\ell-1}(u_j, v_j, w_j)$ for every $j = 1, \ldots, m$, the elements of $\mathbf{C}$ may change, although every changed element is μ^{n+2}-related to the original one.

Project $\mathbf{C}$ to the coordinates $(\ell/2, n+1)$. The assumption $\mathbf{u}\ \mu\ \mathbf{w}$ implies that the changed elements of $\mathbf{C}$ have μ-related coordinates at these two indices. Since the change moves the components in μ, the same is true for the original elements of $\mathbf{C}$. Therefore we get the desired conclusion. □

Corollary 8.3. *Suppose that β/μ is strongly abelian, and that e is an idempotent unary polynomial of $\mathbf{A}$ with parameters from D such that $U = e(A)$ contains the elements c and d, and (U, γ, μ) has the trivial twin property. Then $c \equiv d$ modulo $Cg(\mathbf{a}, \mathbf{b})$ in $\mathbf{D}$.*

Proof. Apply the same argument as in the first paragraph of the previous proof. The $\ell/2$th coordinates of the changed elements of $\mathbf{C}$ are again contained in the subalgebra $\mathbf{D}$. Consider a Maltsev chain in $\mathbf{C}$ modulo $\hat{\mathbf{a}}$ and $\hat{\mathbf{b}}$ that connects $\hat{r}(\hat{\mathbf{a}}, \mathbf{z}^1)$ to $\hat{r}(\hat{\mathbf{b}}, \mathbf{z}^{2n+1})$. Each link has the form

$$(p(\hat{a}_i, \mathbf{s}^1, \ldots, \mathbf{s}^k), p(\hat{b}_i, \mathbf{s}^1, \ldots, \mathbf{s}^k)),$$

where p is a term, i is between 1 and the length of $\mathbf{a}$, and every $\mathbf{s}^j \in C$. Now, perform the replacement action described above. Then each $\mathbf{s}^j$ changes to some $\mathbf{t}^j$ that is μ-related to $\mathbf{s}^j$ in every coordinate. Project the chain down to the $\ell/2$th coordinate and let s^j and t^j denote the $\ell/2$th coordinate of $\mathbf{s}^j$ and $\mathbf{t}^j$, respectively. Then, $s^j\ \mu\ t^j$ and $t^j \in D$ for every j.

Prefixing p by e, produces a polynomial of $\mathbf{D}$ that pushes the Maltsev chain connecting c to d in the $\ell/2$th coordinate into U. Deleting the trivial links from this Maltsev chain gives us that

$$ep(a_i, s^1, \ldots, s^k) \ne ep(b_i, s^1, \ldots, s^k).$$

As (U, γ, μ) has the trivial twin property, we get that

$$ep(a_i, s^1, \ldots, s^k) = ep(a_i, t^1, \ldots, t^k) \quad \text{and} \quad ep(b_i, s^1, \ldots, s^k) = ep(b_i, t^1, \ldots, t^k).$$

Thus, replacing every s^j with t^j throughout we get a Maltsev chain that has the same elements as before. The parameters are now from $\mathbf{D}$, so we have proved that $c \equiv d$ modulo $Cg(\mathbf{a}, \mathbf{b})$ in $\mathbf{D}$. □

9. Strongly solvable implies strongly abelian

First, we establish the strong trivial twin property in DPC varieties.

Lemma 9.1. *Let $\mathbf{A}$ be a finite algebra in a DPC variety, and $0 \prec \mu \le \gamma$ congruences of $\mathbf{A}$ such that γ is strongly nilpotent, and γ/μ is strongly abelian. Let U be a $\langle 0, \mu\rangle$-minimal set. Then, (U, γ, μ) satisfies the strong trivial twin property.*

Proof. Suppose that this fails. Then there exist two binary γ-twin unary polynomials f and g mapping A to U such that both are the identity map on the body of U, but f and g differ on some γ-class that intersects the body B of U. By prefixing both polynomials with the inverse of f on U, we may assume that f is the identity on U.

Let $f(x) = r(a, x)$ and $g(x) = r(b, x)$, where $a\ \gamma\ b$. Thus $r(a, x) = x = r(b, x)$ for every $x \in B$, but there is an element $v \in A$ such that $u := r(a, v)$ and $w := r(b, v)$ are different elements of U, where $v\ \gamma\ s$ for some $s \in B$. Then, $w = r(b, v)\ \gamma\ r(b, s) = s$, hence $w\ \gamma\ v$. As f is the identity map on U we get that $r(a, w) = w = r(b, v)$. But γ/μ is strongly abelian, so this equality implies that $w = r(a, w)\ \mu\ r(a, v) = u$. Thus u and w are contained in a trace N within U, and therefore both elements are in B. Thus we have the equalities

$$\begin{array}{lll} r(a, u) = u & r(a, v) = u & r(a, w) = w \\ r(b, u) = u & r(b, v) = w & r(b, w) = w. \end{array}$$

We have just set up the conditions of Corollary 8.2, where simply $\mathbf{D} = \mathbf{A}$, $\beta = \gamma$, $c = u$ and $d = w$. As $r(b, u) = u = c$, this corollary shows that

$$(c, c) \equiv (d, c) \quad Cg((a, a), (b, b))$$

holds in the subalgebra μ of $\mathbf{A}^2$. This is a failure of $\mathbf{C}(\gamma, \mu; 0)$, which must hold, since γ is strongly nilpotent. This contradiction proves the lemma. □

To prove that strongly solvable congruences are strongly abelian in a DPC variety, we shall go to a factor of a subalgebra of the cube of a finite algebra, and use the DPC construction. We shall perform an important calculation first in a separate lemma. The motivation for the investigation of the situation below will be apparent later in this section.

Let $\mathbf{C}$ be a finite algebra and $0 \prec \alpha \leq \tau$ congruences of $\mathbf{C}$. Suppose that U is a $\langle 0, \alpha\rangle$-minimal set such that every τ-twin of a permutation of U mapping U to U is also a permutation of U. Let N be an α-trace of U such that $Tw(N, \tau)$ is semiregular. Consider a τ, τ-matrix

$$\begin{bmatrix} t(\mathbf{a}', \mathbf{c}') & t(\mathbf{a}', \mathbf{d}') \\ t(\mathbf{b}', \mathbf{c}') & t(\mathbf{b}', \mathbf{d}') \end{bmatrix} = \begin{bmatrix} z & s \\ x & y \end{bmatrix}$$

such that $x \neq y, x, y \in N$ and $z, s \in U$ such that $z \ \alpha \ s$. Let δ be the congruence of the algebra $\mathbf{T} = \tau^{[3]}$ generated by the pairs

$$(t_1, t_2) = ((s, s, x), (s, z, x)) \quad \text{and} \quad (t_3, t_4) = ((y, x, x), (y, y, y)),$$

and $\mathbf{E}$ the subalgebra consisting of those elements of $\mathbf{T}$ whose first two components are equal.

Lemma 9.2. *Suppose that for every τ, τ-matrix above, the restriction of δ to $U^3 \cap E$ is nontrivial. Then, for every such matrix there exists a permutation $f \in Tw(U, \tau)$ such that $f(x) = z$ and $f(y) = s$.*

Proof. We wish to understand the restriction of δ to U^3. The two generating pairs of δ are in U^3. Consider a Maltsev chain modulo δ connecting two elements of U^3. By applying an idempotent polynomial whose range is U componentwise, we may assume that the entire chain proceeds in U. Thus we may restrict our attention to the induced algebra on U^3.

A unary polynomial of this algebra has the form (p_1, p_2, p_3), where these are τ-twin polynomials mapping $\mathbf{C}$ to U, acting componentwise. By our assumption, the p_i are either all permutations of U, or all collapse α to 0. An inspection of the two generators of δ show that the latter kind of polynomials collapse both generators to 0. Let $\mathbf{G} = \mathbf{G}(U^3)$ be the group of all such triples of polynomial permutations. We have shown that the restriction of δ to U^3 is the same as the G-set congruence of $(U^3, \mathbf{G})$ generated by the two pairs above. That is, we have to apply all elements of $\mathbf{G}$ to these pairs, and take transitive closure.

Claim 9.3. *The congruence ψ generated by (t_3, t_4) restricts trivially to $U^3 \cap E$. In particular, $z \neq s$ must hold for every matrix above.*

Proof. Whatever we said so far about the way to generate δ applies also to ψ. Suppose that the restriction of ψ to $U^3 \cap E$ is nontrivial. Then, there exist two different elements (a, a, b) and (c, c, d) of $U^3 \cap E$ that are congruent modulo ψ. Looking at the generator of ψ we see that ψ-congruent pairs have equal first components. Therefore $a = c$. We also see that $\psi \subseteq \alpha^3$, and so $b \ \alpha \ d$ holds. Thus $b \neq d$ are in a trace within U.

Our first aim is to make sure that we can work in the induced algebra on N. Look at the first link of the chain connecting (a, a, b) to (a, a, d). This yields an element $g = (p_1, p_2, p_3) \in \mathbf{G}$ that maps one of the triples t_3, t_4 to (a, a, b). Apply g^{-1} to the entire chain. Then this new chain will run in N^3, since its starting element is here, and $\psi \subseteq \alpha^3$. If $g^{-1}(a, a, b) = t_3 = (y, x, x)$, then $g^{-1}(a, a, d) = (y, x, x')$, where $x' \in N$, but $x' \neq x$, because $b \neq d$. Similarly, if $g^{-1}(a, a, b) = t_4 = (y, y, y)$, then $g^{-1}(a, a, d) = (y, y, y')$, where $y' \neq y$, and $y' \in N$.

Now, we work in the induced algebra on N^3 to get a contradiction. Let $O \subseteq N^3$ be the set of those triples whose last two components are equal. Clearly, the set O contains t_3 and t_4. We show that O is a union of congruence-classes of ψ restricted to N^3. Indeed, if this is not the case, then there is a unary induced polynomial $g = (p_1, p_2, p_3)$ of N^3 such that $(g(t_3), g(t_4))$ straddles O. But if g maps some element $(u, v, v) \in O$ to O, then $p_2(v) = p_3(v)$, so by the semiregularity of $Tw(N, \tau)$ we get that the τ-twin permutations p_2 and p_3 are equal on N. Therefore g maps O to O, and so O is indeed a union of congruence-classes. But O does not contain (y, x, x') or (y, y, y'). Hence, neither of these two elements can be ψ-congruent to t_3 or to t_4. This proves the first statement of the claim.

To prove the second statement, notice that if $z = s$, then $t_1 = t_2$, and so $\delta = \psi$. Hence δ restricts trivially to $U^3 \cap E$ by what we have just proved, which contradicts our assumptions. □

As $z \neq s$ and these two elements are α-related they are in a trace M. Consider a Maltsev chain coming from the generators of δ that connects two different elements e_1 and e_2 of E. Let $e_1 = (a, a, b)$ and $e_2 = (c, c, d)$. Looking at the generators of δ we see that $\delta \subseteq 0 \times \alpha \times \alpha$. Therefore, $a = c$, and the elements b and d are α-related, but different. Furthermore, the first and second components of any triple in the chain are α-congruent. The claim says that the links in such a chain cannot all come from (t_3, t_4). They cannot all come from (t_1, t_2) either, because in such links the last components of the triples are equal, but $b \neq d$. Thus, the chain has links of both kinds, and so there exist $g_1, g_2 \in G$ such that $\{g_1(t_1), g_1(t_2)\}$ and $\{g_2(t_3), g_2(t_4)\}$ intersect. In other words, there exists some $g = (p_1, p_2, p_3) \in \mathbf{G}$ that takes one of t_1 and t_2 to one of t_3 and t_4. Then $p_3(N) = N$ and $p_1(s) = y$. Hence $p_3^{-1} p_1 \in Tw(U, \tau)$ takes M to N.

First we handle the case, when $Tw(N, \tau)$ is nontrivial. Then by Lemma 3.8 it must be transitive, and as all traces are polynomially isomorphic, the same holds for the twin group on every trace. Therefore M and N are contained in an orbit of $Tw(U, \tau)$. Let f be an element of this group that takes x to z, and h an element that takes z to s. The τ, τ-matrix

$$\begin{bmatrix} h(z) & s \\ h(x) & y \end{bmatrix}$$

also satisfies our conditions, with the only possible exception that the elements in the bottom row may be equal. Indeed, this must be the case by the claim above, since the two elements in the top row are equal. Thus, $h(x) = y$, hence $h(N) = N$. Using the commutator $[h, f] = h^{-1}f^{-1}hf$ as in the proof of Lemma 3.11 we see that

$$\begin{bmatrix} [id, id](x) & [id, f](x) \\ [h, id](x) & [h, f](x) \end{bmatrix} = \begin{bmatrix} x & x \\ x & [h, f](x) \end{bmatrix}$$

is a τ, τ-matrix in U. Here

$$[h, f](x) = h^{-1}f^{-1}hf(x) = h^{-1}f^{-1}(s) \ \alpha \ h^{-1}f^{-1}(z) = h^{-1}(x) \in N.$$

Applying the claim to this matrix we get that $h^{-1}f^{-1}hf(x) = x$, hence $s = hf(x) = fh(x) = f(y)$. Therefore, f satisfies the conditions of the lemma, and we are done in the case, when $Tw(N, \tau)$ is nontrivial.

So, assume that the τ-twin group is trivial on the traces. It follows that any two members of $Tw(U, \tau)$ that both map a given $\langle 0, \alpha\rangle$-trace into the same trace must act identically on the given trace. Then, the $\mathbf{G}$-orbit(s) of t_2 and t_3 do not intersect E. Indeed, if some $(q_1, q_2, q_3) \in \mathbf{G}$ maps t_2 or t_3 to E, then $q_1 = q_2$ on M or N respectively which is impossible since $z \neq s$ and $x \neq y$. Now we can say much more about the Maltsev chain connecting e_1 and e_2 considered above. Namely, it must oscillate between the elements of E and the elements outside E, and so a nontrivial shortest chain connecting two different elements of E must have two links only. That is, it has the form $e'_1 - o - e'_2$, where $e'_1 \neq e'_2$ are in E but o is not. Therefore, now we know that in fact t_2 and t_3 are in the same $\mathbf{G}$-orbit (as o). If $(p_1, p_2, p_3) \in G$ maps t_2 to t_3, and $f = p_2^{-1}p_3$, then $f \in Tw(U, \tau)$, and $f(x) = z$.

We have proved that if $Tw(N, \tau)$ is trivial, then for every matrix in the statement of the lemma, the two elements of the first column are in the same orbit of $Tw(U, \tau)$. Switching columns, we see that the elements of the second column are also in the same orbit. That is, there exists some $g \in Tw(U, \tau)$ such that $g(y) = s$. Now $f^{-1}g$ fixes the trace N, and it is the twin of the identity map on U. We have assumed $Tw(N, \tau)$ to be trivial, which implies that $f^{-1}g$ is the identity map on N. Therefore $f(y) = g(y) = s$, and Lemma 9.2 is proved. □

Lemma 9.4. *Let* $\mathbf{C}$ *be a finite algebra in a DPC variety, and* $0 \prec \alpha \leq \tau$ *congruences of* $\mathbf{C}$ *such that* τ *is strongly nilpotent and* τ/α *is strongly abelian. Suppose that* U *is a* $\langle 0, \alpha\rangle$*-minimal set,* N *is an* α*-trace* $N \subseteq U$*, and*

$$\begin{bmatrix} t(\mathbf{a}', \mathbf{c}') & t(\mathbf{a}', \mathbf{d}') \\ t(\mathbf{b}', \mathbf{c}') & t(\mathbf{b}', \mathbf{d}') \end{bmatrix} = \begin{bmatrix} z & s \\ x & y \end{bmatrix}$$

is a τ, τ*-matrix such that* $x \neq y$*,* $x, y \in N$ *and* $z, s \in U$*. Then* $x = z$ *and* $y = s$*.*

Proof. The fact that τ is strongly nilpotent implies that $Tw(N, \tau)$ is semiregular (in fact trivial), and Lemma 3.6 shows that every τ-twin of a permutation of U mapping U to U is also a permutation of U. As τ/α is abelian, we see that $z \ \alpha \ s$. Therefore the conditions described before Lemma 9.2 hold for every matrix above. We show that δ restricts nontrivially to $U^3 \cap E$ for every such matrix.

Suppose that this is not the case for the matrix above. We shall build up the situation in Corollary 8.3. Let $\mathbf{A} = \mathbf{T}/\delta$, and consider the elements and vectors

$$\mathbf{a} = (\mathbf{a}', \mathbf{a}', \mathbf{b}')/\delta, \quad \mathbf{b} = (\mathbf{b}', \mathbf{b}', \mathbf{b}')/\delta,$$
$$\mathbf{u} = (\mathbf{d}', \mathbf{d}', \mathbf{c}')/\delta, \quad \mathbf{v} = (\mathbf{d}', \mathbf{c}', \mathbf{c}')/\delta, \quad \mathbf{w} = (\mathbf{d}', \mathbf{d}', \mathbf{d}')/\delta$$

of $\mathbf{A}$. By this notation, we mean that, for example $\mathbf{a}$ has the same length as $\mathbf{a}'$, and the ith component of $\mathbf{a}$ is $(a'_i, a'_i, b'_i)/\delta$, where a'_i is the ith component of $\mathbf{a}'$ and b'_i is the ith component of $\mathbf{b}'$. Let $r = \hat{t}/\delta$. Then, we have the equalities

$$c := r(\mathbf{a}, \mathbf{u}) = r(\mathbf{a}, \mathbf{v}) \quad \text{and} \quad d := r(\mathbf{b}, \mathbf{v}) = r(\mathbf{b}, \mathbf{w}).$$

Recall that $\mathbf{E}$ is the subalgebra consisting of those elements of $\mathbf{T}$ whose first two components are equal and let $\mathbf{D} = \mathbf{E}/\delta$. Clearly, D contains the elements c, d, and all the components of the vectors $\mathbf{a}$, $\mathbf{b}$, $\mathbf{u}$ and $\mathbf{w}$. Set $\beta = \gamma = \tau^3/\delta$ and $\mu = \alpha^3/\delta$. Lemmas 7.3 and 9.1 imply that $(U^3 \cap T, \tau^3, \alpha^3)$ has the trivial twin property, hence by Lemma 7.4 the triple $((U^3 \cap T)/\delta, \beta, \mu)$ has it, too. We have set up the conditions of Corollary 8.3 in $\mathbf{A}$, so we get that (s, s, x) and (y, y, y) are congruent modulo $\delta|_E \vee Cg^{\mathbf{E}}((\mathbf{a}', \mathbf{a}', \mathbf{b}'), (\mathbf{b}', \mathbf{b}', \mathbf{b}'))$. Pull a Maltsev chain witnessing this into U^3 by applying a suitable idempotent polynomial componentwise. We have assumed that δ restricts trivially to $U^3 \cap E$ and therefore (s, s, x) and (y, y, y) are congruent modulo $Cg^{\mathbf{E}}((\mathbf{a}', \mathbf{a}', \mathbf{b}'), (\mathbf{b}', \mathbf{b}', \mathbf{b}'))$. But this is a contradiction, because the last components of the two triples (a'_i, a'_i, b'_i) and (b'_i, b'_i, b'_i) are equal for every i, but the last components of the two triples (s, s, x) and (y, y, y) are not. This contradiction proves that δ restricts nontrivially to $U^3 \cap E$.

We can now apply Lemma 9.2 to see that there exists an $f \in Tw(U, \tau)$ such that $f(x) = z$ and $f(y) = s$. In particular, $x \ \tau \ z$. Now $f(x) = id(z)$, so the fact that τ/α is strongly abelian implies that $f(x) \ \alpha \ id(x)$. Thus $z \in N$, and f maps N to N. But, $Tw(N, \tau)$ is trivial, so f is the identity map on N, proving that $x = z$ and $y = s$. □

Corollary 9.5. *In a DPC variety, every strongly solvable congruence on every finite algebra is strongly abelian.*

Proof. Let $\mathbf{C}$ be a finite algebra in a DPC variety, and τ a strongly solvable congruence of $\mathbf{C}$. Then τ is strongly nilpotent by Corollary 6.5. Suppose that τ is not strongly abelian. By taking a suitable quotient, we may assume that $\mathbf{C}$ is subdirectly irreducible with monolith α and that τ/α is strongly abelian.

We shall set up the conditions of Lemma 9.4. As τ is not strongly abelian, there exists a polynomial t such that $t(a, \mathbf{c}) = t(b, \mathbf{d})$ for some $a \; \tau \; b$ and $\mathbf{c} \; \tau \; \mathbf{d}$, but $t(e, \mathbf{c}) \neq t(e, \mathbf{d})$ for some $e \; \tau \; a$. If $t(b, \mathbf{c}) \neq t(b, \mathbf{d})$, then consider the τ, τ-matrix

$$\begin{bmatrix} t(a, \mathbf{c}) & t(a, \mathbf{d}) \\ t(b, \mathbf{c}) & t(b, \mathbf{d}) \end{bmatrix} = \begin{bmatrix} z & s \\ x & y \end{bmatrix},$$

and if $t(b, \mathbf{c}) = t(b, \mathbf{d})$, then consider

$$\begin{bmatrix} t(b, \mathbf{c}) & t(b, \mathbf{d}) \\ t(e, \mathbf{c}) & t(e, \mathbf{d}) \end{bmatrix} = \begin{bmatrix} z & s \\ x & y \end{bmatrix}.$$

The fact that τ/α is strongly abelian implies that $x \; \alpha \; y$. Hence we can push this pair nontrivially into a $\langle 0, \alpha \rangle$-trace N, and make t map into the corresponding minimal set U. Lemma 9.4 shows that $x = z$ and $y = s$. In the second matrix this is impossible, because here $z = s$ (but $x \neq y$). In the first matrix this is impossible, too, because in that one $z = y$. This contradiction proves the corollary. □

10. Five problems

The main question would be to ask for a complete characterization of finite algebras generating a DPC variety, as has been done for groups in [1]. That result can be reformulated to say that a finite group generates a DPC variety if and only if, every principal congruence is abelian. In a group, a principal congruence is always generated by a pair $(g, 1)$, and of course the subgroup generated by g is always abelian. Therefore, this result hints that DPC may imply a kind of "commutator extension property", as does its special case, the congruence extension property in modular varieties (see [11]). The results in Section 8 may also point in this direction.

Problem 10.1. Is it possible to find a condition that is satisfied in every finite algebra generating a DPC variety, and which implies, in the case of groups, that every principal congruence is abelian?

It would be interesting to solve the above problem even in the special case, when we assume modularity and/or solvability. At the moment, we do not understand fully how DPC can be spoiled for solvable congruences. In case of strong solvability, strong abelianness is a complete characterization. Hence, the problem is with the presence of type **2** quotients, because we cannot force solvable congruences to be abelian. Is it true that in the solvable case, non-DPC is always caused by the interaction of two type **2** quotients? This question may seem a bit vague, so we try to make it more concrete, as follows.

Problem 10.2. Let $\mathbf{A}$ be a finite algebra in a DPC variety, and $\rho \leq \tau$ congruences of $\mathbf{A}$ such that τ is solvable and ρ is strongly solvable. Does it follow that τ strongly centralizes ρ on both sides? If $\psi \prec \theta \leq \rho$ and M is a $\langle \psi, \theta \rangle$-trace is $Tw(M/\psi, \tau/\psi)$ trivial?

Problem 10.3. Let $\mathbf{A}$ be a finite algebra in a DPC variety, and $\tau \geq \rho \geq \psi$ congruences of $\mathbf{A}$. Suppose that ρ/ψ is abelian and τ/ρ and ψ are strongly abelian. Does it follow that τ is abelian?

Some concrete examples indicate that Lemma 9.2 (which may be general enough in its present form), and a type **2** variant of the construction in Section 8 could help to attack this problem.

A related question may be to investigate β-twin groups on subsets bigger than traces, where β is a solvable congruence.

Problem 10.4. Let $\mathbf{A}$ be a finite algebra in a DPC variety, and β a solvable congruence of $\mathbf{A}$. What can we say about the β-twin group on larger subsets of $\mathbf{A}$? How is it related to translations on type **2** traces? Is it nilpotent?

With respect to this problem, we call the attention of the reader to the proof of Lemma 5.2, where we show that polynomials mapping between type **2** traces must be homomorphisms under certain circumstances. The methods in [7] could also serve as models to work on this question, since in that paper the twin group on the entire algebra is described in the modular case.

The problem of characterizing DPC is almost completely open if we leave solvability, although the first author has some results in this direction, which are not published yet. Even the result in [10], characterizing DPC in the congruence distributive case, is a bit complicated.

Problem 10.5. Investigate DPC, using tame congruence theory, in the non-solvable case. Is it possible to simplify the main result of [10]?

Acknowledgements

The work was supported by the Polish MNiI, the Hungarian National Foundation for Scientific Research (OTKA), grants no. T043671 and T043034 and the NSERC of Canada.

References

[1] K.A. Baker, Definable normal closures in locally finite varieties of groups, Houston J. Math. 7 (4) (1981) 467–471.

[2] J. Baldwin, J. Berman, The number of subdirectly irreducible algebras in a variety, Algebra Universalis 5 (1975) 379–389.

[3] S. Burris, J. Lawrence, Definable principal congruences in varieties of groups and rings, Algebra Universalis 9 (2) (1979) 152–164.

[4] S. Burris, J. Lawrence, A correction to: Definable principal congruences in varieties of groups and rings [Algebra Universalis 9(2) (1979) 152–164; MR 80c:08004], Algebra Universalis 13 (2) (1981) 264–267.

[5] D. Hobby, R. McKenzie, The Structure of Finite Algebras, in: Contemporary Mathematics, vol. 76, American Mathematical Society, 1988, (revised edition 1996).

[6] K.A. Kearnes, An order-theoretic property of the commutator, Internat. J. Algebra Comput. 3 (1993) 491–534.

[7] K.A. Kearnes, Congruence modular varieties with small free spectra, Algebra Universalis 42 (3) (1999) 165–181.

[8] K.A. Kearnes, E.W. Kiss, Finite algebras of finite complexity, Discrete Math. 207 (1–3) (1999) 89–135.

[9] K.A. Kearnes, E.W. Kiss, Residual smallness and weak centrality, Internat. J. Algebra Comput. 13 (2003) 35–59.

[10] E.W. Kiss, Definable principal congruences in congruence distributive varieties, Algebra Universalis 21 (1985) 213–224.

[11] E.W. Kiss, Injectivity and related concepts in modular varieties. II. The congruence extension property, Bull. Austral. Math. Soc. 32 (1) (1985) 45–53.

[12] E.W. Kiss, An easy way to minimal algebras, Internat. J. Algebra Comput. 7 (1997) 55–75.

[13] E.W. Kiss, M.A. Valeriote, Abelian algebras and the Hamiltonian property, J. Pure Appl. Algebra 87 (1993) 37–49.

[14] R. McKenzie, Para primal varieties: A study of finite axiomatizability and definable principal congruences in locally finite varieties, Algebra Universalis 8 (3) (1978) 336–348.

[15] G.E. Simons, Varieties of rings with definable principal congruences, Proc. Amer. Math. Soc. 87 (1983) 397–402.

[16] G.E. Simons, Definable principal congruences and *R*-stable identities, Proc. Amer. Math. Soc. 97 (1986) 11–15.

[17] G.E. Simons, The structure of rings in some varieties with definable principal congruences, Trans. Amer. Math. Soc. 331 (1992) 165–179.

[18] G.E. Simons, Finite rings in varieties with definable principal congruences, Proc. Amer. Math. Soc. 121 (1994) 649–655.