Few subpowers, congruence distributivity and near-unanimity terms

Petar Marković and Ralph McKenzie

Abstract. We prove that for any variety $\mathcal{V}$, the existence of an edge-term (defined in [1]) and Jónsson terms is equivalent to the existence of a near-unanimity term. We also characterize the idempotent Maltsev conditions which are defined by a system of linear absorption equations and which imply congruence distributivity.

1. Introduction and notation

This note is about a very special kind of Maltsev condition that a variety $\mathcal{V}$ may satisfy, namely the existence of a term $t(x_1, \ldots, x_m)$ satisfying in $\mathcal{V}$ a system of equations ε_i, $1 \leq i \leq n$ in two variables x and y, where ε_i is

$$t(\mathbf{a}_1(i), \ldots, \mathbf{a}_m(i)) \approx x$$

and each $\mathbf{a}_j(i) \in \{x, y\}$. Each Maltsev condition of this kind is specified by an $n \times m$ matrix $(\mathbf{a}_j(i))$ of x's and y's, or by a sequence $\mathbf{a}_1, \ldots, \mathbf{a}_m$ of members of $\{x, y\}^n$ (the columns of the matrix). It is easy to see that this Maltsev condition is non-trivial—i.e., is not satisfied by the variety of sets—precisely in case $\mathbf{a}_j \in \{x, y\}^n - \{x\}^n$ for $1 \leq j \leq m$.

Two classical examples of Maltsev conditions of this kind are A. Maltsev's original condition, expressed in the equations $t(x, y, y) \approx x$ and $t(y, y, x) \approx x$; and the existence of an m-ary near-unanimity term, expressed in the system of equations $t(x, \ldots, x, y, x \ldots x) \approx x$ (where the lone y takes each of the m possible positions). A term t obeying any non-empty system of equations of the kind we are considering, over a variety $\mathcal{V}$, is *idempotent* over $\mathcal{V}$, by which we mean that it obeys the equation $t(x, \ldots, x) \approx x$ over $\mathcal{V}$. The equations $\sigma \approx \tau$ we are considering are linear absorption equations, meaning that τ is a variable x (any variable occuring in σ is "absorbed" into x), and neither σ nor τ contains an explicit composition of operations (they are "linear" terms).

A Maltsev condition given by a set Σ of equations is called *idempotent* iff for each operation symbol f appearing in Σ, the equation $f(x, \ldots, x) \approx x$ is implied by Σ. We believe it is an interesting open question whether every variety that satisfies some non-trivial idempotent Maltsev condition consisting of absorption equations

---

Date: August, 2006.

The first author was supported by the grant no. 144011G of the Ministry of Science and Environment of Serbia. The work of the second author was supported by US NSF grant no. DMS 0245622.

must satisfy a non-trivial Maltsev condition of the kind we consider here, namely a condition defined by finitely many linear absorption equations in two variables and one operation symbol.

This kind of Maltsev condition has already been considered at length in [1] where a variety satisfying a non-trivial such condition is said to have a "cube term". The following definition comes from that paper.

Definition 1.1. Let $\Gamma = \{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ be a non-void subset of $\{x,y\}^n - \{x\}^n$. For a variety $\mathcal{V}$, and a $\mathcal{V}$-term $t = t(x_1, \ldots, x_m)$, we say that t is a Γ-*special cube term* for $\mathcal{V}$ if t satisfies in $\mathcal{V}$ the equations ε_i, $1 \leq i \leq n$, where ε_i is

$$t(\mathbf{a}_1(i), \ldots, \mathbf{a}_m(i)) \approx x.$$

When $\Gamma = \{x,y\}^n - \{x\}^n$, we call such a term just an *(n-dimensional) cube term* for $\mathcal{V}$. When Γ consists precisely of all the vectors in $\{x,y\}^n - \{x\}^n$ which have one value equal to y and one more vector which is equal to y at the first two positions and to x elsewhere, this is called an *(n-dimensional) edge term* for $\mathcal{V}$. Finally, when Γ consists exactly of all the vectors in $\{x,y\}^n - \{x\}^n$ which have one value equal to y, this is just a near-unanimity term. We will call the equations ε_i the *defining equations* of the term t.

We note that when $\emptyset \neq \Gamma \subseteq \Gamma' \subseteq \{x,y\}^n - \{x\}^n$, every variety with a Γ-special cube term t also has a Γ'-special cube term t'. (One can construct t' by adding "dummy variables" to t.) Thus every variety that has a Γ-special cube term, where $\Gamma \subseteq \{x,y\}^n - \{x\}^n$, has also an n-dimensional cube term.

In the paper [1] it was proved that $\mathcal{V}$ has an n-dimensional edge term iff it has an n-dimensional cube term. Thus, if $\mathcal{V}$ has a Γ-special cube term for some Γ, then it has a cube term and an edge term of the same dimension. When $\mathcal{V} = \mathcal{V}(\mathbf{A})$ for some finite algebra $\mathbf{A}$, the condition to have a cube term was proved in [1] to be equivalent to $\mathcal{V}$ having few subpowers (the logarithm of the number of subuniverses of $\mathbf{A}^n$ is bounded from above by a polynomial in n and $|A|$). The same paper contains a proof that a congruence distributive variety $\mathcal{V}$ has an n-dimensional edge term iff it has an n-ary near-unanimity term.

It is our purpose in this note to present an alternative proof of the same fact (without the precise dimension), with several other equivalent conditions proved. We believe this alternative proof is interesting and contains some novel ideas that might be useful elsewhere.

Now we need a few technical definitions:

Definition 1.2. Let $\Gamma = \{\mathbf{a}_1, \ldots, \mathbf{a}_m\} \subseteq \{x,y\}^n - \{x\}^n$. We define a matrix $M(\Gamma)$ with n rows and m columns to be $M(\Gamma)(i,j) = 0$ when $\mathbf{a}_j(i) = x$ and $M(\Gamma)(i,j) = 1$ when $\mathbf{a}_j(i) = y$.

Definition 1.3. Let Γ be as above. We say that Γ satisfies the *divisibility property* when

(1) there exists a linear combination of rows of $M(\Gamma)$ with integer coefficients which is equal in $\mathbf{Z}^m$ to a constant row of k, where k is a positive integer and

(2) for each prime divisor p of k there exists a linear combination of rows of $M(\Gamma)$ with positive integer coefficients such that each entry in the resulting row (in $\mathbf{Z}^m$) is congruent to 1 modulo p.

Definition 1.4. [5] Let S be a subset of A^κ. We say S is *totally symmetric* if for any $\mathbf{a} \in S$ and any permutation $\pi \in Sym(\kappa)$, we have that $\mathbf{a}_\pi \in S$, where $\mathbf{a}_\pi(i) := \mathbf{a}(\pi^{-1}(i))$. Clearly, if a subalgebra of $\mathbf{A}^\kappa$ has a totally symmetric generating set, then it is totally symmetric.

We assume that the reader is familiar with basic notions and results of universal algebra. Good textbooks are [2] and [6]. For the Abelian algebras, the term condition and congruence modular varieties, see [3].

2. Main result

Theorem 2.1. *The following are equivalent, for a variety $\mathcal{V}$:*

(1) *$\mathcal{V}$ is congruence distributive and admits an edge term t.*
(2) *$\mathcal{V}$ admits a Γ-special cube term s such that the corresponding Maltsev condition is not satisfied by any nontrivial module over any ring.*
(3) *$\mathcal{V}$ admits a Γ-special cube term s such that the corresponding Maltsev condition is not satisfied by any nontrivial vector space over the field of rationals $\mathbf{Q}$ and not satisfied by any nontrivial vector space over the field $\mathbf{Z}_p$ for any prime p.*
(4) *$\mathcal{V}$ admits a Γ-special cube term s such that Γ satisfies the divisibility property.*
(5) *$\mathcal{V}$ admits a near-unanimity term.*

Proof. (1) $\Rightarrow$ (2) : Let $t = t(x_1, x_1, \dots, x_m)$ be the edge term for $\mathcal{V}$. Let $p_1(x, y, z)$, $\dots, p_k(x, y, z)$ be Jónsson terms for $\mathcal{V}$ witnessing that $\mathcal{V}$ is congruence distributive (see [4]). We can assume that k is even. Thus $\mathcal{V}$ satisfies the equations

$$\begin{array}{rcl} p_i(x,y,x) & \approx & x \ \text{ for } 1 \le i \le k \\ p_1(x,y,y) & \approx & x \\ p_i(x,x,y) & \approx & p_{i+1}(x,x,y) \ \text{ for } i \text{ odd, } 1 \le i < k \\ p_i(x,y,y) & \approx & p_{i+1}(x,y,y) \ \text{ for } i \text{ even, } 2 \le i < k \\ p_k(x,y,y) & \approx & y\,. \end{array}$$

We define a sequence of terms $s_0, \dots, s_k$. We put $s_0 = t$, and given $s_{i-1} = s_{i-1}(z_1, \dots, z_n)$, then define

$$s_i = s_{i-1}(p_i(z_1, z_2, z_3), \dots, p_i(z_{3n-2}, z_{3n-1}, z_{3n})).$$

Call the term $s' := s_k$. It has $l = m3^k$ many variables. Now define

$$s := s'(s'(z_1, \dots, z_l), \dots, s'(z_{l(l-1)+1}, \dots, z_{l^2}))\,,$$

the term obtained by replacing all variables in s' by instances of s' with different variables. Let the absorption equations $s(\mathbf{u}_1, \dots, \mathbf{u}_{\ell^2}) \approx x$ in two variables, $\mathbf{u} \in \{x, y\}^n$, satisfied by s in $\mathcal{V}$ be $S = \{\varepsilon_1, \dots, \varepsilon_n\}$.

Now, from the fact that we get t as identification of blocks of variables of s' and therefore of s as well, the defining equations of t must be consequences of the equations in S. Therefore s is a Γ-special cube term with defining equations S; and analogously, s' is a Γ'-special cube term with defining equations S'. Moreover, each of the p_i can also be obtained by identifying variables of s, even of s', and therefore some of the equations in S express the fact that for all i, $p_i(x, y, x) = x$, that $p_1(x, y, y) = x$ and that $p_k(y, x, x) = x$.

It remains to show that no non-trivial module has a term operation satisfying all equations in the set S. Assume that there is a module $\mathbf{M}$ with a term operation that models S. We write $s^{\mathbf{M}}$ for this operation. For $1 \leq i \leq k$, let $q_i(x, y, z)$ the term obtained from s by identification of variables that equals $p_i(x, y, z)$ in $\mathcal{V}$. Let $q_i^{\mathbf{M}}$ be the term operation of $\mathbf{M}$ obtained from $s^{\mathbf{M}}$ by the same identification of variables. We shall show that $q_1^{\mathbf{M}}, \dots, q_k^{\mathbf{M}}$ are Jónsson operations for $\mathbf{M}$. Since no non-trivial module has term operations that satisfy Jónsson's equations, this will be a contradiction. The contradiction will complete our proof of (1) $\Rightarrow$ (2).

The equations $q_i(x, y, x) \approx x$, $q_1(x, y, y) \approx x$ and $q_k(y, x, x) \approx x$ belong to the set S, and so they hold in $\langle M, s^{\mathbf{M}} \rangle$. We show that $\langle M, s^{\mathbf{M}} \rangle \models q_1(x, x, y) \approx q_2(x, x, y)$. The same argument will establish each of the other Jónsson equations for $\langle M, s^{\mathbf{M}} \rangle$. To this end, for $0 \leq j \leq l$, define a $\mathcal{V}$-term

$$h_j(x, y, z) = s'(q_1(x, y, z), \dots, q_1(x, y, z), q_2(x, y, z), \dots, q_2(x, y, z))$$

(the first j instances of variables of s' are replaced by $q_1(x, y, z)$, while the remaining ones are replaced by $q_2(x, y, z)$). Replacing each occurence of a $q_i(x, y, z)$ in h_j by the $\mathcal{V}$-term which is s' applied to a certain sequence of the variables $\{x, y, z\}$ and which equals $q_i(x, y, z)$ in $\mathcal{V}$, we obtain a term $m_j(x, y, z)$ that is $\mathcal{V}$-equivalent to $h_j(x, y, z)$ and has the form of s applied to an appropriates sequence of variables drawn from $\{x, y, z\}$. Note that $m_0(x, y, z) = q_2(x, y, z)$ and $m_k(x, y, z) = q_1(x, y, z)$ identically. We are going to prove that

$$\langle M, s^{\mathbf{M}} \rangle \models m_j(x, x, y) \approx m_{j+1}(x, x, y)$$

for all $0 \leq j < l$ from which we conclude that $\langle M, s^{\mathbf{M}} \rangle$ models

$$q_1(x, x, y) = m_k(x, x, y) \approx m_0(x, x, y) = q_2(x, x, y)\,.$$

So let $0 \leq j < l$. Since s' is a Γ'-special cube term, there exists an absorption equation in two variables $\varepsilon : s'(z_1, \dots, z_l) \approx x$ (each z_i is either x or y) such that $z_{j+1} = y$. Therefore, by substituting all y in ε by $q_2(x, x, y)$ we obtain the same result x (by the Substitution Rule of equational logic), and so we have a new absorption equation. Replacing in this new equation the occurrence of $q_2(x, x, y)$ which is in place of z_{j+1} by $q_1(x, x, y)$, we get a second new absorption equation. These equations can be rewritten naturally as two members of S, ε_{i_1} and ε_{i_2} ($\varepsilon_{i_2} \in S$ since $\varepsilon_{i_1} \in S$ and $\mathcal{V} \models q_2(x, x, y) \approx q_1(x, x, y)$). So, in particular, the equality of the two terms on the left hand side of these two equations is derivable from S. The equality of these terms can be expressed as a valid equation of $\langle M, s^{\mathbf{M}}\rangle$ in the form

$$\mathbf{M} \models s^{\mathbf{M}}(u_1, \ldots, u_{l^2}) \approx s^{\mathbf{M}}(v_1, \ldots, v_{l^2})$$

where $u_i, v_i \in \{x, y\}$ and $u_i \neq v_i$ only for some i in the range $lj + 1 \leq i \leq l(j + 1)$. Since $\mathbf{M}$ is an Abelian algebra, an application of the term condition to the displayed equation yields that $\mathbf{M} \models m_j(x, x, y) \approx m_{j+1}(x, x, y)$, as we desired.

(2) $\Rightarrow$ (3) is immediate.

(3) $\Rightarrow$ (4) : Assume that $\mathcal{V}$ has a Γ-special cube term $t = t(x_1, \ldots, x_m)$ and the defining equations of t cannot be modelled in any nontrivial vector space over the rational field, or the field $\mathbf{Z}_p$ for any prime p. Notice that a term $t(x_1, \ldots, x_m)$ in any nontrivial vector space over a field $\mathbf{F}$ must have the form

$$t = \sum_{i=1}^{m} b_i x_i,$$

where b_i are elements of the field. To say that the equation ε_i (from the Definition 1.1) holds in this vector space is equivalent to saying that the sum of all coefficients b_j such that $\mathbf{a}_j(i) = y$ is equal to 0, while the sum of the remaining b_j is equal to 1. Let $Y_i = \{j | \mathbf{a}_j(i) = y\}$. Therefore, the vector space will have a term satisfying all of the equations ε_i iff the system of equations

$$\begin{aligned} \sum_{j=1}^{m} b_j &= 1 \\ \sum_{j \in Y_1} b_j &= 0 \\ &\vdots \\ \sum_{j \in Y_n} b_j &= 0 \end{aligned}$$

has a solution in $\mathbf{F}^m$.

We claim that such a solution of the above system of equations will exist iff the row vector $\mathbf{1} := \langle 1, 1, \ldots, 1\rangle \in \mathbf{F}^m$ is not in the subspace of $\mathbf{F}^m$ generated by the row vectors of $M(\Gamma)$. If a solution exists, then the row vector $\mathbf{1}$ obviously can't be in the subspace of $\mathbf{F}^m$ generated by the row vectors of $M(\Gamma)$, as this would imply that $0 = 1$ in $\mathbf{F}$. On the other hand, if the row $\mathbf{1}$ is not in the subspace of $\mathbf{F}^m$ generated by the row vectors of $M(\Gamma)$, and the rank of $M(\Gamma)$ is r, then the matrix of the above system of equations has the rank $r + 1$. Consider the augmented matrix of the system (with the added column of results). It also has the rank $r+1$, because if we take a square submatrix M' which contains the column of results, it will be regular iff the first row (the row $\mathbf{1}$) is included in M' and the submatrix of M' obtained by deleting the first row and last column is regular. But, this is a square submatrix of $M(\Gamma)$, so it must have dimension at most r. Therefore, by Kronecker-Capelli's theorem, the system has a solution.

The converse of the above Claim implies that when the Maltsev condition corresponding to a Γ-special cube term t fails in some nontrivial vector space over $\mathbf{Q}$, then there exist rational numbers $q_1, \ldots, q_n$ such that

$$\sum_{i=1}^{n} q_i \chi_{Y_i}(1) = \sum_{i=1}^{n} q_i \chi_{Y_i}(2) = \cdots = \sum_{i=1}^{n} q_i \chi_{Y_i}(m) = 1,$$

where χ_{Y_i} is the characteristic function of the set Y_i. Let k be the least common multiple of the denominators of all the rationals q_i and let $m_i = q_i k$. Then the last system of equations implies that there are integers m_i such that

$$\sum_{i=1}^{n} m_i \chi_{Y_i}(1) = \sum_{i=1}^{n} m_i \chi_{Y_i}(2) = \cdots = \sum_{i=1}^{n} m_i \chi_{Y_i}(m) = k,$$

the first condition of the divisibility property.

The second condition is obtained by an analogous argument, with $\mathbf{F} = Z_p$, for each prime divisor p of k.

(4) $\Rightarrow$ (5) : Let $\mathcal{V}$ be a variety admitting a Γ-special cube term t which satisfies the divisibility property. We may assume $\mathcal{V}$ is idempotent, otherwise just take the idempotent reduct of the $\mathcal{V}$-free algebra in a countable set of free generators (considered as a clone on itself) and generate a variety $\mathcal{V}'$. If we prove $\mathcal{V}'$ has a near-unanimity term, then the result for $\mathcal{V}$ follows.

Let $\mathbf{F} = \mathbf{F}(x, y)$ be the free algebra in $\mathcal{V}$ freely generated by $\{x, y\}$. Let $\mathbf{y}_i$, $i \in \omega$ be the elements of $\mathbf{F}^\omega$ such that $\mathbf{y}_i(i) = y$ and $\mathbf{y}_i(j) = x$, for $j \neq i$ and let $\mathbf{G} \leq \mathbf{F}^\omega$ be the subalgebra generated by $\{\mathbf{y}_i : i \in \omega\}$. It is easy to see that $\mathcal{V}$ has a near-unanimity term iff $\mathbf{G}$ contains the vector $\mathbf{x}$ which is constantly equal to x. In order to prove that this is so, we shall establish a series of claims about $\mathbf{G}$. The first one should be obvious.

Claim 1. $\mathbf{G}$ is a totally symmetric subpower of $\mathbf{F}$; and for every $\mathbf{a} \in \mathbf{G}$ and all but finitely many $i \in \omega$, $\mathbf{a}(i) = x$.

•

Let $\mathbf{H}$ be the subalgebra of $\mathbf{F}^\omega$ consisting of all functions that take the value x for all but finitely many integers $i \in \omega$. Thus $\mathbf{G} \leq \mathbf{H}$. For elements $\mathbf{a} \in H$, we adopt the notation $\mathbf{a} = a_1^{j_1} a_2^{j_2} \ldots a_l^{j_l}$ to mean that $\mathbf{a}(i) = a_r$ when $\sum_{s=1}^{r-1} j_s < i \leq \sum_{s=1}^{r} j_s$, while $\mathbf{a}(i) = x$ when $\sum_{s=1}^{l} j_s < i$. Now we can define "concatenation", an operation on $\mathbf{H}$ by:

$$\mathbf{ab} = a_1^{j_1} a_2^{j_2} \ldots a_l^{j_l} b_1^{k_1} b_2^{k_2} \ldots b_l^{k_r}$$

when $\mathbf{a} = a_1^{j_1} a_2^{j_2} \ldots a_l^{j_l}$ and $\mathbf{b} = b_1^{k_1} b_2^{k_2} \ldots b_l^{k_r}$. Although $\mathbf{G}$ is not closed under "concatenation", we will use it as a notational shortcut.

Without loss of generality, assume that the first row of $M(\Gamma)$ is of the form $\langle 0, \ldots, 0, 1, \ldots, 1 \rangle$, where the first s elements are 0, and the remaining $m - s$ are 1. We can assume that $s > 0$, for if $s = 0$ then $\mathcal{V} \models x \approx y$ and $\mathcal{V}$ certainly has a near-unanimity term. For $1 \leq i \leq s$, we define $u_i \in F$ to be $t(x, \ldots, x, y, x, \ldots, x)$ (y is at the ith position in t). By the definition of Γ-special cube terms, there must exist at least one defining equation ε of t such that on the left hand side of ε at the ith position of t there is y (otherwise the ith member of Γ would be in $\{x\}^n$). We define $v_i \in F$ to be the result of t applied to a tuple of x's and y's equal to the tuple on the left hand side of ε, except at the ith position, where it is equal to x.

Claim 2. For each tuple $\mathbf{a} = a_1^{r_1} \cdots a_l^{r_l} \in G$, all $1 \leq i \leq s$ and all $j \geq 0$, the tuple $\mathbf{a}u_i^j v_i^j$ is also in G.

Given i, let ε be the defining equation used to define v_i. We apply the term t in $\mathbf{G}$ to a tuple of $\mathbf{y}_1$, $\mathbf{y}_2$ and $\mathbf{y}_3$'s, so that $\mathbf{y}_1$'s are in the positions where xs are in ε, $\mathbf{y}_2$ is in the ith position and $\mathbf{y}_3$'s are in the remaining positions of t. The resulting element of $\mathbf{G}$ is, obviously, yu_iv_i. Because of the total symmetry of $\mathbf{G}$, the tuples of the form $x^p y x^q u_i v_i \in G$. Now, $\mathbf{a} = p(\mathbf{y}_1, \ldots, \mathbf{y}_r)$ for some term p and $r \in \omega$. Therefore,

$$p(yx^{r-1}u_iv_i, \ldots, x^{j-1}yx^{r-j}u_iv_i, \ldots, x^{r-1}yu_iv_i) = \mathbf{a}u_iv_i.$$

Now we can inductively prove that if $\mathbf{a}u_i^j v_i^j \in G$, then $\mathbf{a}u_i^j v_i^j u_i v_i \in G$, and then because of total symmetry of $\mathbf{G}$, we get $\mathbf{a}u_i^{j+1} v_i^{j+1} \in G$. •

Now we fix $k \in \omega$ to be the number from the first condition of the divisibility property of t.

Claim 3. If $\mathbf{a}u_i^k \in G$, or $\mathbf{a}v_i^k \in G$, then $\mathbf{a} \in G$. Also, if $\mathbf{a} \in G$, then $\mathbf{a}u_i^k \in G$ and $\mathbf{a}v_i^k \in G$.

To prove the first sentence of this Claim, let us first rephrase the first condition of the divisibility property: We know that there exist two finite sequences of the defining equations of t, S^+ and S^- (equations can be repeated in each sequence), such that the sum of occurrences of variable y at any coordinate of t in S^+ is by k greater than the sum of occurrences of y at the same coordinate in S^-. Let there be n_j many y's at the jth coordinate of t in the sequence S^- (hence, clearly, there are $n_j + k$ many y's at the jth coordinate of t in the sequence S^+).

Assume $\mathbf{a}u_i^k \in G$. Let the length of the word representing $\mathbf{a}$ be α, and let β and γ be the lengths of the sequences of equations S^+ and S^-, respectively. By the Claim 2, elements $\mathbf{a}'_j$ of the form $\mathbf{a}u_i^{n_j+k} v_i^{n_j} \in G$, for all $1 \leq j \leq m$. We can also use the total symmetry of $\mathbf{G}$ to insert any number of letters x between the letters of the word representing $\mathbf{a}'_j$ and still obtain a word representing an element of G. Therefore, $\mathbf{a}_j \in G$, where we define $\mathbf{a}_j$ by:

- for $1 \leq l \leq \alpha$, $\mathbf{a}_j(l) = \mathbf{a}(l)$,
- for $\alpha < l \leq \alpha + \beta$, $\mathbf{a}_j(l) = u_i$ if the $(l - \alpha)$th equation of S^+ has y at the jth coordinate of t and $\mathbf{a}_j(l) = x$ otherwise,
- for $\alpha + \beta < l \leq \alpha + \beta + \gamma$, $\mathbf{a}_j(l) = v_i$ if the $(l - \alpha - \beta)$th equation of S^- has y at the jth coordinate of t and $\mathbf{a}_j(l) = x$ otherwise, and
- for $\alpha + \beta + \gamma < l$, $\mathbf{a}_j(l) = x$.

We claim that $t(\mathbf{a}_1, \ldots, \mathbf{a}_m) = \mathbf{a}$. Clearly, by the idempotence, $t(\mathbf{a}_1, \ldots, \mathbf{a}_m)(l) = \mathbf{a}(l)$ for $1 \leq l \leq \alpha$ or $\alpha + \beta + \gamma < l$. For the remaining coordinates l we use the substitutions $y \mapsto u_i$ and $y \mapsto v_i$ and the fact that S^+ and S^- consist of defining equations of t to obtain $t(\mathbf{a}_1, \ldots, \mathbf{a}_m)(l) = x = \mathbf{a}(l)$. To finish the proof of the first sentence of this Claim, just notice that we can interchange u_i and v_i in the above proof.

The second sentence of the Claim follows from the first one and the fact that if $\mathbf{a} \in G$, then by the Claim 2, $\mathbf{a}u_i^k v_i^k \in G$. •

We denote by $P(l)$ the property of a positive integer l that for all finite sequences $\mathbf{a}$ in $\mathbf{F}$, $\mathbf{a} \in G$ iff $\mathbf{a}u_i^l \in G$. The above Claim proves $P(k)$.

Claim 4. For any positive integer l such that $l|k$ and any prime $q|l$, if $P(l)$, then $P(l/q)$.

To prove this Claim we use the second part of the divisibility property, for the prime q. We restate this condition similarly as in the previous Claim, and state that there exists a finite sequence of defining equations of t (we again are allowing repetition of equations), S^+, such that for each position j of the term t, the variable y occurs $k_j q + 1$ many times at the jth position of t, for some integer $k_j \geq 0$. Consider the sequence S' of the defining equations of t which is equal to l/q many copies of the sequence S^+ concatenated. The sequence S' has the property that the variable y occurs $k_j l + (l/q)$ many times at the jth position of t.

Now assume that $\mathbf{a}u_i{}^{\frac{l}{q}} \in G$. Then for $1 \leq j \leq m$, $\mathbf{a}'_j = \mathbf{a}u_i^{k_j l + \frac{l}{q}} \in G$, by $P(l)$. Also assume that the length of the word representing $\mathbf{a}$ is α and the length of the sequence S' is β. Analogously as in the proof of the previous Claim, we use the total symmetry of $\mathbf{G}$ to "insert" letters x in the appropriate places in the word for $\mathbf{a}'_j$ to get that $\mathbf{a}_j \in G$, where $\mathbf{a}_j$ is defined by:

- for $1 \leq r \leq \alpha$, $\mathbf{a}_j(r) = \mathbf{a}(r)$,
- for $\alpha < r \leq \alpha + \beta$, $\mathbf{a}_j(r) = u_i$ if the $(r - \alpha)$th equation of S' has y at the jth coordinate of t and $\mathbf{a}_j(r) = x$ otherwise,
- for $\alpha + \beta < r$, $\mathbf{a}_j(r) = x$.

We claim that $t(\mathbf{a}_1, \ldots, \mathbf{a}_m) = \mathbf{a}$. Clearly, by the idempotence, $t(\mathbf{a}_1, \ldots, \mathbf{a}_m)(r) = \mathbf{a}(r)$ for $1 \leq r \leq \alpha$ or $\alpha + \beta < r$. For the remaining coordinates r we use the substitutions $y \mapsto u_i$ and the fact that S' consists of defining equations of t to obtain $t(\mathbf{a}_1, \ldots, \mathbf{a}_m)(r) = x = \mathbf{a}(r)$.

To finish the proof of this Claim just notice that if $\mathbf{a} \in G$, then $\mathbf{a}u_i^l \in G$ by $P(l)$ and then by the already proved direction of $P(l/q)$ applied $q - 1$ times, $\mathbf{a}u_i{}^{\frac{l}{q}} \in G$.•

From the last Claim, it is obvious that $P(1)$ holds. Notice that

$$t(\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_s, \mathbf{y}_{s+1}, \mathbf{y}_{s+1}, \ldots, \mathbf{y}_{s+1}) = u_1 u_2 \ldots u_s \in G.$$

As we have proved that we can "erase" u_i (and $i \leq s$ was any fixed index), we deduce that the constant tuple $\mathbf{x} \in \{x\}^\omega$ is also in G. This means that for some large l, there exists a term p such that $p(\mathbf{y}_1, \ldots, \mathbf{y}_l) = \mathbf{x}$, and that means that the equations of the form $p(x, \ldots, x, y, x, \ldots, x) = x$ (y is in any position) hold in $\mathbf{F}$. As $\mathbf{F}(x, y)$ is the $\mathcal{V}$-free algebra, this means that p is an l-ary near-unanimity term for $\mathcal{V}$.

(5) $\Rightarrow$ (1) is a consequence of the fact that a near-unanimity term implies both the edge term (see [1]) and congruence distributivity. •

We are able to prove that (1) $\Rightarrow$ (5) directly, as well. This other proof, on the other hand, fails to give us the useful criterion (4) which recognizes exactly which Γ-special cube terms imply congruence distributivity, and is less aesthetically pleasing. The reader can find this other proof in [1]). We quote the exact result below:

Theorem 2.2. *A variety $\mathcal{V}$ is congruence distributive and has a $k+1$-ary edge term t iff $\mathcal{V}$ has a k-ary near-unanimity term s ($k \geq 3$).*

•

3. Acknowledgements

The authors wish to thank Keith Kearnes for suggesting that the result proved here might be true, Miklós Maróti for suggesting that a direct syntactical proof could also exist (the proof which was included in [1]) and Igor Dolinka for helpful discussions.

References

[1] J. Berman, P. Idziak, P. Marković, R. McKenzie, M. Valeriote and R. Willard, *Varieties with few subalgebras of powers,* in preparation.
[2] S. Burris and H. P. Sankappanavar, *A course in universal algebra,* Graduate Texts in Mathematics, No. 78, Springer-Verlag, New York-Berlin, 1981.
[3] R. Freese and R. McKenzie, *Commutator theory for congruence modular varieties,* London Mathematical Society Lecture Note Series, 125. Cambridge University Press, Cambridge, 1987.
[4] B. Jónsson, *Algebras whose congruence lattices are distributive,* Math. Scand. **21** (1967), 110–121.
[5] M. Maróti and R. McKenzie, *Existence theorems for weakly symmetric operations,* in preparation.
[6] R. McKenzie, G. McNulty and W. Taylor, *Algebras, lattices, varieties. Vol. I,* The Wadsworth & Brooks/Cole Mathematics Series, Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, CA, 1987.

Department of Mathematics and Informatics, University of Novi Sad, Serbia and Montenegro
E-mail address: pera@im.ns.ac.yu

Department of Mathematics, Vanderbilt University, Nashville, U.S.A.
E-mail address: mckenzie@math.vanderbilt.edu