

## CUBE-TERMS, FINITELY RELATED ALGEBRAS, AND CSP

ABSTRACT. We prove that a finite idempotent algebra is inherently finitely related if and only if it has a cube-term, find the maximal idempotent clones that do not contain a cube term, and make some observations about Valeriote’s conjecture.

### 1. INTRODUCTION

In this talk, all algebras mentioned are assumed to be finite. Andrei Bulyatov, Peter Jeavons and Andrei Krokhin showed that the CSP dichotomy conjecture of Feder and Vardi is equivalent to the statement that for every algebra  $\mathbf{A}$ , either some CSP problem over  $\mathbf{A}$  (built with relations that are compatible with the operations of  $\mathbf{A}$ ) is NP-complete, or else all such CSP problems are tractable (admit polynomial-time deterministic algorithms). Thus they founded the discipline of algebraic CSP studies. The two most important broad families of tractable algebras (with known polynomial-time algorithms) are the class of algebras with a cube term, and the class of algebras that belong to a congruence meet semi-distributive variety. Algebras in the second class are precisely those over which every CSP problem has finite relational width. This is a spectacular result of Libor Barto and Marcin Kozik [5]. Algebras in the first class are thought to exhaust all those whose CSP problems are tractable via some algorithm that is a natural generalization of the Malcev algorithm constructed by Victor Dalmau and Andrei Bulyatov (see [7]).

Beyond these two classes, we have the tractability of conservative algebras, proved by Bulyatov and recently re-proved by Barto, the tractability of algebras having at most four elements, recently proved by a Serbian team of researchers led by Petar Markovic, and the tractability of some classes of algebras that can be built by simple methods of combining algebras in the first two broad classes mentioned. (The “hybrid algorithms” showing tractability for these algebras were developed by Miklos Maroti, and in some special cases, by Markovic and McKenzie.)

All the mentioned results serve to unify our knowledge of tractable algebras, and to lend credence to the algebraic CSP dichotomy conjecture of Jeavons, Bulyatov and Krokhin, according to which  $\text{CSP}(\mathbf{A})$  is tractable for an algebra  $\mathbf{A}$  iff  $\mathbf{A}$  has a Taylor term. (This conjecture is patently stronger than the Feder and Vardi conjecture.)

Attempts to prove the algebraic CSP dichotomy conjecture have generated in the last few years a host of extremely interesting new results about finite universal algebras. In this talk, we shall explicate three of these results.

### 2. TAYLOR OPERATIONS AND CUBE OPERATIONS

A *clone of operations* on a set  $A$  is a family  $\mathcal{C}$  of finitary operations on  $A$  closed under compositions and including all the trivial projection operations,  $f(x_1, \dots, x_n) = x_i$ . A *clone of relations* (on a set  $A$ ) is a family  $\mathcal{R}$  of finitary relations over  $A$  closed under intersections, Cartesian products (concatenation of relations), permutations

of variables and projections, and which contains the 1-ary relation  $A$  and the 2-ary equality relation over  $A$ . If  $f : A^n \rightarrow A$  and  $R \subseteq A^k$  are an operation and a relation, the fundamental relation of admissibility holds between them iff  $f$  is a homomorphism from  $\langle A, R \rangle^n$  to  $\langle A, R \rangle$  or, equivalently,  $R$  is a subuniverse of  $\langle A, f \rangle^k$ . This relation of admissibility is a Galois connection between operations and relations that sets up a dual-isomorphism between the lattice of operational clones on  $A$  and the lattice of relational clones on  $A$ . For an operational clone  $\mathcal{C}$ , the corresponding relational clone is the set  $\mathcal{C}^\partial$  of all relations  $R$  that are admissible for all the operations of  $\mathcal{C}$ . For a relational clone  $\mathcal{R}$ , the corresponding operational clone  $\mathcal{R}^\partial$  is the set of all operations on  $A$  for which all the relations in  $\mathcal{R}$  are admissible. We have  $(\mathcal{C}^\partial)^\partial = \mathcal{C}$  and  $(\mathcal{R}^\partial)^\partial = \mathcal{R}$  for any operational clone  $\mathcal{C}$  and relational clone  $\mathcal{R}$  (over a finite set  $A$ ). This exact Galois connection between operations and relations over a finite set is the basis of the Jeavons-Bulyatov-Krokhin translation of CSP dichotomy into a conjecture about finite algebras.

An operation  $f(x_1, \dots, x_n)$  is called *idempotent* if it satisfies the equational law  $f(x, \dots, x) = x$ , equivalently, if every relation  $\rho_a = \{a\}$  (a 1-ary relation) where  $a$  belongs to the domain of  $f$ , is admissible for  $f$ . We denote the clone of all idempotent operations on  $A$  by  $\mathcal{I}_A$  (or simply  $\mathcal{I}$ ). An algebra  $\mathbf{A}$  is called idempotent if its clone of term operations (which is the clone generated by the basic operations of  $\mathbf{A}$ ) is included in  $\mathcal{I}$ .

We know that to prove the CSP dichotomy conjecture, it suffices to prove it for idempotent algebras (a basic observation of Jeavons-Bulyatov-Krokhin). Henceforth, all algebras considered will be assumed to be idempotent as well as finite.

The notion of a Taylor operation on  $A$  can be best explained by considering the two-generated free algebra  $\mathbf{F}$  in the variety generated by the algebra  $\langle A, f \rangle$ . Say  $\mathbf{F}$  is freely generated (relative to this variety) by elements  $x, y$ . Then  $f$  is a Taylor operation on  $A$  iff  $f$  is idempotent and, where  $f$  is, say,  $n$ -ary, we have some true equation

$$f(\bar{u}) = f(\bar{v})$$

in the algebra  $\mathbf{F}^n$  where  $\bar{u}, \bar{v}$  are  $n$ -tuples of elements of  $\{x, y\}^n$ , say

$$\begin{aligned} \bar{u} &= (u^1, \dots, u^n) \text{ and} \\ \bar{v} &= (v^1, \dots, v^n) \end{aligned}$$

and for all  $1 \leq i \leq n$ , we have  $u_i^i = y$  and  $v_i^i = x$ . Note that the Taylor equation  $f(\bar{u}) = f(\bar{v})$  is equivalent to a system of  $n$  equations, and can be visualized as equating the results of applying  $f$  to two  $n$ -by- $n$  matrices of  $x$ 's and  $y$ 's, namely  $\bar{u}$  and  $\bar{v}$ . The equations making up the system of  $n$  equations are read off by equating, for  $1 \leq i \leq n$ , the results of applying  $f$  in the free algebra  $F$  to the  $i$ 'th row of the matrix  $\bar{u}$  and also to the  $i$ 'th row of matrix  $\bar{v}$ : namely, we have

$$f(u_1^i, \dots, u_n^i) = f(v_1^i, \dots, v_n^i).$$

For a first example, consider a *Malcev operation* on  $A$ . This is, in the usual definition, an operation  $f(x, y, z)$  obeying the equational laws  $f(x, y, y) = x = f(y, y, x)$ . There are several ways to write these Malcev laws as the conjunction of the idempotent law  $f(x, x, x) = x$  and an equality between two applications of  $f$  in

$\mathbf{F}^3$  to two 3 by 3 matrices of  $x$ 's and  $y$ 's. For example

$$f \begin{pmatrix} y & y & x \\ y & y & x \\ x & y & y \end{pmatrix} = f \begin{pmatrix} x & x & x \\ x & x & x \\ x & x & x \end{pmatrix}.$$

Another important type of Taylor operation is the *near unanimity operation*. This is defined to be an  $n$ -ary operation on  $A$  (for some  $n \geq 3$ ) obeying the equations  $f(y, x, \dots, x) = f(x, y, x, \dots, x) = \dots = f(x, \dots, x, y) = x$ . (In other words the result of applying  $f$  to an input in which all but one of the entries is a fixed element  $a$ , must be again the nearly unanimous element  $a$ .) This definition can obviously be written in the Taylor form, as the conjunction of the idempotent equation  $f(x, \dots, x) = x$  and the matrix equation

$$f \begin{pmatrix} y & x & \cdots & \cdots & x \\ x & y & x & \cdots & x \\ & & \cdot & & \\ & & \cdot & & \\ x & x & \cdots & x & y \end{pmatrix} = f \begin{pmatrix} x & x & \cdots & \cdots & x \\ x & x & x & \cdots & x \\ & & \cdot & & \\ & & \cdot & & \\ x & x & \cdots & x & x \end{pmatrix}.$$

We introduce three other important examples of Taylor operations. A *weak near-unanimity operation* is  $f(x_1, \dots, x_n)$  for some  $n > 1$ , which obeys the idempotent equation and the equations  $f(y, x, \dots, x) = f(x, y, x, \dots, x) = \dots = f(x, x, \dots, x, y)$ . A *cyclic operation* is one obeying the idempotent equation and also the equation  $f(x_1, \dots, x_n) = f(x_2, x_3, \dots, x_n, x_1)$ . A *Siggers operation* is one  $S(x, y, z, u)$  obeying the equations  $S(x, x, x, x) = x$  and  $S(x, y, z, z) = S(y, z, x, y)$ . A rather amazing product of the efforts to apply finite universal algebra to prove CSP dichotomy has been the uncovering of the equivalence, for a finite, not necessarily idempotent algebra  $\mathbf{A}$  with clone of term operations  $\mathcal{C}$ , of each pair among the following possible properties of  $\mathbf{A}$ :

- there is a Taylor operation in  $\mathcal{C}$  (i.e.,  $\mathbf{A}$  has a Taylor term);
- there is a weak near-unanimity operation in  $\mathcal{C}$ ;
- for each prime integer  $p > |A|$ , there is a cyclic operation on  $p$  variables belonging to  $\mathcal{C}$ ;
- there is a Siggers operation in  $\mathcal{C}$ .

The equivalence of the first statement with the second was proved by Maroti and McKenzie [10]; of the first with the third was proved by Barto and Kozik [3]; of the first with the fourth was proved by M. Siggers (with simplifications by McKenzie, Markovic and Kearnes).

Amongst the above-defined classes of operations, just the Malcev operations and the near-unanimity operations are examples of cube operations. By a *cube operation* we mean a Taylor operation that satisfies a Taylor equation— $f(\bar{u}) = f(\bar{v})$ —where  $\bar{v}$  is an  $n$  by  $n$  matrix of  $x$ 's (and  $\bar{u}$  is an  $n$  by  $n$  matrix of  $x$ 's and  $y$ 's with purely  $y$  on the main diagonal).

There is a standard form of a cube operation. Let  $f$  be an  $n$ -ary cube operation. This means that for each  $i$ ,  $1 \leq i \leq n$  there is an equation obeyed by  $f$  that can be written as  $f(\bar{w}) = x$  where all  $w_j \in \{x, y\}$  and  $w_i = y$ . We may not need  $n$  equations to satisfy this requirement. For example, if  $f$  is Malcev, then  $n = 3$  whereas just two equations suffice. If  $k$  is the least size of a set of equations of this type demonstrating that  $f$  is a cube operation, then we get an equation in  $\mathbf{F}^k$  that

takes the form

$$f(\bar{u}) = \bar{x}$$

where  $\bar{x}$  is a  $k$  by 1 matrix of  $x$ 's,  $\bar{u}$  is a  $k$  by  $n$  matrix of  $x$ 's and  $y$ 's and each of the  $n$  columns of  $\bar{u}$  has an occurrence of  $y$ . We can assume that every two columns of  $\bar{u}$  are distinct, else by identifying two variables in  $f$  we create a cube operation with fewer variables that generates the same clone that  $f$  generates. Then, by adding dummy variables, we get an operation  $f'$  of  $m = 2^k - 1$  variables that satisfies an equation  $f(\bar{w}) = \bar{x}$  in  $\mathbf{F}^k$  where the columns of the  $k$  by  $m$  matrix  $\bar{w}$  are just all the distinct  $k$ -tuples of  $x$ 's and  $y$ 's that have at least one occurrence of  $y$  (and  $\bar{x}$  is a  $k$  by 1 matrix of  $x$ 's). Finally, by permuting the variables of  $f'$ , we get such an operation  $f''$  for which the  $k$  by  $m$  matrix  $\bar{w}$  has those  $m$  columns occurring in order, left to right, the same as lexicographic order over the alphabet  $\{x, y\}$  with  $x < y$ . This operation is a cube operation generating the same clone as our original  $f$  and its cube equations take a standard form, namely (reading off the rows of  $\bar{w}$ ):

$$\begin{aligned} f''(x^{2^{k-1}-1}y^{2^{k-1}}) &= x \\ f''(x^{2^{k-2}-1}y^{2^{k-2}}x^{2^{k-2}}\dots y^{2^{k-2}}) &= x \\ &\vdots \\ f''(xy^2x^2y^2\dots x^2y^2) &= x \\ f''(yxy\dots xy) &= x. \end{aligned}$$

This analysis explains why such an operation is called a *cobe operation*. In  $\mathbf{F}^k$  we have the  $k$ -dimensional cube  $\{x, y\}^k$ . Acting in  $\mathbf{F}^k$ , the cube operation produces the member  $\bar{x}$  of the cube, when applied to a standard list of all the remaining members of the cube.

Taylor operations were first defined by Walter Taylor who proved (in the 1970's) that any clone  $\mathcal{C}$  of idempotent operations on a set admits a clone homomorphism into the clone of trivial operations on a two-element set iff  $\mathcal{C}$  has no Taylor operation. In the 1980's, David Hobby and Ralph McKenzie proved that for any finite algebra  $\mathbf{P}$  (not necessarily idempotent),  $\mathbf{P}$  has a Taylor operation iff no finite algebra in the variety generated by  $\mathbf{P}$  has a covering pair  $\theta < \lambda$  of unary type in its congruence lattice. For a finite idempotent algebra  $\mathbf{P}$ , it can be shown using, various known results of universal algebra, that  $\mathbf{P}$  fails to have a Taylor term operation iff  $\mathbf{P}$  has a divisor  $\mathbf{Q} \in HS(\mathbf{P})$  which is a two-element algebra with trivial operations. Bulyatov and Krokhin noticed that this fact yields that if  $\mathbf{P}$  fails to have a Taylor term operation then  $CSP(\mathbf{P})$  contains an NP-complete problem. This observation proved (the easy) half of the algebraic CSP conjecture.

Pawel Idziak was probably the first to define cube operations, in 2005. He was trying to find useful necessary and sufficient conditions for an algebra to have few subpowers, where the correct definition of " $\mathbf{A}$  has few subpowers", he guessed, should be: there is a positive integer  $k$  so that for all positive integers  $n > 1$ ,  $|\text{Sub}(\mathbf{A}^n)| \leq 2^{n^k}$ . In fact, it is easy to see that if  $\mathbf{A}$  does not have a  $k$ -dimensional cube term then where  $\mathbf{F}$  is, again, the free algebra over  $\mathbf{A}$  freely generated by  $\{x, y\}$ , then distinct subsets of  $\{x, y\}^k$  generate distinct subalgebras of  $\mathbf{F}^k$ . And since  $\mathbf{F}$  is isomorphic to a subalgebra of  $\mathbf{A}^b$  for some positive integer  $b$ , then a simple calculation shows that if  $\mathbf{A}$  has few subpowers then  $\mathbf{A}$  has a  $k$ -dimensional

cube-term for large  $k$ . The converse implication, that if  $\mathbf{A}$  has a cube-term then it has few subpowers, was harder to prove. That is done in the paper [6], the precursor to [7] where it is shown that CSP problems over an algebra with a cube-term are tractable. These papers marked an amazingly successful outcome to a research effort that began with a vague intuition that if the relational clone corresponding to an algebra  $\mathbf{A}$  is relatively *sparse* (i.e., *if  $\mathbf{A}$  has few subpowers*), then it might be difficult (or impossible) to build relational structures in this clone that could have CSP-problem of high complexity.

### 3. THREE SIGNIFICANT CONSEQUENCES OF HAVING A CUBE-TERM

In this and the next section, we do not assume that an algebra is idempotent.

It was shown in [6] (Theorem 3.10) that any algebra with a  $k$ -dimensional cube-term has also a  $k$ -dimensional cube-term with just  $k + 1$  variables, namely, a  $k$ -edge term  $t(x_0, x_1, \dots, x_k)$  satisfying the equations

$$\begin{aligned} t(y, y, x, \dots, x) &= x \\ t(y, x, y, x, x, \dots, x) &= x \\ t(x, x, x, y, x, \dots, x) &= x \\ &\cdot \\ &\cdot \\ t(x, x, \dots, x, y) &= x. \end{aligned}$$

Here the first two equations each have two occurrences of  $y$  and the remaining equations have just one occurrence of  $y$  substituted, respectively, for the variable  $x_3$ , the variable  $x_4$ , etc.

The  $k$ -edge term and two more derived terms were very useful in proving the following significant Theorem about generating sets of subpowers of  $\mathbf{A}$  where  $\mathbf{A}$  has a  $k$ -dimensional cube-term. (This Theorem implies that having a cube-term necessitates that the algebra  $\mathbf{A}$  has few subpowers.) Let  $X$  be a finite nonvoid set supplied with a linear order, denoted by  $<$ . Suppose that  $R$  is a subalgebra of  $\mathbf{A}^X$ . By an *index* we mean any triple  $(i, a, b)$  with  $i \in X$  and  $\{a, b\} \subseteq A$ . We say that a pair of functions  $(f, g) \in (A^X)^2$  *witnesses the index*  $(i, a, b)$  if  $f(x) = g(x)$  for all  $x < i$  while  $(f(i), g(i)) = (a, b)$ . We say that an *index*  $(i, a, b)$  *is witnessed in*  $R$  if this index has a witness pair  $(f, g) \in R^2$ . The following theorem is an easy consequence of [6] (Corollary 3.9).

**Theorem 3.1.** *Suppose that  $\mathbf{A}$  is a finite algebra with a  $k$ -dimensional cube-term,  $X$  is some finite set supplied with a linear order, and  $R, S$  are subalgebras of  $\mathbf{A}^X$  with  $R \subseteq S$ . If  $R$  and  $S$  witness the same indexes and if, moreover, for every set  $Y \subseteq X$  with  $|Y| < k$  we have that the projections of  $R$  and  $S$  into  $\mathbf{A}^Y$  are equal, then  $R = S$ .*

**Exercise 3.2.** Let  $\mathbf{A}$  be an algebra with a  $k$ -dimensional cube-term. Suppose that  $C(x_1, \dots, x_m)$  ( $m = 2^k - 1$ ) is a  $k$ -dimensional cube-term for  $\mathbf{A}$  with  $2^k - 1$  variables obeying the standard set of  $k$  equations. Show that there exist terms of  $\mathbf{A}$ — $m_0(x, y, z, u), \dots, m_b(x, y, z, u)$ —obtained by substituting  $x, y, z, u$  for the variables of  $C(\bar{x})$ , which satisfy Alan Day's equations. Thus  $\mathbf{A}$  generates a congruence-modular variety.

## 4. EVERY ALGEBRA WITH A CUBE-TERM IS FINITELY RELATED

The title result of this section is proved in [1]. It has a spectacular consequence. If we regard algebras that are isomorphic, or have the same clone of term operations, as essentially identical, then there are only countably many finite algebras with a cube-term. We shall merely present the outline of the proof, leaving the reader to fill in the details.

Let  $\mathbf{A}$  be a finite algebra with a cube-term. We have to show that there is a finite set of admissible relations of  $\mathbf{A}$ , say  $R_1, \dots, R_m$  so that the clone  $\mathcal{C}$  of all term operations of  $\mathbf{A}$  is identical with  $\{R_1, \dots, R_m\}^\partial$ . Since  $\mathcal{C} = \mathcal{R}^\partial$  for some set  $\mathcal{R}$  of relations, then it will suffice to show that the ordered set of clones containing  $\mathcal{C}$  has the descending chain condition. That is what we shall do.

If  $\mathcal{D}$  is a clone containing  $\mathcal{C}$  then for each positive integer  $n$ ,  $\mathcal{D}_n$ , the set of  $n$ -ary members of  $\mathcal{D}$ , is a subalgebra of  $\mathbf{A}^{A^n}$ . We fix a linear order of  $A$ , and with respect to that order, we choose the lexicographic order of  $A^n$ , for each  $n$ . (Later on, we shall be talking about witnesses in  $\mathcal{D}_n$  of indexes  $(\alpha, a, b)$ ,  $\alpha \in A^n$ ,  $(a, b) \in A^2$ . This will be with respect to the lexicographic order on  $A^n$ .)

We write elements of  $A^n$  as words over the alphabet  $A$ . Where

$$W = \bigcup_n A^n$$

is the set of all nonvoid words over the alphabet  $A$ , we define a partial order  $\preceq$  on  $W$ . Namely, for words  $\alpha, \beta$ , we put  $\alpha \preceq \beta$  provided the two words have the same content (i.e., any element of  $A$  occurs in  $\alpha$  iff it occurs in  $\beta$ ) and where, say  $\alpha = a_1 \cdots a_r$  and  $\beta = b_1 \cdots b_s$ , there is a one-one increasing map  $\pi$  from  $\{1, \dots, r\}$  to  $\{1, \dots, s\}$  so that, first,  $b_{\pi(i)} = a_i$  for  $1 \leq i \leq r$ , and second, if  $1 \leq i \leq r$  and for no  $j < i$  is  $a_j = a_i$  then for no  $k < \pi(i)$  is  $b_k = b_{\pi(i)}$  ( $= a_i$ ). (In other words, we can find  $\alpha$  as a sub-sequence  $\alpha'$  of  $\beta$  in such a way that first occurrences of letters in  $\alpha'$  are also first occurrences in  $\beta$ .)

**Exercise 4.1.** Verify that  $\preceq$  is a partial order of  $W$  and prove

**Lemma 4.2.** *The ordered set  $(W, \preceq)$  is well quasi-ordered; i.e., for every infinite sequence  $\alpha_0, \alpha_1, \dots, \alpha_n, \dots$  in  $W$  there is  $i < j$  so that  $\alpha_i \preceq \alpha_j$ .*

Continuing with our proof of the result in the title of this section, suppose that our claim that the ordered set of clones containing  $\mathcal{C}$  has the descending chain condition fails. Then there is a strictly descending sequence of clones on  $A$ ,  $\mathcal{C}^1 > \cdots > \mathcal{C}^n > \cdots > \mathcal{C}$ . We shall show that this leads to a contradiction. For  $\alpha \in W$ ,  $(a, b) \in A^2$  and  $n \geq 1$  we say the index  $(\alpha, a, b)$  is witnessed in  $\mathcal{C}^n$  iff it is witnessed in the algebra  $\mathcal{C}_p^n \leq \mathbf{A}^p$  where  $p$  is the length of  $\alpha$  (so that  $\alpha \in A^p$ ). (Note that for this index to be so witnessed just means that there are  $p$ -ary operations  $f, g \in \mathcal{C}^m$  such that  $(f(\alpha), g(\alpha)) = (a, b)$  and for all  $\beta \in A^p$  with  $\beta$  lexicographically less than  $\alpha$ , we have  $f(\beta) = g(\beta)$ .) Now for  $(a, b) \in A^2$  and  $m \geq 1$  we define

$$W_{(a,b)}^m = \{\alpha \in W : \text{the index } (\alpha, a, b) \text{ is witnessed in } \mathcal{C}^m\}.$$

**Exercise 4.3.** (This is the heart of the proof that  $\mathbf{A}$  is finitely related.) Show that  $W_{(a,b)}^m$  is a down-set in the partially-ordered set  $(W, \preceq)$ .

Now for fixed  $(a, b)$  we have a descending sequence of down-sets

$$W_{(a,b)}^1 \supseteq W_{(a,b)}^2 \supseteq \cdots \supseteq W_{(a,b)}^n \supseteq \cdots$$

in  $(W, \preceq)$ . Since this partially ordered set is well quasi-ordered, there must be  $m = m_{(a,b)}$  so that for all  $k \geq m$ ,  $W_{(a,b)}^k = W_{(a,b)}^m$ .

Since  $A$  is finite, there is  $k(1)$  so that for all  $\ell \geq k(1)$  and for all  $(a,b) \in A^2$ ,  $W_{(a,b)}^\ell = W_{(a,b)}^{k(1)}$ . As a consequence, for any  $\ell, \ell' \geq k(1)$  and for all  $p \geq 1$  we have that  $\mathcal{C}_p^\ell$  and  $\mathcal{C}_p^{\ell'}$  witness the same indexes.

**Exercise 4.4.** Recalling Theorem 3.1, you will see that to use it here, we need to deal also with the projections of the algebras  $\mathcal{C}_p^\ell$  to  $\mathbf{A}^Y$  where  $Y$  ranges over subsets of  $A^p$  of size at most  $k-1$ . (Remember that we assumed  $\mathbf{A}$  has a  $k$ -dimensional cube-term.) Suppose that  $\mathcal{D}, \mathcal{E}$  are clones on  $A$  and that  $\mathcal{D}_s = \mathcal{E}_s$  for  $s = |A|^{k-1}$ . Show that in this case, for all  $Y \subseteq A^p$  with  $|Y| \leq k-1$  we have that the projections of  $\mathcal{D}_p$  and  $\mathcal{E}_p$  to  $\mathbf{A}^Y$  are equal.

Now for  $s = |A|^{k-1}$  since  $A^{A^s}$  is finite and  $\mathcal{C}_s^1, \mathcal{C}_s^2, \dots$  is a decreasing sequence of subsets of  $A^{A^s}$ , there is  $k(2)$  so that  $\mathcal{C}_s^\ell = \mathcal{C}_s^{\ell'}$  for all  $\ell, \ell' \geq k(2)$ .

Finally, suppose that  $k(3)$  is the max of  $k(1)$  and  $k(2)$ , and we have  $\ell' > \ell \geq k(3)$ . For any  $p > 1$ , we have the algebras  $R = \mathcal{C}^{\ell'} \subseteq S = \mathcal{C}^\ell \subseteq \mathbf{A}^{A^p}$ . We have shown that  $R$  and  $S$  witness the same indexes, and have the same projections to  $\mathbf{A}^Y$  whenever  $Y$  is a subset of  $A^p$  of size less than  $k$ . According to Theorem 3.1, it follows that  $\mathcal{C}_p^{\ell'} = \mathcal{C}_p^\ell$ . Since this is true for all  $p \geq 1$ , then  $\mathcal{C}^{\ell'} = \mathcal{C}^\ell$  whenever  $\ell' > \ell \geq k(3)$ . This contradiction finishes the proof that finite algebras with cube-terms are finitely related.

## 5. DECIDING WHEN AN IDEMPOTENT ALGEBRA $\langle A, f_1, \dots, f_n \rangle$ HAS A CUBE-TERM

The remaining pages of these notes are constructed from the paper [9]. Henceforth, all algebras mentioned will be assumed to be idempotent.

Let  $A$  be a finite set. We shall now define some clones that will turn out to be precisely all the maximal members of the family of not finitely related subclones of the clone  $\mathcal{I}$  of idempotent operations on  $A$ . They will also prove to be precisely all the maximal members of the family of all subclones of  $\mathcal{I}$  that fail to contain a cube operation. They are finite in number. Using them, we get an easy algorithm to determine if an idempotent algebra  $\langle A, f_1, \dots, f_n \rangle$  has a cube-term.

Choose any pair  $D, S$  of nonvoid subsets of  $A$  with  $D$  properly included in  $S$ . For each  $n \geq 1$  let  $R_n(D, S)$  be the  $n$ -ary relation  $S^n \setminus (S \setminus D)^n$  (which consists of all the  $n$ -tuples from  $S$  that have at least one entry from  $D$ ). We define

$$\mathcal{C}(D, S) = \{R_n(D, S) : n \geq 1\}^\partial \cap S^\partial$$

and we put  $\mathcal{C}_i(D, S) = \mathcal{C}(D, S) \cap \mathcal{I}$ .

**Exercise 5.1.** Prove that an operation  $f(x_1, \dots, x_k)$  over  $A$  belongs to  $\mathcal{C}(D, S)$  iff  $S$  is a subalgebra in  $\langle A, f \rangle$  and there is  $i$ ,  $1 \leq i \leq k$ , so that whenever  $\bar{a} \in S^k$  and  $a_i \in D$  then  $f(\bar{a}) \in D$ .

It is easy to see that each of the clones  $\mathcal{C}(D, S)$  and  $\mathcal{C}_i(D, S)$  fails to be finitely related. For example, to show that  $\mathcal{C}_i(D, S)$  is not finitely related, it suffices to show that for  $n > 1$ , there is an idempotent operation  $g$  that respects  $S$ , respects  $R_1(D, S)$  ( $= D$ ) and respects  $R_2(D, S), \dots, R_n(D, S)$ , and does not respect  $R_{n+1}(D, S)$ . Define  $g(a_0, \dots, a_n)$  (where  $\{a_0, \dots, a_n\} \subseteq A$ ) to be  $a_0$  if for at most one  $i$ ,  $0 \leq i \leq n$  do we have  $a_i \in D$ , and otherwise, define it to be  $a_i$  where  $a_i \in D$  and for no  $j < i$  is  $a_j \in D$ .

**Exercise 5.2.** Show that if  $(D, S)$  and  $(D', S')$  are two distinct pairs of subsets of  $A$  as above, then  $\mathcal{C}(D, S) \not\subseteq \mathcal{C}(D', S')$  and  $\mathcal{C}_i(D, S) \not\subseteq \mathcal{C}_i(D', S')$ .

Let  $\mathbf{A}$  be an algebra (idempotent, of course) with  $A$  as its universe. Let  $\mathcal{C}$  be the clone of term operations of  $\mathbf{A}$ . If  $\mathbf{A}$  has a cube-term then  $\mathcal{C} \subseteq \mathcal{C}_i(D, S)$  holds for no pair  $(D, S)$ , because  $\mathcal{C}_i(D, S)$  obviously contains no cube-term. The main work of this section consists in showing that conversely, if  $\mathbf{A}$  has no cube-term then in fact,  $\mathcal{C} \subseteq \mathcal{C}_i(D, S)$  for some pair  $(D, S)$ .

So assume that  $\mathbf{A}$  has no cube-term. If  $\mathbf{B}$  is a subalgebra of  $\mathbf{A}$  and there is a pair of nonvoid subalgebras  $(D, S)$  of  $\mathbf{B}$  with  $D$  properly included in  $S$  and the clone of term operations of  $\mathbf{B}$  contained in  $\mathcal{C}_i(D, S)$  as defined on  $B$ , then it's easy to see that  $\mathcal{C}$  (the clone of term operations of  $\mathbf{A}$ ) is included in  $\mathcal{C}_i(D, S)$  as defined on  $A$ . This means that it will suffice to choose among all the subalgebras of  $\mathbf{A}$  that fail to have a cube-term, a minimal one, and demonstrate the desired conclusion for that algebra. Or better, we shall simply assume that although  $\mathbf{A}$  has no cube-term, every proper subalgebra of  $\mathbf{A}$  does have a cube-term.

To continue, we need some notation. For elements  $a, b$  in a finite idempotent algebra  $\mathbf{P}$  let us write  $a \prec b$  to denote that  $\mathbf{P}$  has a term  $t(x_1, \dots, x_n)$  such that for some  $k$  there is an  $\{a, b\}$ -valued  $k$  by  $n$  matrix  $\bar{u}$  so that we have  $t(\bar{u}) = \bar{a}$  where  $\bar{a}$  is the  $k$  by 1 constant matrix with entries  $a$ , and such that every column of  $\bar{u}$  has an occurrence of  $b$ . When  $a \prec (a, b)$  via  $t$ , we say that  $t$  is a *cube-term for*  $\{(a, b)\}$ . We say that  $t$  is a cube-term for  $\{(a_1, b_1), \dots, (a_k, b_k)\} \subseteq P^2$  if  $t$  is a cube-term for  $\{(\bar{a}, \bar{b})\}$  in  $\mathbf{P}^k$  where  $\bar{a} = (a_1, \dots, a_k)$  and  $\bar{b} = (b_1, \dots, b_k)$ .

Next, for terms  $p = p(x_1, \dots, x_e)$  and  $q = q(x_1, \dots, x_f)$ , by  $p \star q$  we denote the term

$$p(q(x_{11}, \dots, x_{1f}), q(x_{21}, \dots, x_{2f}), \dots, q(x_{e1}, \dots, x_{ef})),$$

with  $ef$  many distinct variables. Finally, for  $\{a, b\} \subseteq P$  we denote as  $\langle a, b \rangle_{\mathbf{P}}$  the subalgebra of  $\mathbf{P}$  generated by  $\{a, b\}$ .

**Lemma 5.3.** *In any idempotent algebra  $\mathbf{P}$  the following are true.*

- (1) *Suppose that  $t_1, \dots, t_k$  are terms,  $t = t_1 \star t_2 \star \dots \star t_k$ , and  $a, b \in A$ . If for some  $i$ ,  $a \prec b$  via  $t_i$ , then  $a \prec b$  via  $t$ . If for some  $i$ ,  $c \in \langle a, b \rangle_{\mathbf{P}}$  via  $t_i$  then  $c \in \langle a, b \rangle_{\mathbf{P}}$  via  $t$ .*
- (2) *If  $\mathbf{P}$  is finite, then there exists a term  $m(x_1, \dots, x_p)$  such that whenever  $a, b, c \in A$  then  $a \prec b$  implies that  $a \prec b$  via the term  $m$ , and whenever  $c \in \langle a, b \rangle_{\mathbf{P}}$  then  $c \in \langle a, b \rangle_{\mathbf{P}}$  via  $m$ .*

**Theorem 5.4.** *Let  $\mathbf{P}$  be a (finite, idempotent) algebra. Then  $\mathbf{P}$  has a cube-term iff for all  $a, b \in P$  we have  $a \prec b$ .*

One of the implications constituting this theorem is clear. For the other, assume that  $a \prec b$  holds for all  $\{a, b\} \subseteq P$  and prove by induction on  $n$  that for all  $\{(a_1, b_1), \dots, (a_k, b_k)\} \subseteq P^2$  there is a cube-term for this set of pairs. When the set of pairs exhausts  $P^2$ , a cube-term for the set will be a cube-term for  $\mathbf{P}$ . For the inductive step, suppose that

$$\{(a_1, b_1), \dots, (a_k, b_k), (a_{k+1}, b_{k+1})\} \subseteq P^2$$

is given and  $t$  is a cube-term for  $\{(a_1, b_1), \dots, (a_k, b_k)\}$ . Thus there is a cube-term equation  $t(\bar{u}) = \bar{x}$  where  $\bar{x}$  is, say, an  $m$  by 1 column vector of  $x$ 's and  $\bar{u}$  is an  $m$  by  $n$  matrix of  $x$ 's and  $y$ 's with a  $y$  in every column so that the equation  $t(\bar{u}) = \bar{x}$

(or the package of  $m$  equations in  $\mathbf{P}$  signified by the rows of these two matrices) is validated whenever  $(x, y)$  is substituted by  $(a_i, b_i)$  for  $1 \leq i \leq k$ . When  $(x, y)$  is substituted by  $(a_{k+1}, b_{k+1})$  in  $\bar{u}$  to get a matrix  $\bar{u}'$ , then  $t(\bar{u}') = \bar{e}$  say, where we will denote the  $i$ 'th entry (counting from the top) in  $\bar{e}$  by  $e^i$ . Since  $a \prec b$  always holds then by the lemma there is a term  $m$  so that  $a_{k+1} \prec e^i$  via  $m$  for all  $1 \leq i \leq m$ .

**Exercise 5.5.** Verify that  $m \star t$  is a cube-term for  $\{(a_1, b_1), \dots, (a_k, b_k), (a_{k+1}, b_{k+1})\}$ , thus completing the inductive proof that every finite set of pairs in  $\mathbf{P}$  has a cube-term, establishing Theorem 5.4.

We can now finish the main proof of this section.

**Exercise 5.6.** Prove that for each  $b \in A$ ,  $\{x \in A : x \prec b\}$  is a subalgebra of  $\mathbf{A}$ . Hint: Let  $m$  be a term with the properties stated in Lemma 5.3 (2), taking  $\mathbf{P} = \mathbf{A}$ . Suppose that  $s(x_1, \dots, x_s)$  is some term and  $c_1, \dots, c_s$  are elements of  $P$  with  $c_i \prec b$  for  $1 \leq i \leq s$ , and put  $c = s(c_1, \dots, c_s)$ . Since  $\mathbf{A}$  is minimal, if  $\{c, b\}$  does not generate  $\mathbf{A}$  then  $c \prec b$  in the algebra generated by  $\{c, b\}$ , and thus in  $\mathbf{A}$ . So you can assume that  $\{c, b\}$  generates  $\mathbf{A}$ , and thus  $c_i \in \langle c, b \rangle_{\mathbf{A}}$  via  $m$  for  $1 \leq i \leq s$ . Also,  $c_i \prec b$  via  $m$  for all  $i$ . Show that  $c \prec b$  via the term  $s \star m \star s \star m$ .

To continue, by Theorem 5.4 we can choose  $(a, b) \in A^2$  with  $a \not\prec b$ . Take for  $D$  the algebra  $\{x \in A : x \prec b\}$  (see the last exercise) and for  $S$  take  $A$ . Now we claim that  $\mathcal{C} \subseteq \mathcal{C}_i(D, A)$ . Suppose this fails. Then we have some term  $s(x_1, \dots, x_\ell)$  which defines a term operation of  $\mathbf{A}$  that does not belong to  $\mathcal{C}_i(D, A)$ . By Exercise 5.1 this means that we have a system of  $\ell$  equations  $s(\bar{u}) = \bar{e}$  where  $\bar{u}$  is an  $\ell$  by  $\ell$  matrix of elements of  $A$  with  $u_i^i \in D$  for  $1 \leq i \leq \ell$ , and  $\bar{e}$  is an  $\ell$  by 1 matrix with  $e^i \in A \setminus D$  for  $1 \leq i \leq \ell$ . Thus  $u_i^i \prec b$  and  $e^i \not\prec b$  for each  $i$ . It follows by minimality of  $\mathbf{A}$  that  $\{e^i, b\}$  generates  $\mathbf{A}$  for each  $i$ .

**Exercise 5.7.** Using the same term  $m$  as in the last exercise, show that  $a \prec b$  via the term  $m \star s \star m \star m$ . This contradiction concludes the proof that we have found  $(D, S) = (D, A)$  so that  $\mathcal{C} \subseteq \mathcal{C}_i(D, S)$ .

So far in this section we have proved

**Theorem 5.8.** *A finite idempotent algebra  $\mathbf{A}$  has a cube-term iff its clone of term operations is included in none of the clones  $\mathcal{C}_i(D, S)$ .*

Given idempotent operations  $f_1, \dots, f_n$  on  $A$ , to decide if the algebra  $\mathbf{A} = \langle A, f_1, \dots, f_n \rangle$  has a cube-term, first compile a table showing for each choice of operation  $f_j$  and clone  $\mathcal{C}_i(D, S)$ , whether or not  $f_j \in \mathcal{C}_i(D, S)$ . This is easy using the criterion demonstrated in Exercise 5.1. Then use the table to decide if for some clone  $\mathcal{T} = \mathcal{C}_i(D, S)$ , all  $f_j$  belong to  $\mathcal{T}$ . If yes, then  $\mathbf{A}$  has no cube-term. If no, then  $\mathbf{A}$  has a cube-term. This algorithm is polynomial-time, so long as  $A$  is fixed and only the list  $f_1, \dots, f_n$  is allowed to vary.

It is clear from the result of §4, from the Exercise 5.2 and the remark preceding this exercise, and from Theorem 5.8, that a clone on  $A$  belongs to the family of clones  $\mathcal{C}_i(D, S)$  iff it is maximal among the subclones of  $\mathcal{T}$  that have no cube-term iff it is maximal among the subclones of  $\mathcal{T}$  that are not finitely related. The next corollary is also immediate.

**Corollary 5.9.** *A finite idempotent algebra has a cube-term iff its clone of term operations is inherently finitely related—i.e., every clone containing the basic operations of  $\mathbf{A}$  is finitely related.*

## 6. VALERIOTE'S CONJECTURE

Matthew Valeriote has conjectured that every finite and finitely related algebra in a congruence modular variety has a cube-term. The conjecture is plausible; L. Barto [2] recently proved the weaker conjecture of L. Zadori: every finite and finitely related algebra in a congruence-distributive variety has a near-unanimity term (and hence has a cube-term). Valeriote's conjecture, if true, would be a powerful fact. From it would follow that every finite idempotent algebra in a congruence-modular variety has tractable CSP problems.

In [9] (Theorem 4.1) the authors showed that Valeriote's conjecture holds iff for every finite algebra  $\mathbf{E}$  in any congruence-modular variety, if  $\mathbf{E}$  is finitely related then for every divisor  $\mathbf{D}$  of  $\mathbf{E}^2$ , every expansion of  $\mathbf{D}$  by adding constants is finitely related.

Here we note another equivalent of Valeriote's conjecture. Namely, it is equivalent to this statement: Let  $\rho$  be a finitary relation on a finite set  $A$ . Let  $(D, S)$  be a pair of nonvoid subsets of  $A$  with  $D$  properly included in  $S$ . If  $\rho$  is admissible for a system of Day operations on  $A$ , then for large enough  $n$ , the relation  $R_n(D, S)$  does not belong to the relational clone generated by  $\rho$ —i.e., it is not definable from  $\rho$  by a positive primitive formula of first order logic.

**Exercise 6.1.** Prove that this assertion is equivalent to Valeriote's conjecture.

## REFERENCES

- [1] E. Aichinger, R. McKenzie, P. Mayr, *On the number of finite algebraic structures*, (manuscript).
- [2] L. Barto, *CD implies NU*, (manuscript).
- [3] L. Barto, M. Kozik, *New conditions for Taylor varieties and CSP*, Logical Methods in Computer Science (to appear).
- [4] L. Barto, M. Kozik, *New conditions for Taylor varieties and CSP*. Proceedings of 25th IEEE Symposium on Logic in Computer Science, LICS'10, 100–109, 2010.
- [5] L. Barto, M. Kozik, *Constraint satisfaction problems of bounded width*. in *FOCS'09: Proceedings of the 50th Symposium on Foundations of Computer Science*, pages 595–605, 2009.
- [6] J. Berman, P. Idziak, P. Marković, R. McKenzie, M. Valeriote, R. Willard, *Varieties with few subalgebras of powers*, Transactions AMS **362** (2009), 1145–1173.
- [7] P. Idziak, P. Marković, R. McKenzie, M. Valeriote, R. Willard) *Tractability and learnability arising from algebras with few subpowers*, Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science, 221–230.
- [8] P. Marković, R. McKenzie, *Few subpowers, congruence distributivity, and near-unanimity terms*, Algebra Universalis (to appear).
- [9] P. Marković, M. Maroti, R. McKenzie, *Finitely related clones and algebras with cube-terms*, Order (to appear in the special BLAST issue).
- [10] M. Maroti, R. McKenzie, *Existence theorems for weakly symmetric operations*, Algebra Universalis **59** (2008), 463–489.
- [11] M. Valeriote, *A subalgebra intersection property for congruence distributive varieties*, Canadian J. Math **61** (2009), no. 2, 451–464.

DEPARTMENT OF MATHEMATICS, VANDERBILT UNIVERSITY, NASHVILLE, U.S.A.  
*E-mail address:* `rn.mckenzie@vanderbilt.edu`