

Some cardinal functions on algebras

J. Donald Monk

With any universal algebra $\mathfrak{U} = \langle A, f_i \rangle_{i \in I}$ one can associate several cardinal numbers important for the structure of \mathfrak{U} . In this note we shall consider the following ones: $|A|$; $|\text{Aut } \mathfrak{U}|$, where $\text{Aut } \mathfrak{U}$ is the group of automorphisms of \mathfrak{U} ; $|\text{Con } \mathfrak{U}|$, where $\text{Con } \mathfrak{U}$ is the lattice of congruence relations on \mathfrak{U} ; and $|\text{Sub } \mathfrak{U}|$, where $\text{Sub } \mathfrak{U}$ is the lattice of subalgebras of \mathfrak{U} . (Here we consider the empty set as a subalgebra of \mathfrak{U} , and for simplicity all operations are assumed to have positive rank.) We shall describe the possible relationships between these cardinals, assuming GCH and $|A| \geq \aleph_0$ (see Theorem 9). (GCH is the generalized continuum hypothesis.) A much more difficult question, which we do not completely answer, is to fully describe the variations $|A|$ can have for given automorphism group, congruence lattice, and subalgebra lattice. We do prove that if $|A|$ is ‘big’, then it can take on any possible value (Theorem 1, which is essentially known). Most of our efforts are with ‘small’ algebras, and here the constructions are standard except for the proof of the basic Lemma 3, where a rather unusual algebra is constructed. Various open questions are discussed at the end of the paper. The role of the GCH is also discussed. Some of the constructions here are relevant for the incorporation of the cardinal $|\text{End } \mathfrak{U}|$ (endomorphisms of \mathfrak{U}) into our problem setting. We intend to consider this cardinal function in a later note.

Our paper is self-contained; some relations to other papers are mentioned below.

Modifying slightly Lampe’s construction in [5], we can obtain the following result. (For any algebraic lattice L , let $\text{Cmp } L$ be the collection of compact elements of L .)

THEOREM 1. *Let G be a group and L_0 and L_1 algebraic lattices each with at least two elements. Let m be any cardinal $\geq |G| + |\text{Cmp } L_0| + |\text{Cmp } L_1| + \aleph_0$. Then there is an algebra \mathfrak{U} such that $|A| = m$, $\text{Aut } \mathfrak{U} \cong G$, $\text{Con } \mathfrak{U} \cong L_0$ and $\text{Sub } \mathfrak{U} \cong L_1$.*

Proof. It suffices to modify Lemma 19 of [5] so that the resulting partial algebra \mathfrak{B} has power m . For this purpose one lets $B = C_1 \times C_0^* \times G \times m$ with notation as in Lemma 19, and modifies the partial operations in the following way. For each $g \in G$ and $\alpha < m$ define a unary partial operation $f_{g\alpha}$ on B by $\text{Dmn } f_{g\alpha} = \{0\} \times \{y\} \times G \times m$ and $f_{g\alpha}(0, y, h, \beta) = (0, y, g \cdot h, \alpha)$ for each $h \in G$ and $\beta < m$. For each $(a, b) \in C_1 \times C_0^*$ define a binary partial operation $f_{a,b}$ by

$$\text{Dmn } f_{a,b} = \{((0, y, g, \alpha), (a, b, g, \alpha)) : g \in G, \alpha < m\}$$

and

$$f_{a,b}((0, y, g, \alpha), (a, b, g, \alpha)) = (0, y, g, \alpha) \quad \text{for all } g \in G, \alpha < m.$$

Presented by B. Jónsson. Received May 10, 1974. Accepted for publication in final form September 2, 1974.

Let \mathfrak{B} be B together with all of these operations plus the identity on B . It is lengthy but straightforward to carry through the rest of the proof as given in [5].

This theorem, although it is very strong, does not give all possible values for $|A|$, even when $|A| \geq \aleph_0$, since it is possible that $|A| < |\text{Aut } \mathfrak{U}|$. Note the following trivial cardinality restrictions for A infinite:

$$|\text{Aut } \mathfrak{U}| \leq \exp |A|, \quad |\text{Con } \mathfrak{U}| \leq \exp |A|, \quad |\text{Sub } \mathfrak{U}| \leq \exp |A|.$$

Since $\text{Cmp Sub } \mathfrak{U}$ is the collection of finitely generated subalgebras of \mathfrak{U} , we have $|\text{Cmp Sub } \mathfrak{U}| < |A|$, and similarly $|\text{Cmp Con } \mathfrak{U}| \leq |A|$.

In case $|A| < |\text{Aut } \mathfrak{U}|$, some restriction on $|\text{Sub } \mathfrak{U}|$ occur:

LEMMA 2. *If $|\text{Aut } \mathfrak{U}| > |A| \geq \aleph_0$, then in $\text{Sub } \mathfrak{U}$ the unit element is not a sum of $< m$ compact elements, where m is the least cardinal such that $|A|^m > |A|$.*

Proof. If the conclusion is false, then A is generated by a set X with $|X| < m$. Now

$$\text{Aut } \mathfrak{U} = \bigcup \{\{f \in \text{Aut } \mathfrak{U} : h \subseteq f\} : h \in {}^X A\}.$$

Since $|\{f \in \text{Aut } \mathfrak{U} : h \subseteq f\}| \leq 1$ for each $h \in {}^X A$, it follows that $|\text{Aut } \mathfrak{U}| \leq |A|$.

The following Lemma is basic for our treatment of the case $|A| < |\text{Aut } \mathfrak{U}|$:

LEMMA 3. *Let $m \geq \aleph_0$, and let n be the least cardinal such that $m^n > m$. Then there is an algebra \mathfrak{U} such that $|A| = m$, $|\text{Sub } \mathfrak{U}| = n$, and $|\text{Aut } \mathfrak{U}| = m^n$.*

Proof. Set $A = \bigcup_{\alpha < n} {}^\alpha m$. Thus $|A| = m$. For each $\alpha < n$ we introduce a unary operation r_α on A . For $x \in A$,

$$r_\alpha x = \begin{cases} x & \text{if } \text{Dmn } x \leq \alpha, \\ x \upharpoonright \alpha & \text{if } \alpha < \text{Dmn } x. \end{cases}$$

Let \circ be a group operation on m . Let B be the set of all $x \in {}^n m$ such that there is an $\alpha < n$ with $x_\beta = (\text{identity of } \langle m, \circ \rangle)$ for all β with $\alpha \leq \beta < n$. For each $x \in B$ we introduce a unary operation t_x on A . For each $y \in A$, let $\text{Dmn } t_x y = \text{Dmn } y$, and for any $\alpha < \text{Dmn } y$ let $(t_x y)_\alpha = x_\alpha \circ y_\alpha$. Let $\mathfrak{U} = \langle A, r_\alpha, t_x \rangle_{\alpha < m, x \in B}$. Then

$$\text{Sub } \mathfrak{U} = \{x \in A : \text{Dmn } x < \alpha\} : \alpha \leq n\}. \quad (1)$$

For, the inclusion \supseteq is clear. Now let $S \in \text{Sub } \mathfrak{U}$. Set $\alpha = \sup \{\text{Dmn } x + 1 : x \in S\}$. Clearly then $S \subseteq \{x \in A : \text{Dmn } x < \alpha\}$. Let $x \in A$, $\text{Dmn } x < \alpha$. Then $\text{Dmn } x \leq \text{Dmn } y$ for some $y \in S$. Let $\beta = \text{Dmn } x$, $z = r_\beta y$. Thus $z \in S$. For each $\gamma < \alpha$ let $u_\gamma = x_\gamma \circ z_\gamma^{-1}$ and $u_\gamma = \text{identity of } \langle m, \circ \rangle$ for $\alpha \leq \gamma < n$. Clearly then $t_u z = x$, so $x \in S$. Hence (1) holds.

For any $x \in {}^n m$ we define a mapping φ_x of A into A . For any $y \in A$, $\text{Dmn } \varphi_x y = \text{Dmn } y$, and for any $\alpha < \text{Dmn } y$, $(\varphi_x y)_\alpha = y_\alpha \circ x_\alpha$. It is easily checked that $\varphi_x \in \text{Aut } \mathfrak{U}$.

Let ψ be any automorphism of \mathfrak{U} . For any $x \in A$, say with $\text{Dmn } x = \alpha$, we have $\psi x = \psi r_\alpha x = r_\alpha \psi x$, and hence $\text{Dmn } \psi x \leq \text{Dmn } x$. Applying this to ψ^{-1} we get $\text{Dmn } \psi^{-1}$

$\psi x \leq Dmn \psi x \leq \alpha$ and hence $Dmn \psi x = Dmn x$. Furthermore, if also $y \in A$ and $x \leq y$, then $\psi x \leq \psi y$, since $\psi x = \psi r_\alpha y = r_\alpha \psi y$. Let $x = \bigcup \{\psi u_\alpha : \alpha < n\}$, where u_α is the element of A such that $Dmn u_\alpha = \alpha$ and $u_{\alpha\beta} = \text{identity of } \langle m, o \rangle$ for all $\beta < \alpha$. We claim that $\psi = \varphi_x$. For, let $y \in A$, say $Dmn y = \alpha$. Then with $z \in B$ such that $y \leq z$,

$$\psi y = \psi t_z u_\alpha = t_z \psi u_\alpha = t_z(x \upharpoonright \alpha) = \varphi_x y.$$

This completes the proof of the lemma.

LEMMA 4. *Let m and n be as in Lemma 3. Assume $n \leq p \leq m$. Then there is an algebra \mathfrak{A} such that $|A| = m$, $|\text{Sub } \mathfrak{A}| = p$, $|\text{Con } \mathfrak{A}| = 2$, and $|\text{Aut } \mathfrak{A}| = m^n$.*

Proof. Let $\mathfrak{A} = \langle A, f_i \rangle_{i \in I}$ be the algebra of Lemma 3. Let B be a set disjoint from A with $|B| = p$. Let $C = A \cup B$. Say $B = \{b_\alpha : 0 < \alpha < p\}$ with b one-one. Note that 0 (the empty sequence) is a member of A . Set $b_0 = 0$. We extend each operation f_i to an operation f_i^+ on C by letting f_i^+ act as the identity on B . For each $\alpha < p$ we introduce a unary operation S_α on C . S_α is to act as the identity on A , while for any $\beta < p$, $S_\alpha b_\beta = b_{\alpha \cap \beta}$. Finally, we introduce a ternary operation h on A : for any $a_0, a_1, a_2 \in A$,

$$h(a_0, a_1, a_2) = \begin{cases} a_0 & \text{if } a_1 \neq a_2, \\ a_1 & \text{if } a_1 = a_2. \end{cases}$$

Let $\mathfrak{C} = \langle C, f_i^+, S_\alpha, h \rangle_{i \in I, \alpha < p}$. Clearly $|C| = m$. Each automorphism of \mathfrak{A} clearly extends to an automorphism of \mathfrak{C} . The subalgebras of \mathfrak{C} are exactly all sets of the form $D \cup \{b_\alpha : \alpha < \beta\}$, where $D \in \text{Sub } \mathfrak{A}$ and $\beta \leq p$. Thus $|\text{Sub } \mathfrak{C}| = p$. Also, each automorphism of \mathfrak{C} fixes each element of B . For, each element of A is fixed by S_0 but each element of B is moved by S_0 , so ψ fixes B as a set. Now suppose $\psi b_\alpha = b_\beta$ with $\alpha \neq \beta$. We may assume that $\alpha < \beta$ (working with ψ^{-1} if $\beta < \alpha$). Then

$$b_\beta = \psi b_\alpha = \psi S_\alpha b_\alpha = S_\alpha \psi b_\alpha = S_\alpha b_\beta = b_\alpha.$$

contradiction. Finally, it is clear that $|\text{Con } \mathfrak{A}| = 2$.

LEMMA 5. *Let $m \geq n_0$. Then there is an algebra \mathfrak{A} of power m such that $|\text{Con } \mathfrak{A}| = 2$ and $|\text{Aut } \mathfrak{A}| = |\text{Sub } \mathfrak{A}| = 2^m$.*

Proof. Let $A = m$. Let h be the ternary operation on m such that for any $\alpha, \beta, \gamma < m$,

$$h(\alpha, \beta, \gamma) = \begin{cases} \alpha & \text{if } \beta \neq \gamma, \\ \beta & \text{if } \beta = \gamma. \end{cases}$$

The desired properties are easily checked.

The following lemma is well-known.

LEMMA 6. *Let \mathfrak{A} and \mathfrak{B} be algebras. Then there is an algebra \mathfrak{C} with universe $\mathfrak{A} \times \mathfrak{B}$ such that $\text{Sub } \mathfrak{C} \cong \text{Sub } \mathfrak{A}$, $\text{Aut } \mathfrak{C} \cong \text{Aut } \mathfrak{A}$, while $\text{Con } \mathfrak{C}$ has a smallest non-zero element and $\text{Con } \mathfrak{B}$ is isomorphic to the lattice of non-zero elements of $\text{Con } \mathfrak{C}$.*

Proof. Say $\mathfrak{A} = \langle A, f_i \rangle_{i \in I}$, $\mathfrak{B} = \langle B, g_j \rangle_{j \in J}$. For $i \in I$, say f_i m -ary, and for $a \in {}^m A$, $b \in {}^m B$, we set

$$f_i^+((a_0, b_0), \dots, (a_{m-1}, b_{m-1})) = (f_i(a_0, \dots, a_{m-1}), b_0).$$

The operations g_j^+ on $C = A \times B$ are similarly defined. For each $b \in B$ we define a unary operation h_b on C : for any $(a, c) \in C$, $h_b(a, c) = (a, b)$. Finally we define a ternary operation K . For any $(a_0, b_0), (a_1, b_1), (a_2, b_2) \in C$,

$$K((a_0, b_0), (a_1, b_1), (a_2, b_2)) = \begin{cases} (a_1, b_0) & \text{if } (a_1, b_1) \neq (a_2, b_2), \\ (a_0, b_0) & \text{if } (a_1, b_1) = (a_2, b_2). \end{cases}$$

Let $\mathfrak{C} = \langle C, f_i^+, g_j^+, h_b, K \rangle_{i \in I, j \in J, b \in B}$. To show that $\text{Sub } \mathfrak{C} \cong \text{Sub } \mathfrak{A}$, for any $D \in \text{Sub } \mathfrak{A}$ let $D^+ = \{(a, h) : a \in D\}$. Clearly $D^+ \in \text{Sub } \mathfrak{C}$, and $D \subseteq E$ iff $D^+ \subseteq E^+$ for $D, E \in \text{Sub } \mathfrak{A}$. Now suppose $F \in \text{Sub } \mathfrak{C}$. Fix $b_0 \in B$, and let $D = \{a : (a, b_0) \in F\}$. Clearly $D \in \text{Sub } \mathfrak{A}$. If $(a, b) \in D^+$, then $(a, b_0) \in F$, hence $(a, b) = h_b(a, b_0) \in F$. Thus $D^+ \subseteq F$, and similarly $F \subseteq D^+$. So ${}^+$ is the desired isomorphism.

For each $\varphi \in \text{Aut } \mathfrak{A}$, define $\varphi^+(a, b) = (\varphi a, b)$ for any $(a, b) \in C$. Clearly $\varphi^+ \in \text{Aut } \mathfrak{C}$ and ${}^+$ is an isomorphism of $\text{Aut } \mathfrak{A}$ into $\text{Aut } \mathfrak{C}$. Now let $\psi \in \text{Aut } \mathfrak{C}$. For any $(a, b) \in C$, $\psi(a, b) = \psi h_b(a, b) = h_b \psi(a, b)$, so $\psi(a, b) = (a', b)$ for some a' . If $\psi(a, b) = (a', b)$ and $\psi(a, b') = (a'', b')$ with $b \neq b'$, then

$$\begin{aligned} (a', b) &= \psi(a, b) = \psi K((a, b), (a, b'), (a, b)) \\ &= K(\psi(a, b), \psi(a, b'), \psi(a, b)) \\ &= K((a', b), (a'', b'), (a', b)) = (a'', b). \end{aligned}$$

Thus $a' = a''$. It follows that there is a permutation φ of A such that $\psi(a, b) = (\varphi a, b)$ for all $(a, b) \in C$. Clearly $\varphi \in \text{Aut } \mathfrak{A}$ and $\psi = \varphi^+$.

For $R \in \text{Con } \mathfrak{B}$ let $R^+ = \{((a_0, b_0), (a_1, b_1)) : b_0 R b_1\}$. Clearly $R^+ \in \text{Con } \mathfrak{C}$, and $R \subseteq S$ if $R^+ \subseteq S^+$ for $R, S \in \text{Con } \mathfrak{B}$. It remains to take any $T \in \text{Con } \mathfrak{C}$ with $T \neq \text{Id} \upharpoonright C$ and find $R \in \text{Con } \mathfrak{B}$ with $R^+ = T$. Say $((c_0, d_0) T (c_1, d_1))$ with $(c_1, d_0) \neq (c_1, d_1)$. Let $R = \{(b_0, b_1) : ((c_0, b_0) T (c_0, b_1))\}$. Clearly $R \in \text{Con } \mathfrak{B}$. Now let $(a_0, b_0) R^+ (a_1, b_1)$. Thus $(c_0, b_0) T (c_0, b_1)$, so $(a_0, b_0) = K((a_0, b_0), (c_1, d_1), (c_1, d_1)) T K((a_0, b_0), (c_0, d_0), (c_1, d_1)) = (c_0, b_0)$ and similarly $(a_1, b_1) T (c_0, b_1)$, and so $(a_0, b_0) T (a_1, b_1)$. Hence $R^+ \subseteq T$. Similarly $T \subseteq R^+$, so $T = R^+$. This completes the proof.

Combining Lemmas 4 and 6, we obtain

THEOREM 7. *Let $m \geq n_0$, and let n be the least cardinal such that $m^n > m$. Assume that $n \leq p \leq m$. Let L be an algebraic lattice with a smallest non-zero element such that $|\text{Cmp } L| \leq m$. Then there is an algebra \mathfrak{A} such that $|A| = m$, $\text{Con } \mathfrak{A} \cong L$, $|\text{Sub } \mathfrak{A}| = p$, and $|\text{Aut } \mathfrak{A}| = m^n$.*

Combining Lemmas 5 and 6:

THEOREM 8. Let $m \geq \aleph_0$. Let L be an algebraic lattice with a smallest non-zero element such that $|\text{Cmp } L| \leq m$. Then there is an algebra \mathfrak{A} such that $|A| = m$, $\text{Con } \mathfrak{A} \cong L$, and $|\text{Sub } \mathfrak{A}| = |\text{Aut } \mathfrak{A}| = 2^m$.

Now we can combine the preceding results to give a complete description of the relationships between the cardinals mentioned at the outset:

THEOREM 9. Assume GCH. Let m, p, q, r be cardinals such that $m \geq \aleph_0$, $p > 0$, and $q, r > 1$. Let n be minimal such that $m^n > m$. Then the following conditions are equivalent:

- (i) there is an algebra \mathfrak{A} such that $|A| = m$, $|\text{Aut } \mathfrak{A}| = p$, $|\text{Con } \mathfrak{A}| = q$, and $|\text{Sub } \mathfrak{A}| = r$;
- (ii) one of these conditions holds:
 - (1) $m \geq p$ and $q, r \leq m^+$
 - (2) $p = m^+$, $n \leq r \leq m^+$, and $q \leq m^+$.

Proof. Assume (i) and (1) fails. Then by the trivial inequalities, $p = m^+$. Hence by Lemma 2, $n \leq r$; the inequalities $r \leq m^+$ and $q \leq m^+$ are trivial.

Now assume (1). Let G be a group with $|G| = p$, and let L_0 and L_1 be the algebraic lattices such that $|L| = q$, $|L_1| = r$, and $|\text{Cmp } L_0| \leq m$, $|\text{Cmp } L_1| \leq m$; it is easy to find such lattices. Then an application of Theorem 1 gives the desired result.

That (2) implies (i) is an easy consequence of Theorems 7 and 8.

Note that under GCH the cardinal n of Theorem 9 coincides with the cofinality of m .

With regard to dropping the assumption GCH in Theorem 9, the following two results are relevant.

THEOREM 10. If \mathfrak{A} is a denumerable algebra and $m = |\text{Aut } \mathfrak{A}|$ or $|\text{Con } \mathfrak{A}|$ or $|\text{Sub } \mathfrak{A}|$, then $m \leq \aleph_0$ or $m = 2^{\aleph_0}$.

This theorem was established by Kueker and Reyes independently for $m = |\text{Aut } \mathfrak{A}|$, and by Burris and Kwatinetz in the remaining cases. The following theorem is a simple generalization of an unpublished result of Stephen Comer:

THEOREM 11. $\text{Con}(ZF) \rightarrow \text{Con}(ZFC + \text{for every regular cardinal } m \geq \aleph_0 \text{ there is an algebra } \mathfrak{A} \text{ of power } m^+ \text{ such that if } n = |\text{Aut } \mathfrak{A}| \text{ or } |\text{Con } \mathfrak{A}| \text{ or } |\text{Sub } \mathfrak{A}| \text{ then } m^+ < n < 2^{m^+})$.

Proof. By Easton's theorem, using the function F such that $Fm = m^{++}$ for every regular cardinal m , it suffices to prove within ZFC the following statement:

- (1) If $\aleph_0 \leq m < n < 2^m < 2^n$, then there is an algebra \mathfrak{A} of power n with $|\text{Aut } \mathfrak{A}| = |\text{Con } \mathfrak{A}| = |\text{Sub } \mathfrak{A}| = 2^m$.

To construct such an algebra, let $A = n$. For each $\alpha \in n \sim m$ let f_α be the unary operation on n such that, for any $\beta < n$, $f_\alpha \beta = \alpha$. Let g be the ternary operation on n such that for any $\alpha, \beta, \gamma < n$,

$$g(\alpha, \beta, \gamma) = \begin{cases} \beta & \text{if } \beta, \gamma \in n \sim m \text{ and } \beta \neq \gamma, \\ \alpha & \text{otherwise.} \end{cases}$$

Let $\mathfrak{U} = \langle n, f_\alpha, g \rangle_{\alpha \in n \sim m}$. Then the automorphisms of \mathfrak{U} are the permutations of n which are the identity on $n \sim m$. The subalgebras of \mathfrak{U} are the empty set and all subsets $\beta \cup (n \sim m)$ of n with $\beta \subseteq m$. The congruence relations of \mathfrak{U} are $n \times n$ and all equivalence relations on n which are the union of an equivalence relation on m with the identity on $n \sim m$.

These two theorems rule out some natural possibilities for generalizing Theorem 9 when GCH is eliminated. Many other generalizations or variations of Theorem 9 are conceivable. We mention just a few:

- (1) Consider the case $m < \aleph_0$.
- (2) Adjoin to the discussion some other cardinal functions, such as $|I|$, Gould and Grätzer's multiplicity types, $|\text{End } \mathfrak{U}|$.
- (3) Give a full description of the structures $\text{Aut } \mathfrak{U}$, $\text{Con } \mathfrak{U}$, etc., for a given cardinal $m = |\mathcal{A}|$; Theorem 1 is an important result in this direction.
- (4) Consider all of the questions for special kinds of algebras, such as groups, lattices, Boolean algebras. In McKenzie, Monk [6] the relationship of $|\mathcal{A}|$ to $|\text{Aut } \mathfrak{U}|$ is completely given for Boolean algebras, assuming GCH.

REFERENCES

- [1] S. N. Burris and M. K. Kwatinetz, *Some cardinality results for certain classes of mathematical structures*, Notices Amer. Math. Soc. 19 (1972), A-96.
- [2] W. B. Easton, *Powers of regular cardinals*, Ann. Math. Logic 1 (1970), 139–178.
- [3] M. Gould, *Multiplicity type and subalgebra structure in universal algebras*, Pacific J. Math. 26 (1968), 469–485.
- [4] D. Kueker, *Definability, automorphisms and infinitary languages*, in *The Syntax and Semantics of Infinitary Languages*, Notes in Math. No. 72, 1968, Springer-Verlag (1968), 152–165.
- [5] W. Lampe, *The independence of certain related structures of a universal algebra, IV*, Alg. Univ. 2 (1972), 296–302.
- [6] R. McKenzie and J. D. Monk, *On automorphism groups of Boolean algebras*, to appear.

*Eidgenössische Technische Hochschule
Zürich
Switzerland
and
University of Colorado
Boulder, Colorado
U.S.A.*