Some cardinal functions on algebras II

J. Donald Monk

In [2], knowledge of which is assumed here, the relationships between the cardinals $|A|$, $|\text{Aut} \mathcal{A}|$, $|\text{Sub} \mathcal{A}|$, and $|\text{Con} \mathcal{A}|$ were completely described, assuming that $|A|\geq \aleph_0$ and that the GCH holds. The purpose here is to do the same thing for the cardinals $|A|$, $|\text{Aut} \mathcal{A}|$, $|\text{End} \mathcal{A}|$, and $|\text{Sub} \mathcal{A}|$. The results here are easy adaptations from [2] and Gould, and Platt [1] except for Lemma 7. The construction in Lemma 7 is a generalization of an example by Ralph McKenzie of a denumerable algebra $\mathcal{A}$ with $|\text{Aut} \mathcal{A}| = 1$, $|\text{End} \mathcal{A}| = 2^{\aleph_0}$, and $|\text{Sub} \mathcal{A}| = \aleph_0$; another denumerable algebra with these properties was constructed by James S. Johnson.

First we consider the case of 'large' $\mathcal{A}$, i.e., algebras $\mathcal{A}$ with $|\text{End} \mathcal{A}| \leq |A|$. In this case we shall just generalize slightly a construction of Gould and Platt [1].

**Lemma 1.** Let $\mathcal{M}$ be a monoid in which every element is either right cancellative or a right zero. Let $m \geq |M| + \aleph_0$. Then there is an algebra $\mathcal{A}$ such that $|A| = m$, $\text{End} \mathcal{A}$ contains $\mathcal{M}$ as a submonoid, $|\text{Sub} \mathcal{A}| = 2$, and the subalgebra generated by the empty set has power $m$.

**Proof.** We modify slightly the proof of sufficiency in Theorem 3 of [1]. We may assume that $(S_0 \cup S_1) \cap m = 0$. Note that $|M| \leq |S_0 \cup S_1| \leq |M| + \aleph_0$. Let $A = S_0 \cup S_1 \cup m$. Thus $|A| = m$. We extend $f_2^\alpha$ to $A$ by setting $f_2^\alpha x = x$ for all $x \in m$. Let $\mathcal{A} = \langle A, a, f_2^\alpha \rangle_{\alpha \in S_0 \cup m; \gamma, \gamma' \in S_1}$. The desired properties of $\mathcal{A}$ are easily checked.

Now we can apply the proofs of Theorems 1 and 2 of [1] to obtain the following result:

**Theorem 2.** Let $\mathcal{M}$ be a monoid in which every element is either right cancellative or a right zero. Assume that $m \geq |M| + \aleph_0$. Let $\mathcal{L}$ be an algebraic lattice with at least two elements, with $|\text{Cmp} \mathcal{L}| \leq \aleph_0$. Then there is an algebra $\mathcal{A}$ such that $|A| = m$, $\text{End} \mathcal{A} \cong \mathcal{M}$, and $\text{Sub} \mathcal{A} \cong \mathcal{L}$.

Next, we treat the case in which both $\text{End} \mathcal{A}$ and $\text{Aut} \mathcal{A}$ are big, while $\text{Sub} \mathcal{A}$ is small. Note by Lemma 2 of [2], valid also for $\text{End} \mathcal{A}$ in place of $\text{Aut} \mathcal{A}$, that if $|\text{End} \mathcal{A}| > |A|$ then in $\text{Sub} \mathcal{A}$ the unit element is not a sum of $<m$ compact elements, where $m$ is the least cardinal such that $|A|^m > |A|$.

Presented by B. Jónsson. Received January 22, 1975. Accepted for publication in final form May 8, 1975.
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 $|\text{Aut } \mathfrak{U}| = |\text{End } \mathfrak{U}| = m^n$.

Proof. We use exactly the algebra of Lemma 3 of [2]. We must determine the endomorphisms of this algebra. Obviously each map $r_\alpha$, $\alpha < n$, is an endomorphism of $\mathfrak{U}$. We claim that any endomorphism $\psi$ of $\mathfrak{U}$ which is not an automorphism has the form $\phi_\alpha \circ r_\alpha$, and hence $|\text{End } \mathfrak{U}| = m^n$. To prove this, first note

1. $x = r_\alpha x$ iff $\text{Dmn } x \leq \alpha$.

Now for any $x$, say with $\text{Dmn } x = \alpha$, we have $\psi x = \psi r_\alpha x = r_\alpha \psi x$, so by (1), $\text{Dmn } \psi x \leq \alpha$.

Thus

2. $\text{Dmn } \psi x \leq \text{Dmn } x$ for all $x \in A$.

As in [2] one sees that

3. if $\text{Dmn } \psi x = \text{Dmn } x$ for all $x \in A$, then $\psi$ is an automorphism.

By (2) and (3), fix $x \in A$ such that $\text{Dmn } \psi x < \text{Dmn } x$. Let $\alpha = \text{Dmn } \psi x$. Now

4. if $\alpha < \text{Dmn } y < \text{Dmn } x$, then $\text{Dmn } \psi y = \alpha$.

For, write $\text{Dmn } x = \beta$. Then for some $z$, $x = t_\alpha r_\beta y$, so $\psi x = t_\alpha r_\beta \psi y$, so $\text{Dmn } \psi y = \alpha$. Also,

5. if $\alpha < \text{Dmn } y < \text{Dmn } x$, then $\text{Dmn } \psi y = \alpha$.

For, write $y = t_\alpha r_\beta x$, where $\beta = \text{Dmn } y$. Then $\psi y = t_\alpha r_\beta \psi x$, so $\text{Dmn } \psi y = \alpha$.

Now let $\mathfrak{U}$ have domain $\alpha$, with $u_\beta = \text{Identity}$ for all $\beta < \alpha$. Thus by (5), $\text{Dmn } \psi u = \alpha$.

Let $\psi = \psi \cup \langle \text{Identity: } \alpha < \beta < n \rangle$. We claim that $\psi = \phi_\alpha \circ r_\alpha$. Let $z \in A$ be arbitrary. We distinguish two cases.

Case 1. $\alpha \leq \text{Dmn } z$. Then $\text{Dmn } \psi z = \alpha$ by (4), (5), so, with $r_\alpha z \leq w \in B$,

$$\psi z = r_\alpha \psi z = r_\alpha \psi (t_\alpha w) = t_\alpha \psi (r_\alpha z) = \phi \alpha r_\alpha z.$$  

Case 2. $\text{Dmn } z < \alpha$. Say $\text{Dmn } z = \beta$. Then with $z \leq w \in B$,

$$\psi z = \psi (t_\alpha r_\beta w) = t_\alpha r_\beta \psi w = \phi \alpha r_\alpha z.$$  

This completes the proof.

THEOREM 4. Assume that $m \geq \aleph_0$, and let $n$ be the least cardinal such that $m^n > m$. Assume that $n < p < m$. Then there is an algebra $\mathfrak{U}$ such that $|A| = m$, $|\text{Sub } \mathfrak{U}| = p$, and $|\text{Aut } \mathfrak{U}| = |\text{End } \mathfrak{U}| = m^n$.

Proof. Let $\mathfrak{C}$ be formed as in Lemma 4 of [2], except without the operation $h$. It is clear that $|\mathfrak{C}| = m$, $|\text{Sub } \mathfrak{C}| = p$, and $|\text{Aut } \mathfrak{C}| = m^n$. It remains only to check that $|\text{End } \mathfrak{C}| = m^n$. If $\psi \in \text{End } \mathfrak{C}$ and $\alpha < p$, define $\chi_{\phi_\alpha} x = \psi x$ if $x \in A$, and $\chi_{\phi_\alpha} b_\beta = b_{\alpha \beta}$. Then $\chi_{\phi_\alpha} \in \text{End } \mathfrak{C}$. To prove this, first note

1. $\psi b_0 = b_0$.

For, $\psi b_0 = \psi r_0 b_0 = r_0 \psi b_0 = 0 = b_0$.

Obviously $\chi_{\phi_\alpha}$ preserves the operations $f^+_i$. Also we have

$$\chi_{\phi_\alpha} S_{\gamma} b_\gamma = b_{\alpha \gamma} \land \gamma = S_{\gamma} \chi_{\phi_\alpha} b_\gamma,$$
so $\chi_{\varphi}$ is in End $C$. If $\psi \in \text{End } A$, then $\psi^* x = \psi x$, $\psi^* b = b$ for $b \in B$ defines an endomorphism $\psi^*$ of $C$.

Now let $\varphi \in \text{End } C$; we claim that $\varphi$ has the form $\psi^*$ or $\chi_{\varphi}$. To prove this, first note

(2) $\forall x \in A \ (\varphi x \in A)$.

For, suppose $x \in A$ and $\varphi x = b$. Then $b_0 = S_0 b = S_0 \varphi x = \varphi S_0 x = \varphi x = b$, so $\varphi x = b$ = $b_0 \in A$. Also,

(3) $\varphi b_0 = b_0$.

For, $\varphi b_0 = \varphi r_0 b_0 = r_0 \varphi b_0 = 0 = b_0$ by (2). Next,

(4) $\forall x \in B \ (\varphi(x) \in B \cup \{b_0\})$.

For, suppose $\varphi b = x \in A$ with $x > 0$. Then $x = S_0 x = S_0 \varphi b = \varphi S_0 b = \varphi b_0 = b_0$.

By (2), (3), (4) it is clear that if $\varphi \uparrow B$ is the identity then $\varphi$ is $\psi^*$ for some $\psi \in \text{End } A$.

So, assume $\varphi b = b$ where $b, b_0 \in B \cup \{b_0\}$ and $\varphi \neq \beta$. If $\alpha < \beta$, then $\beta = \varphi b = \varphi S_0 b = S_0 \varphi b = S_0 b = b$, contradiction. Thus $\beta < \varphi$. If $\alpha \leq \gamma$, then

$\beta = \varphi b = \varphi S_0 b = S_0 \varphi b = S_0 b = b$,

so $\varphi b = b$. If $\beta \leq \gamma < \alpha$, then

$\varphi b = \varphi S_0 b = S_0 \varphi b = S_0 b = b$.

Finally, if $\gamma < \beta$, then

$\varphi b = \varphi S_0 b = S_0 \varphi b = S_0 b = b$.

Thus $\varphi$ has the form $\chi_{\varphi}$.

Now we take up the construction of an algebra $A$ with $\text{Aut } A$ small and $\text{End } A$, $\text{Sub } A$ big. The construction depends on the following lemma.

**Lemma 5.** For any $m \geq 2^n$ there is an algebra $A$ such that $|A| = m$, $|\text{End } A| = 2^m$,

$|\text{Aut } A| = 1$, and $|\text{Sub } A| = 2^m$.

**Proof.** Let $A = \langle m, \cap \rangle$. Then, as is easily seen,

(1) for any $X \subseteq m$, $X$ is a subalgebra of $A$;

(2) $f \in \text{End } A$ iff $\forall x, \beta \in m \ (\alpha \leq \beta \Rightarrow f x \leq f \beta)$.

From (2) it follows that any automorphism of $A$ is an order-preserving map of $m$ onto $m$; hence only the identity is an automorphism of $A$.

Now we exhibit $2^m$ endomorphisms of $A$. For any $f \in 2^m$ let $g_f : m \to m$ be defined as follows. Given $\gamma < m$, write $\gamma = \omega \cdot \alpha + \mu$ with $\alpha < m, m < \omega$. Set $g_f \gamma = \omega \cdot \alpha + \mu$. Then $g_f$ is an endomorphism of $A$. For, suppose that $\gamma \leq \delta < m$. Write $\gamma = \omega \cdot \alpha + \mu, \delta = \omega \cdot \beta + \nu$. If $\alpha < \beta$, then $g_f \gamma < g_f \delta$. If $\alpha = \beta$, then $g_f \gamma = g_f \delta$. Hence by (2), $g_f \in \text{End } A$.

Obviously $g_f \neq g$, if $f \neq f'$. This completes the proof.

**Theorem 6.** If $G$ is a group with $|G| \leq m$, then there is an algebra $A$ with $|A| = m, \text{Aut } A \cong G$, and $|\text{Sub } A| = |\text{End } A| = 2^m$. 
Proof. Let \( \mathcal{A} \) be as in Lemma 5, and let \( \mathcal{B} \) be an algebra with \( |\mathcal{B}| = m \) and \( \text{Aut} \mathcal{B} \cong \mathbb{G} \). We may assume that \( A \cap \mathcal{B} = 0 \) and \( (A \cup \mathcal{B}) \cap 2 = 0 \). Let \( C = A \cup B \cup 2 \). For \( f_i \), a fundamental operation of \( \mathcal{A} \), we define \( f_i^+ \) on \( C \):

\[
f_i^+ (x_0, \ldots, x_{m-1}) = \begin{cases} f_i (x_0, \ldots, x_{m-1}) & \text{if all } x_i \in A, \\ x_0 & \text{otherwise}. \end{cases}
\]

Similarly, the operations \( g_j \) of \( \mathcal{B} \) are extended to operations \( g_j^+ \) on \( C \). The algebra \( \mathcal{C} \) is to consist of all operations \( f_i^+, g_j^+ \), the distinguished elements 0, 1, and the following unary operation \( k \):

\[
k(x) = \begin{cases} 0 & x \in A \cup \{0\}, \\ 1 & x \in B \cup \{1\}. \end{cases}
\]

Clearly

1. If \( x \in \text{Sub} \mathcal{A} \), then \( x \cup \{0, 1\} \in \text{Sub} \mathcal{C} \).

Thus \( |\text{Sub} \mathcal{C}| = 2^m \).

Next, if \( h \) is an endomorphism of \( \mathcal{A} \), define for any \( x \in C \)

\[
h^+ x = \begin{cases} hx & x \in A, \\ x & x \in B \cup \{0, 1\}. \end{cases}
\]

It is easily checked that \( h^+ \) is an endomorphism of \( \mathcal{C} \). Thus \( |\text{End} \mathcal{C}| = 2^m \).

Now if \( h \) is an automorphism of \( \mathcal{B} \), define for any \( x \in C \)

\[
h' x = \begin{cases} hx & x \in B, \\ x & x \in A \cup \{0, 1\}. \end{cases}
\]

Then \( h' \) is an automorphism of \( \mathcal{C} \). Finally, we must show that any automorphism \( l \) of \( \mathcal{C} \) has the form \( h' \). Clearly \( l0 = 0 \) and \( l1 = 1 \). Suppose \( la = b \) with \( a \in A, b \in B \). Then

\[
l = kba = kla = 0 = n,
\]

a contradiction. Thus \( l^* A \subseteq A \). Similarly \( l^* B \subseteq B \), so \( l^* A = A \) and \( l^* B = B \). Now \( l \mid A \in \text{Aut} \mathcal{A} \), so \( l \mid A = \text{identity on } A \). Thus \( l \) has the form \( h' \).

Our final aim is to produce an algebra \( \mathcal{U} \) in which \( \text{Aut} \mathcal{U} \) and \( \text{Sub} \mathcal{U} \) are small while \( \text{End} \mathcal{U} \) is big.

Lemma 7. Let \( m \geq \aleph_0 \), and let \( n \) be minimal such that \( m^n > m \). Then there is an algebra \( \mathcal{U} \) such that \( |\mathcal{U}| = m, |\text{Aut} \mathcal{U}| = 1, |\text{End} \mathcal{U}| = m^n, \) and \( |\text{Sub} \mathcal{U}| = n \).

Proof. Let \( Y = \bigcup_{\alpha < n} \mathcal{U} \), let \( X \) be a set disjoint from \( Y \) with \( |X| = n \), and let \( A = X \cup Y \). For each \( \alpha < n \) we introduce an operation \( f_\alpha \) on \( A \). Let \( X = \{ x_\alpha : \alpha < n \} \) with \( x \) one-one. For all \( \alpha, \beta < n \) let \( f_\alpha x_\beta = x_{\alpha \beta} \). For any \( y \in Y \) let \( f_\alpha y = y \alpha \). In addition,
for any \( y \in Y \) introduce the constant operation \( g_y \) on \( A \) with value \( y \). Let \( \mathfrak{A} = \langle A, s, g_y \rangle_{y \in Y} \). The subalgebras of \( \mathfrak{A} \) are the empty set and all subsets of \( A \) of the form \( \{ x \in A : \beta \prec x \} \cup Y \), where \( \alpha \in \mathfrak{A} \). Thus \( |\text{Sub} \mathfrak{A}| = \mathfrak{A} \). It is easily seen that \( \mathfrak{A} \) has only the identity automorphism. Also, it is easily checked that the following are the only non-identity endomorphisms of \( \mathfrak{A} \). For \( ze^{=m} \), the following operation \( h_z \) on \( A : h_zx = z[x, h_z \text{ the identity on } Y] \). For \( \mathfrak{A}G \), \( \alpha \in \mathfrak{A} \), \( \alpha \prec \mathfrak{A} \), an operation \( h_{z\alpha} \) on \( A : h_{z\alpha}x = z[\alpha \cap \beta, h_{\alpha} \text{ the identity on } Y] \). Finally, for any \( \alpha \in \mathfrak{A} \) an operation \( h_{\alpha} \) on \( A : h_{\alpha}x = x_{\alpha, \beta}, h_{\alpha} \text{ the identity on } Y \). 

**Lemma 8.** Let \( m \geq \mathfrak{A} \), and let \( n \) be minimal such that \( m^n > m \). Let \( n \leq p \leq m \); then there is an algebra \( \mathfrak{A} \) such that \( |G| = m, |\text{Sub} \mathfrak{A}| = p, |\text{Aut} \mathfrak{A}| = 1 \), and \( |\text{End} \mathfrak{A}| = m^n \). 

**Proof:** The proof of Lemma 4 of [2], without the operation \( h \), easily gives the desired result (see the proof of Theorem 4 above).

**Theorem 9.** Let \( m \geq \mathfrak{A} \), let \( n \) be minimal such that \( m^n > m \), and let \( n \leq p \leq m \). Suppose \( \mathfrak{G} \) is a group such that \( |G| = m \). Then there is an algebra \( \mathfrak{A} \) such that \( |G| = m, |\text{Aut} \mathfrak{A}| = \mathfrak{G}, |\text{End} \mathfrak{A}| = m^n \), and \( |\text{Sub} \mathfrak{A}| = p \).

**Proof:** Let \( \mathfrak{A} \) be as in Lemma 8, and let \( \mathfrak{B} \) be an algebra such that \( |B| = m \), \( |\text{Aut} \mathfrak{B}| = \mathfrak{G} \), and \( |\text{Sub} \mathfrak{B}| = \mathfrak{B} \}. Form \( \mathfrak{C} \) by the process of the proof of Theorem 6. Obviously then \( |\text{Aut} \mathfrak{C}| = \mathfrak{G} \) and \( |\text{Sub} \mathfrak{C}| = p \). The endomorphisms of \( \mathfrak{C} \) are as follows. For \( h \) an endomorphism of \( \mathfrak{A} \), let \( h(x) = \begin{cases} hx & \text{if } x \in A, \\ 0 & \text{if } x = 0, \\ 1 & \text{if } x \in B \cup \{0\}. \end{cases} \) Then \( h^* \) is an endomorphism of \( \mathfrak{C} \). Similarly define \( l^* \) for \( l \in \text{End} \mathfrak{B} \). Finally, for \( h \in \text{End} \mathfrak{A}, l \in \text{End} \mathfrak{B} \) define \( (h, l)^* = \begin{cases} hx & \text{if } x \in A, \\ x & \text{if } x \in \{0, 1\}, \\ lx & \text{if } x \in B. \end{cases} \) The maps \( l^* \) and \( (h, l)^* \) are also endomorphisms of \( \mathfrak{C} \). To see that any endomorphism of \( \mathfrak{C} \) is of one of these forms, the only hard step is to check the following statement:

1. If \( a \in \text{End} \mathfrak{C} \) and \( ax = 0 \) for some \( a \in A \), then \( ax = x \) for all \( x \in A \). 

The proof of this statement relies on the particular construction of \( \mathfrak{A} \). In fact, let \( R = \{(x, y) \in A : x = y \text{ for some operation } t \text{ of } \mathfrak{A}, tx = y \text{ or } ty = x \} \). Then (1) follows from the following two easily checked statements:

2. \( A \) is the transitive closure of \( R \);

3. If \( ax = 0 \), then \( ay = 0 \).

The main theorem of this note now follows:
THEOREM 10. Assume GCH. Let $m$, $n$, $p$, $q$ be cardinals such that $m \geq \aleph_0$ and $q > 1$. Then the following conditions are equivalent:

(i) there is an algebra $\mathcal{A}$ such that $|\mathcal{A}| = m$, $|\text{Aut} \mathcal{A}| = n$, $|\text{End} \mathcal{A}| = p$, and $|\text{Sub} \mathcal{A}| = q$;

(ii) one of these conditions holds:

(1) $1 \leq n \leq p \leq m$ and $q \leq m^+$,

(2) $1 \leq n \leq p = m^+$ and $\cf m \leq q \leq m^+$.

REFERENCES


Eidgenössische Technische Hochschule
Zürich
Switzerland

and

University of Colorado
Boulder, Colorado
U.S.A.