NON-CONSTRUCTIVE PROPERTIES OF CARDINAL NUMBERS

BY

JEAN E. RUBIN*

ABSTRACT

Let Σ be some standard set theory (Eg. Zermelo Fraenkel or Von Neumann-Bernays-Godel) which does not contain the axiom of choice. Using Σ as the underlying set theory, we shall study operations on infinite cardinals, closely related to exponentiation, and compare the results with known results about exponentiation.

Introduction

Let Σ be some standard set theory (Eg. Zermelo-Fraenkel or Von Neuman-Bernays-Gödel) which does not contain the axiom of choice. Using Σ as the underlying set theory, we shall study operations on infinite cardinals, closely related to exponentiation, and compare the results with known results about exponentiation.

The paper is divided into three sections. The first contains notation and preliminary remarks; the second is based on the work of Tarski [7], [18], and [19]; and the third is based on the work of Specker [14] and Kruse [5] and [6].

1. We assume the reader is familiar with the standard notation of set theory. In particular we shall use the following notation:
$M \precsim N$ iff there is a 1-1 function mapping M into N. ($|M| \leqq |N|$).

$E(M)$ is the set of all finite subsets of M. If $|M| = m$ then, $|E(M)| = e(m)$.
$\aleph(M) = \{\alpha \mid \alpha \text{ is an ordinal number and } \alpha \precsim M\}$.

* I should like to take this opportunity to thank both my husband, Herman and my son, Arthur, for their help in preparing this paper.

Received February 9, 1971 and in revised form June, 24, 1971.

If $|M| = m$, $|\aleph(M)| = \aleph(m)$. (Hartog's aleph.)

$M \precsim^* N$ if $M = \varnothing$ or there is a function mapping N onto M.

If $|M| = m$ and $|N| = n$ then $m \leqq^* n$ iff $M \precsim^* N$.

We shall also assume the following properties of $\leqq^*$, $\aleph$, and e. (See [7] and [3]).

THEOREM 1.1.

(a) *If* $m \leqq n$ *then* $m \leqq^* n$.

(b) *If* $m \leqq^* n$ *then* $2^m \leqq 2^n$.

(c) *If* m *is infinite,* $\aleph(m)$ *is the smallest aleph which is not* $\leqq$ *to* m.

(d) If m and n *are infinite then,*

$$\aleph(m+n) = \aleph(m) + \aleph(n) = \aleph(m \cdot n) = \aleph(m) \cdot \aleph(n).$$

(e) *If* m *is infinite,* $\aleph(m^2) = \aleph(m)$.

(f) $\aleph(m) \leqq^* 2^{m^2}$.

(g) $\aleph(m) \leqq^* 2^{2^m}$.

(h) $\aleph(\aleph_\alpha) = \aleph_{\alpha+1}$.

(i) $\aleph_{\alpha+1} \leqq^* 2^{\aleph_\alpha}$.

(j) $m \leqq e(m) \leqq 2^m$.

(k) $e(\aleph_0) = \aleph_0$.

(l) $e(m+n) = e(m) \cdot e(n)$.

(m) $\aleph_0 \cdot e(m) = \aleph_0 \cdot e(km)$, for all $k \in \omega \sim \{0\}$, *provided that every set with cardinal number* m *can be linearly ordered.*

Moreover, we shall assume familiarity with the standard Cohen models of set theory in which the axiom of choice is false [2] pp. 136–142. (Alternatively, the Fraenkel-Mostowski model [9].) Specifically, we shall use the following properties.

THEOREM 1.2. *If* Σ *is consistent, there exists a model of* Σ *in which every set can be linearly ordered and there is an infinite cardinal number* m *with the following properties*:

(a) $\aleph_0 \nleqq^* m$. (Consequently, $\aleph_0 \nleqq m$.)

(b) $2m \nleqq m + \aleph_0$.

(c) $2m^2 \nleqq m^2 + \aleph_0 \cdot m$.

(d) $m + \aleph_0 < 2m + \aleph_0 < 3m + \aleph_0 < \cdots$.

(e) $\aleph_0 \cdot m < \aleph_0 \cdot m^2 < \aleph_0 \cdot m^3 < \cdots$.

PROOF. We obtain the model by adding the following sets to the Cohen hierarchy (see [2] p. 142):

$A = \{a_{mn} \mid m, n \in \omega\}$, the a_{mn} are generic subsets of ω,

$A_m = \{a_{mn} \mid n \in \omega\}$,

$M = \{A_m \mid m \in \omega\}$,

$N = \{\{A_m, A_n\} \mid m, n \in \omega\}$, and

R is a linear ordering of M of type η, the order type of the rationals.

Let $|M| = m$. Then it is easy to show that if $\aleph_0 \leqq^* m$ then $\aleph_0 \leqq m$. But using Cohen's method, it can be shown that the latter property implies a contradiction.

Parts (d) and (e) follow from (b) and (c) respectively, and (b) and (c) follow from (a) and the definition of m.

Now, let $LO(m)$, $INF(m)$ and $AC(e(m))$ be the following three statements:

$LO(m)$: Every set with cardinal number m can be linearly ordered. (The ordering principle).

$INF(m)$: There exists infinite cardinals p and q such that $m = p + q$.

$AC(e(m))$: There is a choice function on $E(M)$, for all sets M of cardinality m.

It is known that if Σ is consistent neither of these three propositions are provable. (To see this, omit the sets N and R in the construction of the model in the Proof of 1.2.) It is also easy to show that $\aleph \leqq^* m$ implies $INF(m)$, $LO(m)$ implies $AC(e(m))$, and if m is infinite, $LO(m)$ implies $INF(m)$. In Sections 2 and 3 we use $LO(m)$ in the hypotheses of theorems where it would have been sufficient to use $AC(e(m))$. (Referee's comment) see Lemma 2.6 ff.

The following theorem is due to Tarski and Kuratowski [15] and [7].

THEOREM 1.3. $\aleph_0 \leqq^* m$ iff $\aleph_0 \leqq 2^m$.

PROOF. It follows from 1.1 (b) that if $\aleph_0 \leqq^* m$ then $\aleph_0 \leqq 2^m$. The proof the other way is given in [15] pp. 94–95.

The following implications clearly hold for all $m > 0$.

$$m = 2m \rightarrow (2^m)^2 = 2^m$$

$$\aleph_0 \leqq m \rightarrow 2 \cdot 2^m = 2^m.$$

But, if Σ is consistent, the arrows do not go the other way. The proof of this depends on the following result of Lauchli [8].

THEOREM 1.4. *If m is infinite then* $(2^{e(m)})^{\aleph_0} = 2^{e(m)}$.

There exist models of Σ in which $e(m)$ is infinite but $\aleph_0 \nleqq e(m)$, [2].

2. We now make the following definitions.

DEFINITION 2.1. If $|M| = m$ and $|N| = n$,

(a) $M^{(N)} = \{f \mid f : N \precsim M\}$; $|M^{(N)}| = m^{(n)}$.

(b) $N^{[N]} = \{u \subseteq M \mid |u| = n\}$; $|M^{[N]}| = m^{[n]}$.

(c) $M^{\langle N\rangle} = \{u \subseteq M \mid |u| < n\}$; $|M^{\langle N\rangle}| = m^{\langle n\rangle}$.

(d) $M^{\langle\langle N\rangle\rangle} = \{u \subseteq M \mid |u| \leqq n\}$; $|M^{\langle\langle N\rangle\rangle}| = m^{\langle\langle n\rangle\rangle}$.

M^N is the set of all functions mapping N into M ($|M^N| = m^n$), while $M^{(N)}$ is the set of all 1-1 functions mapping N into M.

The following lemma follows easily from 2.1.

LEMMA 2.2.

(a) $M^{[N]} \cup M^{\langle N\rangle} = M^{\langle\langle N\rangle\rangle}$

(b) $M^{(N)} \subseteq M^N$

(c) $M^{\langle\langle M\rangle\rangle} = \mathscr{P}(M)$

(d) *If* $M_1 \precsim M_2$ *then* $M_1^{(N)} \precsim M_2^{(N)}$, $M_1^{[N]} \precsim M_2^{[N]}$, $M_1^{\langle N\rangle} \precsim M_2^{\langle N\rangle}$, *and* $M_1^{\langle\langle N\rangle\rangle} \precsim M_2^{\langle\langle N\rangle\rangle}$.

First, we shall study these pseudo-exponentiation operations for the case that the exponent is finite. We have defined $E(M)$ to be the set of all finite subsets of M. We shall define $F(M)$ to be the set of all finite sequences of elements of M without repetition and $FF(M)$ to be the set of all finite sequences of elements of M.

DEFINITION 2.3. If $|M| = m$,

(a) $F(M) = \bigcup_{i \in \omega} M^{(i)}$, where $M^{(0)} = \{\varnothing\}$; $|F(M)| = f(m)$.

(b) $FF(M) = \bigcup_{i \in \omega} M^i$, where $M^0 = \{\varnothing\}$; $|FF(M)| = ff(m)$.

Some of the following results can be found in Ellentuck [3].

LEMMA 2.4. *If* $m > 0$,

(a) $ff(m) = ff(ff(m)) = \aleph_0 \cdot ff(m)$.

(b) $ff(m) = \aleph_0 \cdot e(m)$.

PROOF. Ellentuck [3] p. 246.

LEMMA 2.5. *If m is infinite, then* $m^k \leqq f(m)$ *for all* $k \in \omega$.

PROOF. Let $|M| = m$. The lemma is true if $k = 0$ so suppose $1 \leqq k \in \omega$. Let v_{ij}, w_{ij}, $1 \leqq i \leqq k$, $1 \leqq j \leqq 2k$ be $4k^2$ distinct elements of M and let $u = \langle u_1, u_2, \cdots, u_k\rangle$ be any element of M^k. Suppose $u_1, u_2, \cdots, u_{j-1}$ are all distinct and $u_j = u_i$ for $1 \leqq i < j \leqq k$. Then replace u_j by the first v_{il}, $l = 1, 2, \cdots, 2k$, which is distinct from $u_1, u_2, \cdots, u_k$. Let w_{il_1} be the first w_{il}, $l = 1,2,\cdots,2k$, which is distinct from $u_1, u_2, \cdots, u_k$.

Suppose the next repetition occurs at the j_1-st coordinate and suppose i_1 is the smallest i so that $u_i = u_{j_1}$, $1 \leqq i < j_1 \leqq k$. Replace u_{j_1} by the first $v_{i_1,l}$, $l = 1,2,\cdots,2k$, which is distinct from $u_1, u_2, \cdots, u_k$ and let w_{j_1,l_2} be the first $w_{j_1 l}$, $l = 1,2,\cdots,2k$, which is distinct from $u_1, u_2, \cdots, u_k$. Continue this process until all repetitions are eliminated.

Let us illustrate what is going on by an example. Suppose $k = 5$ and $u = \langle v_{11}, w_{11}, v_{11}, v_{11}, w_{11} \rangle$. Then we shall map u onto the element $\langle v_{11}, w_{11}, v_{12}, v_{13}, v_{21}, w_{31}, w_{41}, w_{51} \rangle$. The element $\langle v_{11}, w_{11}, v_{11}, v_{11}, v_{21} \rangle \in M^k$ would be mapped on $\langle v_{11}, w_{11}, v_{12}, v_{13}, v_{21}, w_{31}, w_{41} \rangle$. So the first subscript on the w's tells us which coordinates have been replaced and the first subscript on the v's tells us which element was there originally. Thus we have constructed a 1-1 mapping of M^k into $F(M)$.

In many of the following theorems we assume $LO(m)$ in the hypothesis. A typical way in which it is used is illustrated in the following.

LEMMA 2.6. $LO(m) \to (\forall k \in \omega) m^{[k]} \leqq m^{(k)}$.

PROOF. The conclusion holds without $LO(m)$ if $m \leqq 1$ or $k \leqq 1$. So suppose both m and k are greater than 1. Suppose $|M| = m$ and let $u = \{u_1, u_2, \cdots, u_k\} \in M^{[k]}$. Suppose R is a linear ordering of M and suppose also

$$u_1 R u_2 R \cdots R u_k.$$

Then define $\phi(u) = \langle u_1, u_2, \cdots, u_k \rangle$. It is easy to see that ϕ is a 1-1 mapping of $M^{[k]}$ into $M^{(k)}$.

Alternatively, to prove the lemma we could have used $AC(e(m))$ to define $\phi(u)$. For each $u \in M^{[k]}$ let

$$\psi_1(u) \in u,\ \psi_2(u) \in u \sim \{\psi_1(u)\},\ \cdots,\ \psi_k(u) \in u \sim \{\psi_1(u), \cdots, \psi_{k-1}(u)\}.$$

Then let $\phi(u) = \langle \psi_1(u), \cdots, \psi_k(u) \rangle$. Thus, $LO(m)$ is used as a substitute for $AC(e(m))$.

LEMMA 2.7. $LO(m) \to (\forall k \in \omega) LO(m^{[k]})$.

PROOF. Suppose $|M| = m$, then $M^{[k]}$ can be linearly ordered, for example, by the lexicographical ordering.

THEOREM 2.8. *If $LO(m)$ then each of the following are equivalent.*

(1) $\aleph_0 \leqq m$

(2) $e(m) = f(m)$

(3) $e(m) = ff(m)$.

PROOF. Using 2.2(b) and 2.6, it is easy to show that $(3) \to (2)$. Clearly, $e(m) \leqq e(m) + 1 \leqq f(m)$. Thus, (2) implies $\aleph_0 \leqq e(m)$, and this along with $LO(m)$ implies (1). Finally (1) implies

$$\begin{aligned} e(m) &= e(m + \aleph_0) & \\ &= \aleph_0 \cdot e(m) & \text{1.1(k)(1)} \\ &= ff(m). & \text{2.4(b)} \end{aligned}$$

Therefore, $(1) \to (3)$.

Without using $LO(m)$ we can prove the following:

THEOREM 2.9. *If $1 < k < \omega$ then the following are equivalent.*

(1) $\aleph_0 \leqq m$

(2) $m^k = m^{(k)}$ *and* $m > 1$.

PROOF. Suppose $\aleph_0 \leqq m$. Then it is easy to show that

$$m^{(k)} \leqq m^k \leqq (m + \aleph_0)^{(k)} = m^{(k)}$$

(See Ellentuck [3] p. 255.) Thus $(1) \to (2)$.

Conversely, suppose (2) holds. Then, since $m^{(k)} \leqq m^{(k)} + 1 \leqq m^k$, it follows from (2) that $\aleph_0 \leqq m^{(k)}$. But this implies $\aleph_0 \leqq m$.

LEMMA 2.10. $\aleph_0 \nleqq m \to (\forall k \in \omega) m^k = \sum_{j=1}^{k} s_{jk} m^{(j)}$, *where the s_{jk} are Stirling numbers*

$$s_{jk} = \frac{j^k}{j!} \sum_{i=0}^{j} (-1)^i \frac{j!}{i!(j-1)!} \left(\frac{j-i}{j}\right)^k$$

PROOF. For a proof of this for finite m see, for example, Harris [4] pp. 25–26. The proof is essentially the same for infinite m.

LEMMA 2.11. *If $j, k \in \omega$ and $m \geqq jk + j + k$ then $j \cdot m^{[k]} \leqq m^{[k+1]}$, provided that $j, k \neq 0$.*

PROOF. Suppose $|M| = m$ and $u \subseteq M$ with $|u| = q$, where $q = jk + j + k$. For all $i \leqq q$,

$$q^{[i]} = \frac{q!}{i!(q-i)!}.$$

Thus, if $i \leqq k$, $j \cdot q^{[i]} \leqq q^{[i+1]}$, provided that $j \neq 0$. Therefore, for each $i \leqq k$ there are j functions $\phi_{i1}, \phi_{i2}, \cdots, \phi_{ij}$ such that for each l, $1 \leqq l \leqq j$, ϕ_{il} is 1-1, $\mathscr{D}(\phi_{il}) = u^{[i]}$, $\mathscr{R}(\phi_{il}) \subseteq u^{[i+1]}$, and if $1 \leqq j_1 < j_2 \leqq k$ then

$$\mathscr{R}(\phi_{ij_1}) \cap \mathscr{R}(\phi_{ij_2}) = \varnothing.$$

Now we can construct j 1-1 functions from $M^{[k]}$ to $M^{[k+1]}$ with pair-wise disjoint ranges as follows: let $X \in M^{[k]}$. Suppose $v = X \cap u$ and $|v| = i$. Define,

$$\Psi_l(X) = \phi_{il}(v) \cup (u \sim v).$$

Then it follows from the definition of ϕ_{il} that for each l, $1 \leqq l \leqq j$, $\mathscr{D}(\Psi_l) = M^{[k]}$ $\mathscr{R}(\Psi_l) \subseteq M^{[k+1]}$, Ψ_l is 1-1, and the Ψ_l's have pairwise disjoint ranges.

COROLLARY 2.12. *If m is infinite then for all $j, k \in \omega$, $jm^{[k]} \leqq m^{[k+1]}$.*

LEMMA 2.13. *$LO(m) \to (\forall k \in \omega) m^{(k)} = k! \cdot m^{[k]}$.*

PROOF. Ellentuck [3] p. 254.

LEMMA 2.14. *If m is infinite then $LO(m) \to (\forall k \in \omega) m^k \leqq m^{[k+1]}$.*

PROOF. If $\aleph_0 \leqq m$, by 2.9, $m^k = m^{(k)}$. By 2.13, $m^{(k)} = k! m^{[k]}$. Thus, the desired result follows from 2.12.

If $\aleph_0 \nleqq m$, by 2.10

$$\begin{aligned} m^k &= \sum_{j=1}^{k} s_{jk} m^{(j)} \\ &= \sum_{j=1}^{k} s_{jk} j! \, m^{[j]} \qquad [2.13] \end{aligned}$$

Therefore, it follows from 2.12 that there is an $l \in \omega$ such that $m^k \leqq l m^{[k]} \leqq m^{[k+1]}$.

COROLLARY 2.15. *If m is infinite then $LO(m) \to (\forall k \in \omega) m^k \leqq e(m)$.*

THEOREM 2.16. *If $LO(m)$, $m > 1$, and $1 < k \in \omega$ then each of the following are equivalent:*

(1) $m^k = 2m^k$

(2) $m^{(k)} = 2m^{(k)}$

(3) $m^{[k]} = 2m^{[k]}$

(4) $m^{(k)} = m^{[k]}$

(5) $m^k = m^{[k]}$.

PROOF. First we note that (1) and (2) are equivalent because they each imply $\aleph_0 \leqq m$ which, by 2.9, implies $m^k = m^{(k)}$. (Thus the equivalence of (1) and (2) does not depend on the assumption $LO(m)$).

The fact that (2) and (3) are equivalent follows from 2.13 and the Tarski cancellation laws. ([7] p. 305 and [19]. If $1 \leqq k < \omega$ then for all cardinals m and n if $km = kn$ then $m = n$.)

To prove (5) → (4) → (3) → (5) use 2.6, 2.2(b), 2.13, and 2.9.

THEOREM 2.17. *If $LO(m)$, m is infinite, and $k \in \omega$ then each of the following are equivalent.*

(1) $m^k = m^{k+1}$

(2) $m^{(k)} = m^{(k+1)}$

(3) $m^{[k]} = m^{[k+1]}$

(4) $e(m) = m^k$.

PROOF. The proof that (1) and (2) are equivalent is similar to the proof that (1) and (2) of 2.16 are equivalent and again does not use $LO(m)$.

Suppose (2) holds. Then it follows from the monotonicity laws that for all j such that $1 \leqq j \in \omega$,

$$\text{(I)} \qquad m^{(k)} = j \cdot m^{(k)}.$$

By 2.13, we obtain from (2),

$$k! \cdot m^{[k]} = (k+1)! \cdot m^{[k+1]}$$

which implies, using (I) that

$$(k+1)! \cdot m^{[k]} = (k+1)! \cdot m^{[k+1]}.$$

Thus (3) is obtained by using Tarski's cancellation law.

Before proving (3) implies (4) it is convenient to prove first that (3) implies (2) thus showing (1), (2) and (3) are all equivalent. First, we note that (3) implies that for all i, j, $1 \leqq i, j \in \omega$,

$$\text{(II)} \qquad i \cdot m^{[k]} = j \cdot m^{[k]}.$$

Thus,

$$\begin{aligned} (k+1)! \cdot m^{[k+1]} &= (k+1)! \cdot m^{[k]} && (3) \\ &= k! \cdot m^{[k]} && (\text{II}) \end{aligned}$$

Therefore (2) follows from (2.13).

By 2.15, $m^k \leqq e(m)$ for all $k \in \omega$. We shall show that (1) implies $e(m) \leqq m^k$. It follows from (1) that $m^k = m^{k+j}$ for all $j \in \omega$. Since (1) and (3) are equivalent, it follows that $m^{[k]} = m^{[k+j]}$ for all $j \in \omega$. Therefore,

$$\begin{aligned} e(m) &\leqq 1 + m + m^{[2]} + \cdots + \aleph_0 m^{[k]} \\ &= 1 + m + m^{[2]} + \cdots + m^{[k]} \\ &\leqq (k+1) m^{[k]} && [2.12] \\ &= m^{[k]} && (3) \\ &= m^k && [2.16]. \end{aligned}$$

Finally, it follows from 2.15 that $m^k \leqq m^{k+1} \leqq e(m)$. Thus, it is easy to see that (4) implies (1).

COROLLARY 2.18. *If $LO(m)$, m is infinite, and $k \in \omega$ then each of the following are equivalent*:

(1) $m^k = m^{k+1}$

(2) $e(m) = m^{(k)}$

(3) $e(m) = m^{[k]}$.

In Σ we can prove the following:

$$m^{k+l} = m^k \cdot m^l$$

$$(m^k)^l = m^{kl}.$$

The question arises whether we can prove similar laws for the other types of exponentiation defined in 2.1. The following theorems answer these questions in part.

THEOREM 2.19. *If $LO(m)$, m is infinite and $0 < k$, $l \in \omega$ then each of the following are equivalent.*

(1) $m^{k+l} = m^{[k+l]}$

(2) $m^{[k+l]} = m^{[k]} \cdot m^{[l]}$.

PROOF. It follows immediately from $LO(m)$ that $m^{[k+l]} \leqq m^{[k]} \cdot m^{[l]}$. We shall show (1) $\rightarrow m^{[k]} \cdot m^{[l]} \leqq m^{[k+l]}$. (1) implies

$$m^{[k+l]} = m^{k+l} = m^k \cdot m^l.$$

By 2.6,

$$m^{[k]} \cdot m^{[l]} \leqq m^k \cdot m^l.$$

Thus (1) $\rightarrow$ (2).

Conversely, suppose (2) holds. Let $|M| = m$ and let $u = \{u_1, u_2, \cdots, u_k, v_1, v_2, \cdots, v_l\} \subseteq M$, and $|u| = k + l$. Suppose R linearly orders M and $u_1 R u_2 R \cdots R u_k R v_1 R v_2 R \cdots R v_l$. Define

$$\phi_1(u) = \langle \{u_1, u_2, \cdots, u_k\}, \{v_1, v_2, \cdots, v_l\} \rangle$$

$$\phi_2(u) = \langle \{v_1, u_2, \cdots, u_k\}, \{u_1, v_2, \cdots, v_l\} \rangle.$$

Then ϕ_1 and ϕ_2 are each 1-1 mappings of $M^{[k+l]}$ into $M^{[k]} \times M^{[l]}$ and $\mathscr{R}(\phi_1) \cap \mathscr{R}(\phi_2) = \varnothing$. Thus

$$2m^{[k+l]} \leqq m^{[k]} \cdot m^{[l]}.$$

Therefore, (2) implies $m^{[k+l]} = 2m^{[k+l]}$, which, by 2.16, implies (1).

THEOREM 2.20. *If $LO(m)$, m is infinite and $1 < k$, $l \in \omega$ then each of the following are equivalent:*

(1) $m^{kl} = m^{[kl]}$

(2) $m^{[kl]} = (m^{[k]})^{[l]}$

(3) $m^{[kl]} = (m^{[k]})^{(l)}$

(4) $m^{[kl]} = (m^{(k)})^{[l]}$

(5) $m^{[kl]} = (m^{[k]})^{l}$

(6) $m^{[kl]} = (m^{k})^{[l]}$

We shall omit the proof of this theorem and the next since the techniques used are similar to those used previously.

THEOREM 2.21. *If m is infinite and $1 < k$, $l \in \omega$ then each of the following are equivalent.*

(1) $\aleph_0 \leqq m$

(2) $m^{(k+l)} = m^{(k)}m^{(l)}$

(3) $m^{(kl)} = (m^{(k)})^{(l)}$.

It is easy to obtain similar results for $m^{\langle k \rangle}$ and $m^{\langle\langle k \rangle\rangle}$, but instead we shall discuss pseudo-exponentiation when the exponent is infinite.

LEMMA 2.22. *If M is a set and S a hereditary system of subsets of M, (S is called hereditary if every subset of an element of S is an element of S), then if $|S| \leqq |M|$, there is a subset $N \subseteq M$ such that N can be well-ordered and $N \notin S$.*

PROOF. Tarski [18], p. 178. We shall sketch the proof here because we want to generalize the lemma slightly and use essentially the same proof.

Let ϕ be a 1-1 function mapping S into M. Define a function Ψ on the class of ordinals such that for each ordinal α,

$$\Psi(\alpha) = \begin{cases} \phi(\Psi''\alpha) & \text{if } \Psi''\alpha \in S \\ u \notin M & \text{otherwise.} \end{cases}$$

Let γ be the smallest ordinal number δ such that $\Psi(\delta) = u$. Then since ϕ is 1-1, $\Psi \mid \gamma$ is 1-1, so $\Psi''\gamma$ is a subset of M which can be well-ordered and $\Psi''\gamma \notin S$.

Let us call a system of sets "almost hereditary" if every well-ordered subset of an element is an element. Then using the same proof as of 2.22 we can prove,

COROLLARY 2.23. *If M is a set and S an almost hereditary system of subsets* *of M, then if $|S| \leqq |M|$, there is a subset $N \subseteq M$ such that N can be well-ordered and $N \notin S$.*

The following theorem follows from 2.22.

THEOREM 2.24. *If $m > 1$ then*

(a) *If $n > 2$ and $m^{\langle n \rangle} = m$ then there is an aleph, $\aleph$, such that $\aleph \leqq m$ and $\aleph \nless n$.*

(b) *If $n \geqq 2$ and $m^{\langle\langle n \rangle\rangle} = m$ then there is an aleph, $\aleph$, such that $\aleph \leqq m$ and $\aleph \nleqq n$. (See 2.13 for the definition of $m^{\langle n \rangle}$ and $m^{\langle\langle n \rangle\rangle}$.)*

COROLLARY 2.25. *If $m > 1$ and $m^{\langle m \rangle} = m$ then m is an aleph.*

We shall next consider the relationship between m^n, $m^{(n)}$, $m^{[n]}$, $m^{\langle n \rangle}$, and $m^{\langle\langle n \rangle\rangle}$.

THEOREM 2.26. *If $m = m^2$ and $0 < n \leqq m$ then $m^n \leqq m^{[n]}$.*

PROOF. It follows from the hypothesis that $m = m \cdot n$. Let $|M| = m$ and $|N| = n$. Then there is a 1-1 function ϕ such that

$$\phi: M \times N \approx M.$$

If $f \in M^N$, define

$$\Psi(f) = \{\phi(f(u), u) \mid u \in N\}$$

For each $f \in M^N$, $\Psi(f) \subseteq M$ and $|\Psi(f)| = n$. Moreover, Ψ is 1-1. Therefore, $m^n \leqq m^{[n]}$.

In the case that n is finite in 2.26, "$m = m^2$" can be replaced by "$m = 2m$", because in this case $m = 2m$ implies $m = n \cdot m$.

COROLLARY 2.27. *If $0 < m = 2m$ and $0 < n \in \omega$ then $m^n \leqq m^{[n]}$.*

COROLLARY 2.28. *If m is infinite and $n \in \omega$ then $m^{[n]} = m \to m^n = m$.*

PROOF. The corollary is true if $n = 0, 1$. Suppose $1 < n \in \omega$. By 2.12, $2m \leqq m^{[n]}$. Consequently, $m^{[n]} = m$ implies $m = 2m$. So, by 2.27, $m^n \leqq m^{[n]}$. Therefore, $m^{[n]} = m$ implies $m^n = m$.

THEOREM 2.29. *If m is an aleph and $0 < n \leqq m$ then $m^{[n]} \leqq m^{(n)}$.*

PROOF. Suppose $|M| = m$, $N_0 \subseteq M$, and $|N_0| = n$. Let N be any subset of M such that $|N| = n$. Define $\phi(N) = f \in M^{(N_0)}$ where $f: N_0 \approx N$ and f preserves order. Then ϕ is a 1-1 function mapping $M^{[N]}$ into $M^{(N)}$. (See [11] Theorem 7.4.5).

THEOREM 2.30. *If m is an aleph and $0 < n \leqq m$ then $m^n = m^{(n)} = m^{[n]}$.*

PROOF. 2.26, 2.29 and 2.2 (b).

THEOREM 2.31. *If m is an aleph and $0 < n \leqq m$ then $m^{\langle n\rangle} \leqq m^{n}$.*

PROOF. Let $|M| = m$, $|N| = n$ and suppose $P \subseteq M$, $|P| = p < n$. Then $P \precsim N$. Let N' be the smallest initial segment of N such that $P \approx N'$. Let f' be the 1-1 function which maps N' onto P and preserves order. For $u \in N \sim N'$ define $f(u) = u_0$ where $u_0 \in P$. Let $\Psi(P) = f \cup f'$. Then Ψ is a 1-1 function mapping $M^{\langle N\rangle}$ into M^{N}.

In the case that n is finite, we may replace "m is an aleph" in the hypothesis of 2.31 by "$LO(m)$".

COROLLARY 2.32. *If $LO(m)$, $n \in \omega$ and m is infinite then $m^{\langle n\rangle} \leqq m^{n}$.*

THEOREM 2.33. *If m is an aleph and $0 < n \leqq m$ then*

$$m^{n} = m^{(n)} = m^{\langle\langle n\rangle\rangle} = m^{[n]}.$$

PROOF. By 2.30

$$\text{(I)} \qquad m^{n} = m^{(n)} = m^{[n]}.$$

By 2.2 (a), $m^{\langle\langle n\rangle\rangle} = m^{\langle n\rangle} + m^{[n]}$. So

$$\text{(II)} \qquad m^{[n]} \leqq m^{\langle\langle n\rangle\rangle}.$$

By 2.31, $m^{\langle n\rangle} \leqq m^{n}$; by 2.29, $m^{[n]} \leqq m^{(n)}$; and by 2.2 (b) $m^{(n)} \leqq m^{n}$. So,

$$\text{(III)} \qquad m^{\langle\langle n\rangle\rangle} \leqq m^{n} + m^{n} = m^{n}.$$

The theorem follows from (I), (II), and (III).

In the case the exponent is finite we get the following result.

THEOREM 2.34. *If $0 < m = 2m$, $LO(m)$, and $n \in \omega$ then*

$$m^{n} = m^{(n)} = m^{\langle\langle n\rangle\rangle} = m^{[n]}.$$

PROOF. 2.16, 2.32, and 2.2 (a).

A special case of the following lemma was originally proved by the author (see 2.36) but subsequently the lemma was generalized by H. Rubin. We shall give the more general result here.

Lemma 2.35. *If $\aleph_0 \cdot p \leqq n \leqq m$ then $m^{[p]} \leqq m^{[n]}$.*

PROOF. Suppose $|M| = m$, $N \subseteq M$, $|N| = n$, and $|R| = p$. Suppose also that

$$M = (R \times \omega) \cup Q \cup T, \; N = (R \times \omega) \cup Q$$

where the sets $R \times \omega$, Q, and T are pairwise disjoint. For any $\langle u, k\rangle \in R \times \omega$ let $f(u, k) = \langle u, 2k\rangle$ and let ω' be the set of all odd natural numbers.

Let P be any subset of M such that $|P| = p$. Define

$$\phi(P) = (P \cap T) \cup (Q \sim P) \cup (R \times \omega') \cup (f''P \cap (R \times \omega)).$$

It is easy to see that $\phi(P) \subseteq M$ and ϕ is 1-1. To complete the proof we must show $|\phi(P)| = n$. First, $|\phi(P)| \leqq n$ because $|P \cap T| \leqq p$, $|Q \sim P| \leqq |Q|$, $|R \times \omega'| = \aleph_0 \cdot p$, and $|f''P \cap (R \times \omega)| \leqq \aleph_0 \cdot p$. Therefore,

$$|\phi(P)| \leqq p + |Q| + \aleph_0 p + \aleph_0 p = \aleph_0 \cdot p + |Q| = n.$$

On the other hand, $\phi| (P) | \geqq n$ because $|(Q \sim P) \cup (R \times \{1\}| \geqq |Q|$ and $|R \times (\omega' \sim \{1\})| = \aleph_0 p$.

Corollary 2.36. *If $p \leqq n \leqq m$ and either p is finite and $\aleph_0 \leqq n$,* or *p is an aleph then $m^{[p]} \leqq m^{[n]}$.*

The following theorem is stated in Tarski [18] without proof. As far as we know the proof has not been published.

Theorem 2.37. *If $m > 1$, $n \geqq \aleph_0$ and $m^{[n]} = m$ then there is an aleph, $\aleph$, such that $\aleph \leqq m$ but $\aleph \nleqq n$.*

Proof. It follows from the hypothesis and 2.36 that $m^{[p]} = m$ for all $p \leqq n$ such that $1 \leqq p < \omega$ or p is an aleph. In particular, $m^{[2]} = m$. By 2.12, $2m \leqq m^{[2]}$. Thus $m = 2m$, so by 2.27, $m^2 \leqq m^{[2]}$. This implies $m = m^2$.

Now it follows that

$$S = \{P \subseteq M| \ |P| \leqq n \,\&(|P| < \omega \text{ or } |P| \text{ is an aleph})\}$$

is an almost hereditary system of subsets of M such that $|S| = m$. (Because if $P \in S$ and $|P| = p$, $m^{[p]} = m$; so $|S| = m$ follows from the fact that $m^2 = m$.) Therefore it follows from 2.23 that there is a subset $A \subseteq M$ such that A can be well ordered and $A \notin S$. Thus, $|A|$ is an aleph such that $|A| \nleqq n$ and $|A| \leqq m$.

Corollary 2.38. *If $m > 1$, $n \geqq \aleph_0$ and $m^{[n]} = m$ then $m^n = m$*

Proof. In the proof of 2.37 we showed that under the given hypothesis, $m = m^2$. Thus the corollary follows from 2.26.

Corollary 2.39. *If $m > 1, 0 < n = 2n$, and $m^{[n]} = m$ then $m^{\langle n \rangle} = m$ and $m^{\langle\langle n \rangle\rangle} = m$.*

Proof. Suppose $n = 2n$ and $p \leqq n$. Then it is easy to see that $m^p \leqq m^{[2n]} = m^{[n]} = m$. (See the proof of 2.35 and of 2.37.) Thus, for all $p \leqq n$, $m^{[p]} = m$ and $m = m^2$. Therefore, $m^{\langle n \rangle} = m$ and $m^{\langle\langle n \rangle\rangle} = m$.

The following theorem follows directly from the definition of $m^{[m]}$.

Theorem 2.40. $\aleph_0 \leqq m \leftrightarrow m^{[m]} > 1$.

THEOREM 2.41. *If* $m > 0$ *then*

$$m = 2m \to 2^m = m^{[m]} \to \aleph_0 \leqq m.$$

PROOF. Clearly $m^{[m]} \leqq 2^m$. We shall show $0 < m = 2m \to 2^m \leqq m^{[m]}$, thereby proving the first implication. Let M and N be sets such that $|M| = |N| = m$, $M \cap N = \varnothing$ and $M \cup N \approx M$. Let $\phi: M \approx N$. For each $u \subseteq M$, define

$$\Psi(u) = u \cup \{x \in N \mid x \notin \phi''u\}.$$

Then for $u \subseteq M$, $\Psi(u) \subseteq M \cup N$ and $|\Psi(u)| = m$. Thus, Ψ is a 1-1 function mapping $\mathscr{P}(M)$ into $(M \cup N)^{[m]}$, which proves $2^m \leqq m^{[m]}$.

To prove the second implication we note that if $m > 0$ and $2^m = m^{[m]}$ then $m^{[m]} > 1$. Therefore, by 2.40, $\aleph_0 \leqq m$.

The last result of this section strengthens Cantor's theorem that $m < 2^m$.

THEOREM 2.42. $\aleph_0 \leqq m \to (\forall k \in \omega) km < m^{[m]}$.

PROOF. Let $M_0, M_1, \cdots, M_k$ be $k+1$ pairwise disjoint sets such that $|M_i| = m$ for all $i \leqq k$. Let $u_i \in M_i$ and $\phi_i: M_i \approx M_0$ for each $i = 1,2,\cdots,k$. For each $u \in M_i$, $i = 1,2,\cdots,k$, we define

$$\Psi(u) = (M_0 \cup \{u_i\}] \sim \{\phi_i(u)\}.$$

Then Ψ is a 1-1 function from $M = M_1 \cup M_2 \cup \cdots \cup M_k$ into $\mathscr{P}(M_0 \cup \{u_1, \cdots, u_k\})$ and since $\aleph_0 \leqq m$, $|M_0 \cup \{u_1, \cdots, u_k\}| = m$. Moreover, $|\Psi(u)| = m$ for each $u \in M$. Thus $km \leqq m^{[m]}$.

Suppose $km = m^{[m]}$. Then, since $km \leqq 2km \leqq m^{[m]}$, we would have $km = 2km$. By Tarski's cancellation theorem this implies $m = 2m$. But if $m = 2m$, by 2.41, $2^m = m^{[m]}$, and $m = 2^m$ which contradicts Cantor's theorem.

3. Specker [14] proves the following interesting results. Let $G(m)$ be the generalized continuum hypotheses for m. That is,

$G(m)$: $$(\nexists p)(m < p < 2^m)$$

THEOREM 3.1. *If* $m \geqq 5$ *then* $2^m \nleqq m^2$ *and if* m *is infinite then*

(a) $G(m) \to \aleph_0 \leqq m$

(b) $G(m) \to m = 2m$.

(c) $G(m) \to m = m^2$.

(d) $(G(m)\ \&\ G(2^m)) \to 2^m = \aleph(m)$.

(e) $(G(m)\ \&\ G(2^m)) \to m$ is an aleph.

PROOF. Specker [14].

Whether $G(m)$ implies that m is an aleph is an open question. It was already known in 1926 [7] that $G(m)$, $G(2^m)$ and $G(2^{2^m})$ imply that m is an aleph. (Later proved by Sierpinski [12].)

Consider the following proposition.

$G_1(m)$: $$(\nexists p)\ (m < p < m^{[m]}).$$

THEOREM 3.2. *(m is infinite & $\in G(m)$) $\leftrightarrow$ ($\aleph_0 \leqq m$ & $G_1(m)$).*

PROOF. Clearly $G(m)$ implies $G_1(m)$ and if m is infinite, then by 3.1(a), $G(m)$ implies $\aleph_0 \leqq m$.

Conversely, suppose $\aleph_0 \leqq m$ and $G_1(m)$. By 2.35 $m^{[2]} \leqq m^{[m]}$, and by 2.12, $km \leqq m^{[2]}$ for all $k \in \omega$. Thus,

$$m \leqq 2m \leqq 4m \leqq m^{[2]} \leqq m^{[m]}.$$

The theorem follows from Tarski's cancellation law and 2.41.

Tarski [20] proved the following lemma.

LEMMA 3.3. *If $\aleph_0 \leqq m$ then $m < m + \aleph(m)$ and $(\nexists p)(m < p < m + \aleph(m))$.*

Consider the following proposition:

$H(m)$: $$(\nexists p)(\aleph(m) < p < m + \aleph(m)).$$

LEMMA 3.4. *If m is infinite and $0 < k \in \omega$ then $H(m^{k+1}) \to H(m^k)$.*

PROOF. 1.1(e).

THEOREM 3.5. *If m is infinite then $H(m^2) \to m = m^2$.*

PROOF. First, we have

(I) $$m \leqq m^2 < m^2 + \aleph(m).$$

Also,

$$\aleph(m^2) = \aleph(m) \leqq m + \aleph(m) \leqq m^2 + \aleph(m)$$

Thus, $H(m^2)$ implies

(II) $$\aleph(m) = m + \aleph(m)$$

or

(III) $$m + \aleph(m) = m^2 + \aleph(m).$$

From (II) we obtain m is an aleph. From (III) and (I) we get $m \leqq m^2 < m + \aleph(m)$, and from III, $\aleph_0 \leqq m$. Thus. using 3.3, we obtain $m = m^2$.

Clearly, if m is an aleph, then $H(m)$ holds. However, if Σ is consistent then $m = m^2$ does not imply $H(m)$. For let n be an infinite cardinal so that $\aleph_0 \nleqq n$ and let $m = n^{\aleph_0}$. Then $m = m^2$ and we claim

$$\aleph(m) < n + \aleph(m) < m + \aleph(m).$$

It is clearly true that

$$\aleph(m) \leqq n + \aleph(m) \leqq m + \aleph(m).$$

If either of the equality signs hold it is easy to obtain a contradiction.

Assuming the consistency of Σ we can also prove that $H(m)$ does not imply $\aleph_0 \leqq^* m$. It follows from 1.2 and the discussion that follows 1.2 that there is an infinite cardinal m such that $\aleph_0 \nleqq {}^*m$ and there do not exist infinite cardinals p and q such that $m = p + q$. Let m be such a cardinal. Then $\aleph(m) = \aleph_0$. Suppose

(IV) $\quad \aleph_0 = \aleph(m) < n < m + \aleph(m) = m + \aleph_0.$

Then there exist cardinals $p \leqq m$ and $q \leqq \aleph_0$ such that $n = p + q$. If $q < \aleph_0$ then $\aleph_0 \leqq p \leqq m$ which is a contradiction. If $q = \aleph_0$ then either p is finite and $n = \aleph_0$ or p is infinite and there is a finite p_1 such that $p + p_1 = m$. In this case $n = p + \aleph_0 = m + \aleph_0$. Thus (IV) is false, so $H(m)$ is true, but $\aleph_0 \nleqq {}^*m$.

Now let us consider the statements

$H_1(m)$: $\quad (\nexists p)\ (m < p < m^2)$

$H_2(m)$: $\quad (\nexists p)\ (m < p < 2m).$

Clearly if $m > 1$,

$$m = m^2 \to H_1(m) \to m = 2m$$

and

$$m = 2m \to H_2(m) \to \aleph_0 \leqq m.$$

However, if Σ is consistent, $m = 2m$ does not imply $H_1(m)$. For let p be an infinite cardinal such that $\aleph_0 \nleqq p$ and such that $\aleph_0 \cdot p < \aleph_0 \cdot p^2$. (See 1.2). Then, if $m = \aleph_0 \cdot p$, $m = 2m$ and it is easy to show that $m < m + p^2 < m^2$.

Similarly, there is an infinite cardinal p such that $\aleph_0 \nleqq p$ and $\aleph_0 + 2p < \aleph_0 + 3p < \aleph_0 + 4p$ (see 1.2). Thus if $m = \aleph_0 + 2p$ then $\aleph_0 \leqq m$ but $H_2(m)$ is false.

In the last part of this section we shall extend some results of Kruse [5] and [6].

DEFINITION 3.6. If $|M| = m$,

(a) $W(M) = \{f \mid (\exists \alpha) f : \alpha \precsim M\}$; $|W(M)| = w(m)$.

(b) $W'(M) = \{R \subseteq M \times M \mid R \text{ well-orders } \mathscr{D}(R)\}$.

(c) $S(M) = \{u \subseteq M \mid (\exists R \subseteq u \times u)\ R \text{ well-orders } u\}$; $|S(M)| = s(m)$.

(d) $S'(M) = \{u \subseteq M \mid | (\exists \alpha)\, u \approx \alpha\}$.

W is the function defined by Kruse [5]. $W(M)$ is the set of all well-ordered sequences, without repetition, of elements of M. $W'(M)$ is the set of all relations which well-order a subset of M. $S(M)$ and $S'(M)$ are the set of all subsets of M which can be well-ordered.

LEMMA 3.7.

(a) $W(M) \approx W'(M)$.

(b) $S(M) = S'(M)$.

Thus it follows from 3.6 and 3.7 that $|W(M)| = |W'(M)| = w(m)$ and $|(S(M)| = |S'(M)| = s(m)$.

The following two functions are defined by Kruse [5].

DEFINITION 3.8.

(a) $\phi_1 : W(M) \to W'(M)$

where for each $f \in W(M)$, $\phi_1(f) = R$ where R is the well-ordering relation such that $\mathscr{D}(R) = \mathscr{R}(f)$ and $(\forall u, v \in \mathscr{D}(R)) \langle u, v \rangle \in R$ if and only if $f^{-1}(u) \leqq f^{-1}(v)$.

(b) $\phi_2 : W(M) \to \mathscr{P}(\mathscr{P}(M))$

where for each $f \in W(M)$, $\phi_2(f) = \{u : u \text{ is an initial segment of } \phi_1(f)\} \cup \{\mathscr{R}(f)\}$. It is easy to show that ϕ_1 and ϕ_2 are 1-1 functions.

LEMMA 3.9.

(a) $\phi_1 : W(M) \approx W'(M) \subseteq \mathscr{P}(M \times M)$.

(b) $\phi_2 : W(M) \precsim \mathscr{P}(\mathscr{P}M))$.

The next lemma follows easily from 3.6 and 3.9.

LEMMA 3.10.

(a) $m \leqq w(m) \leqq 2^{m^2}$.

(b) $m \leqq w(m) \leqq 2^{2^m}$.

(c) $m \leqq s(m) \leqq 2^m$.

Moreover, we have

LEMMA 3.11.

(a) $m < w(m)$.

(b) $m < s(m)$.

PROOF. The proof of (a) is given by Kruse [5] p. 546, and that of (b) by Tarski [18] p. 179.

The next lemma gives some monotonicity laws for w and s. The proof follows directly from 3.6.

LEMMA 3.12.

(a) $m \leqq n \to w(m) \leqq w(n)$.

(b) $m \leqq n \to s(m) \leqq s(n)$.

LEMMA 3.13.

(a) *If m is infinite,* $\aleph(m) \leqq^* w(m)$.

(b) $s(m) \leqq^* w(m)$.

(c) *If m is infiinte,* $\aleph(w(m)) \leqq \aleph(2^m)$.

PROOF. Suppose $|M| = m$. Then if $f \in W(M)$, define

$$\Psi_1(f) = \mathscr{D}(f), \quad \Psi_2(f) = \mathscr{R}(f).$$

Then Ψ_1 is a function mapping $W(M)$ onto $\aleph(M)$ and Ψ_2 is a function mapping $W(M)$ onto $S(M)$.

The proof of (c) is given by Kruse [5] p. 547.

THEOREM 3.14. *If m is an aleph, then*

(a) $w(m) = 2^m$.

(b) $s(m) = 2^m$.

PROOF. The proof of (a) is due to Kruse, but we shall sketch it here. It follows from the hypothesis that $m = m^2$. Therefore, by 3.10(a), $w(m) \leqq 2^m$. To get the inequality the other way, let R be a relation which well-orders M, where $|M| = m$. Let u be any subset of M. Then there exists a unique ordinal number α and a unique function f such that $f\colon \alpha \approx u$ and f preserves order. Define $\Psi(u) = f$. Then Ψ is a 1-1 function mapping $\mathscr{P}(M)$ into $W(M)$.

The proof of (b) follows directly from 3.6(c).

Some additional properties of Kruse's function are given in the following lemma.

LEMMA 3.15.

(a) $w(m) \cdot w(n) \leqq w(m+n)$

(b) $(\forall k \in \omega)\, w(km) \geqq [w(m)]^k$.

PROOF. The proof of (a) is given by Kruse [6] p. 137, and (b) follows from (a).

THEOREM 3.16.

(a) $\aleph_0 \leqq m \to w(m) = 2^{\aleph_0} \cdot w(m)$.

(b) $m = 2m \to w(m) = [w(m)]^2$.

PROOF.

(a) $2^{\aleph_0} \cdot w(m) \;=\; w(\aleph_0)w(m)$ [3.14(a)]

$$
\begin{aligned}
& \leqq w(m+\aleph_0) && [3.15]\\
& = w(m) && [\mathrm{Hyp}]\\
\text{(b)}\quad [w(m)]^2 & \leqq w(2m) && [3.15(\mathrm{b})]\\
& = w(m) && [\mathrm{Hyp.}].
\end{aligned}
$$

THEOREM 3.17.

(a) $G(m) \to s(m) = 2^m$.

(b) $G(m) \to w(m) = 2^m$.

PROOF. (a) 3.10(c) and 3.11(b).

(b) 3.1(c), 3.10(a), and 3.11(a).

THEOREM 3.18. *Each of the following are equivalent:*

(1) $\aleph_0 \leqq m$.

(2) $\aleph_0 \leqq w(m)$.

(3) $w(m) = w(m) + m \;\&\; m \neq 0$.

(4) $w(m) = 2w(m)$.

(5) $w(m) = 2^{\aleph_0} w(m)$.

(6) $w(m) = m \cdot w(m) \;\&\; m \neq 1$

PROOF. Clearly, if $m \geqq 2$.

$$m < w(m) \leqq w(m) + 1 \leqq w(m) + m \leqq 2w(m) \leqq \begin{cases} 2^{\aleph_0} \cdot w(m) \\ m \cdot w(m) \end{cases}$$

Therefore,

$$(6) \to (4) \to (3) \to (2) \to (1)$$

and

$$(5) \to (4) \to (3) \to (2) \to (1).$$

In 3.16(a) we proved (1) $\to$ (5). Therefore, it remains to be shown that (1) $\to$ (6).

Suppose $\aleph_0 \leqq m$ and let $|M| = m$. For each $u \in M$, let ϕ_u be a 1-1 function mapping M onto $M \sim \{u\}$. For each $f \in W(M)$, define $\phi_u(f)$ to be the function g such that $g(0) = u$, $g(\alpha+1) = \phi_u(f(\alpha))$ if $\alpha \in \omega$, and $g(\alpha) = \phi_u(f(\alpha))$ if $\alpha \geqq \omega$. Thus, if $f \in W(M)$, $\phi_u(f) \in W(M)$. Moreover, if $f_1, f_2 \in W(M)$, $f_1 \neq f_2$ then $\phi_u(f_1) \neq \phi_u(f_2)$ because ϕ_u is 1-1 on M.

Now we define a function Ψ on $M \times W(M)$ to $W(M)$ as follows: for each $\langle u,f \rangle \in M \times W(M)$,

$$\Psi(u,f) = \phi_u(f).$$

Then Ψ is a 1-1 function from $M \times W(M)$ into $W(M)$, so $m \cdot w(m) \leqq w(m)$.

Kruse [5] p. 549 proves the following results which extend properties of Hartog's $\aleph$-function. (see 1.1(f), (g)).

LEMMA 3.19. *If m is infinite*

(a) $m^2 \cdot \aleph(m) \leqq^* 2^{m^2}$

(b) $2^m \cdot \aleph(m) \leqq^* 2^{2^m}$

We shall show we can obtain somewhat similar results if "$\aleph(m)$" is replaced by "$w(m)$". It is clear that if $\aleph_0 \leqq m$, then $2^m \cdot 2^{2^m} = 2^{2^m}$. Also, it follows from 3.18 that $\aleph_0 \leqq m$ implies $m^2 \cdot w(m) = w(m)$. Therefore, using 3.10(a) and (b) we obtain,

THEOREM 3.20. *If $\aleph_0 \leqq m$ then*

(a) $m^2 \cdot w(m) \leqq 2^{m^2}$

(b) $2^m \cdot w(m) \leqq 2^{2^m}$.

However, we shall show that the second inequality holds for all infinite m.

THEOREM 3.21. *If m is infinite then*

$$2^m \cdot w(m) \leqq 2^{2^m}$$

PROOF. If $\aleph_0 \leqq m$ the theorem follows from 3.20(b), so suppose m is infinite but $\aleph_0 \nleqq m$. Let $|M| = m$. Define a function

$$\Psi \colon \mathscr{P}(M) \times W(M) \to \mathscr{P}(\mathscr{P}(M))$$

as follows. If $N \subseteq M$ and $f \in W(M)$,

$$\Psi(N,f) = \phi_2(f) \cup \{M \sim \{u\} \mid u \in N\}$$

(ϕ_2 is defined in 3.8). Let

$$P_N = \{M \sim \{u\} \mid u \in N\}$$

Every element of $\phi_2(f)$ is a well-ordered set while $M \sim \{u\}$ is not well-ordered for any u. Thus, $\phi_2(f) \cap P_N = \emptyset$ for each $N \subseteq M$, $\phi_2(f)$ uniquely determines f, and P_N uniquely determines N. Therefore Ψ is 1-1 and $2^m w(m) \leqq 2^{2^m}$.

Next, we will show that the function s has some properties similar to w.

LEMMA 3.22.

(a) $s(m) \cdot s(n) \leqq s(m + n)$

(b) $(\forall k \in \omega) s(km) \geqq [s(m)]^k$

PROOF. Similar to the Proof of 3.15.

THEOREM 3.23.

(a) $\aleph_0 \leqq m \to s(m) = 2^{\aleph_0} \cdot s(m)$

(b) $m = 2m \to s(m) = [s(m)]^2$.

PROOF. Similar to the proof of 3.16.

Suppose $H_3(m)$ and $H_4(m)$ are the following propositions,

$H_3(m)$: $$(\nexists p)\ (m < p < w(m))$$

and

$H_4(m)$: $$(\nexists p)\ (m < p < s(m))$$

Since it is easy to prove that for $m \geqq 2$, $m \leqq 2m \leqq w(m)$ and $m \leqq 2m \leqq s(m)$, the following theorem follows from 3.11.

THEOREM 3.24. *If* $m \geqq 2$

(a) $H_3(m) \to m = 2m$.

(b) $H_4(m) \to m = 2m$.

LEMMA 3.25. *If m is infinite,*

(a) $(\forall k \in \omega)\ m^k \leqq w(m)$.

(b) $LO(m) \to (\forall k \in \omega) m^k \leqq s(m)$.

PROOF. Clearly $f(m) \leqq w(m)$. Thus (a) follows from 2.5.

Similarly, $e(m) \leqq s(m)$, so (b) follows from 2.15.

THEOREM 3.26. *If m is infinite,*

(a) $H_3(m) \to m^2 = m^3$.

(b) $LO(m) \to (H_4(m) \to m^2 = m^3)$.

PROOF. (a) It follows from 3.25(a) that $H_3(m)$ implies either $m = m^2$ or $m^2 = w(m)$. Clearly $m = m^2$ implies $m^2 = m^3$.

The proof of (b) is analogous, using 3.25(b) instead of 3.25(a).

Note. The referee has commented that Mr. John Truss of Leeds University, England, has proved the following theorem:

If m is infinite then $w(m) \nleqq m^k$ and $s(m) \nleqq m^k$ for every $k \in \omega$.

The proof uses a method similar to that used by Specker in the Proof of 3.1. Thus, it follows that 3.25 and 3.26 can be strengthened to the following:

If m is infinite then

$$(\forall k \in \omega) m^k < w(m).$$

$$LO(m) \to (\forall k \in \omega) m^k < s(m).$$

$$H_3(m) \to m = m^2.$$

$$LO(m) \to (H_4(m) \to m = m^2).$$

References

1. H. Bachman, *Transfinite Zahlen*, Springer-Verlag, New York, 1967.

2. P. Cohen, *Set Theory and the Continuum Hypothesis*, W. A. Benjamin Inc. New York, 1966.

3. E. Ellentuck, *Generalized idempotence in cardinal arithmetic*, Fund. Math. **58** (1966), 241–258.

4. B. Harris, *Theory of Probability*, Addison-Wesley, Reading Mass., 1966.

5. A. Kruse, *Some developments in the theory of numerations*, Trans. Amer. Math. Soc. **97** (1960), 523–553.

6. A. Kruse, *Some observations on the axiom of choice*, Z. Math. Logik Grundlagen Math., **8** (1962), 125–146.

7. A. Lindenbaum and A. Tarski, *Communication sur les recherches de la théorie des ensembles*, C.R. Varsovie, **19** (1926), 299–330.

8. H. Lauchli, *Ein Beitrag zur Kardinalzahlarithmetik ohne Auswahlaxiom*, *Z.* Math. Logik Grunglagen Math. **7** (1961), 141–145.

9. A. Mostowski, *Über die Unabhangigkeit des Wohlordungssatzes vom Ordnungs prinzip*, Fund. Math. **32** (1939), 201–252.

10. H. Rubin and J. E. Rubin, *Equivalents of the Axiom of Choice*, North-Holland Amsterdam, 1963.

11. J. E. Rubin, *Set Theory for the Mathematician*, Holden-Day San, Francisco, 1967.

12. W. Sierpinski, *L'hypothèse géneralisée du continu et l'axiom du choix*, Fund. Math. **34** (1947), 1–5.

13 W. Sierpinski, *Cardinal and Ordinal Numbers*, Pânstwome Wydawnictwo Naukowe, Warsawa, 1958.

14 E. Specker, *Verallgemeinerte Kontinuums-hypothese und Auswahlaxiom*, Arch. Math. **5** (1954), 332–337.

15. A. Tarski, *Sur les ensembles finis*, Fund. Math. **6** (1924), 45–95.

16. A. Tarski, *Sur les classes d'ensembles closes par rapport a certaines operations élémentaires*, Fund. Math. **16** (1930), 181–304.

17. A. Tarski, *Eine aquivalente Formulierung des Auswahlaxioms*, Fund. Math. **30** (1938) 197–201.

18. A. Tarski, *On well-ordered subsets of any set*, Fund. Math. **32** (1939), 176–183.,

19. A. Tarski, *Cancellation laws in the arithmetic of cardinals*, Fund. Math. **36** (1949), 77–92.

20. A. Tarski, *Theorems on the existence of successors of cardinals, and the axiom of choice*, Indag. Math. **16** (1954), 26–32.

Purdue University,
Lafayette, Indiana