Factorials of infinite cardinals

by

John W. Dawson, Jr. (University Park, Pa.) and
Paul E. Howard (Ypsilanti, Mich.)

Abstract. Cardinalities of the power set and the symmetric group of an infinite set are compared, both in the presence and absence of the axiom of choice.

According to Cantor's well-known theorem, the power-set operation applied to any set yields a set of strictly greater cardinality. So we are led to ask: Are there any other natural, yet inherently different set-theoretic operations with this property?

To anyone acquainted with algebra, one candidate immediately suggests itself: the operation of forming the symmetric group of a set. Unfortunately $n! = n$ for $n = 1, 2$, so in trivial cases the analogue of Cantor's theorem fails. Nonetheless for $n>3$, $n!>2^n$, so it is natural to inquire what happens in the infinite case. That question is the subject of this paper.

In what follows we use $\mathscr{P}(X)$ and $S(X)$ to denote, respectively, the power set and the symmetric group of the set X (assumed infinite unless otherwise stated). We denote the cardinality of X by $|X|$ and define $X! = |S(X)|$ and $2^X = |\mathscr{P}(X)|$. Zermelo-Fraenkel set theory is abbreviated as ZF, while ZFC stands for ZF plus the axiom of choice (AC). In Section 2 we also use ZFU to denote Zermelo-Fraenkel set theory weakened to permit a set U of urelements.

We show first of all that in ZF, $|X|<X!$ whenever $|X|\geqslant 3$. This result is presumably part of the folklore of axiomatic set theory, but we are aware of no explicit statement or proof in the literature. Indeed, even such a standard reference as [8] makes no mention of $|S(X)|$. Perhaps the reason for this is that those who have considered the question have come to realize that *in* ZFC $X! = 2^X$ for all infinite X. In one direction, the most apparent method for demonstrating $X!\geqslant 2^X$ is to prove that for every $Y\subseteq X$ such that $|X-Y|\neq 1$, there is a permutation of X leaving fixed exactly the set Y. (This approach is taken, e.g., in Bourbaki [1], where the result occurs as Exercise III. 6.5.) On the other hand, the equation $|X|^2 = |X|$ arises naturally in showing $X!\leqslant 2^X$, so that in either case one is soon led to believe that some use of the axiom of choice is unavoidable.

Indeed, in the absence of the axiom of choice, any of the three alternatives (i) $X!$ and 2^X are incomparable, (ii) $X!>2^X$, or (iii) $X!<2^X$, are possible. This is

established is Section 2 below in the context of ZFU by exhibiting appropriate Fraenkel-Mostowski models in which X is taken to be the set of urelements. The transfer to ZF then follows directly by results of Jech and Sochor.

Our methods do not suffice to demonstrate the independence of the axiom of choice from the assertion that $X! = 2^X$ for all infinite X. Since the appearance of the preliminary version of this paper, however, that result has been established in ZF by David Pincus, to whom we are also indebted for several improvements to our original exposition.

§ 1. Except where otherwise stated, results of this section are understood to be proved in ZF. To distinguish tuples from cycles, we separate terms of the latter by semicolons instead of commas.

THEOREM 1.1. *If* $|X| \geqslant 3$, $|X| < X!$.

Proof. Since $|X| \leqslant |2 \times X|$, we consider two cases.

If $|X| < |2 \times X|$ then it suffices to show $|2 \times X| \leqslant X!$. For this, pick three distinct elements $a, b, c \in X$ and define f: $2 \times X \overset{1-1}{\to} S(X)$ by $f(0, x) = (x; a)$ and $f(1, x) = (x; b)$ if $x \notin \{a, b\}$; $f(0, a) = (a; b)$ and $f(0, b) =$ the identity; and $f(1, d) = (a; b; c)$, $f(1, b) = (a; c; b)$.

If $|X| = |2 \times X|$ then $X! = (2 \times X)!$, so by Cantor's theorem it suffices to show $2^X \leqslant (2 \times X)!$. Thus, given any $A \in \mathscr{P}(X)$, define Ψ_A in $S(2 \times X)$ by

$$\Psi_A(0, y) = \begin{cases} (0; y) & \text{if} \quad y \notin A, \\ (1; y) & \text{if} \quad y \in A, \end{cases}$$

$$\Psi_A(1, y) = \begin{cases} (1; y) & \text{if} \quad y \notin A, \\ (0; y) & \text{if} \quad y \in A. \end{cases}$$

THEOREM 1.2. *If* $1 < |X| = |X|^2$, *then* $X! = 2^X$.

Proof. Since $S(X) \subseteq \mathscr{P}(X \times X)$, we have $X! \leqslant 2^{X \times X} = 2^X$. But the hypothesis immediately implies $|X| = |2 \times X|$, so as in the proof of 1.1, $2^X \leqslant X!$.

COROLLARY 1.3. *For any infinite set* X, *if* X *can be well-ordered then* $X! = 2^X$. *In particular, in* ZFC $X! = 2^X$ *for all infinite* X.

COROLLARY 1.4. AC$\leftrightarrow(\forall X)$ (X *well-orderable* $\to S(X)$ *well-orderable*).

Proof. This follows immediately from 1.3 and the well-known (but often misproved) equivalence AC$\leftrightarrow(\forall X)$ (X well-orderable $\to \mathscr{P}(X)$ well-orderable) (cf. [7]).

With regard to 1.4, note that any proof of the equivalence of the axiom of choice with either of the statements $(\forall X)$ (X well-orderable $\to \mathscr{P}(X)$ well-orderable) or $(\forall X)$ (X well-orderable $\to S(X)$ well-orderable) must make essential use of the axiom of foundation, since both of these statements are true in all Fraenkel-Mostowski models of ZFU.

Finally, we remark that in the countable case Corollary 1.3 also has a simple "analytic" proof, due to Q. Klein. For if $X = \{x_i \mid i < \omega\}$, let each x_i correspond

to $a_i = 1/(i+1)$. Then the conditionally convergent series $\sum_{i=0}^{\infty} (-1)^i a_i$ can be canonically rearranged to converge to any real number, so $2^X = |R| \leqslant \omega!$.

§ 2. In this section we show that any of the alternatives $X! < 2^X$, $X!$ and 2^X are incomparable, and $2^X < X!$ are possible. This is done by exhibiting three permutation models of the theory ZFU.

We refer the reader to Jech [4] for elementary facts about permutation models. We first prove that in the ordered Mostowski model of [5], $U! > 2^U$ where U is the set of urelements. This is the same model used in Halpern [2] to show the independence of the Boolean Prime Ideal Theorem from AC.

Here is a description of the model: Let M' be a model of ZFU+AC with a countable set U of urelements. Let $<$ be an ordering of U with order type that of the rationals. Let G be the group of all order preserving permutations of U. If e is any subset of U, let

$$\operatorname{fix}(e) = \{\psi \in G\colon (\forall t \in e)(\psi(t) = t)\}.$$

Let $\mathfrak{F}$ be the filter of subgroups of G generated by the set $\{\operatorname{fix}(e)\colon e \text{ is a finite subset of } U\}$ and let M be the permutation model determined by U and $\mathfrak{F}$.

We will usually observe the following notational convention: When a permutation of U is thought of as an element of G we will use the symbol ψ (possibly subscripted or primed) to denote the permutation. If a permutation is thought of as an element of $S(X)$ the symbol φ will be used.

If $x \in M$, a finite subset $e \subseteq U$ is a *support* of x if $\forall \psi \in \operatorname{fix}(e)$, $\psi(x) = x$. An argument for the following lemma is given in [4], p. 50.

LEMMA 2.1. *Each element of* M *has a unique minimal support; further, if* e *is a minimal support of* x, *then*

$$\psi \in \operatorname{fix}(e) \to \psi(x) = x.$$

LEMMA 2.2. *If* $e \subseteq U$ *and* $|e| = k$, *then there are at most* 2^{2k+1} *subsets of* U *in* M *with minimal support* e.

Proof. Suppose $e = \{t_1, \ldots, t_k\}$ where $t_1 < \ldots < t_k$. Let

$$\begin{aligned} A_1 &= (-\infty, t_1) \quad (= \{t \in U\colon t < t_1\}), \\ A_2 &= \{t_1\}, \\ A_3 &= (t_1, t_2), \\ &\cdots\cdots\cdots \\ A_{2k-1} &= (t_{k-1}, t_k), \\ A_{2k} &= \{t_k\}, \\ A_{2k+1} &= (t_k, \infty). \end{aligned}$$

Suppose $B \subseteq U$ has minimal support e. Then for each i, $1 \leqslant i \leqslant 2k+1$, $B \cap A_i = \emptyset$ or $B \cap A_i = A_i$. Hence B is of the form $\bigcup_{i \in L} A_i$ where $L \subseteq \{1, 2, \ldots, 2k+1\}$, and there are 2^{2k+1} such sets.

LEMMA 2.3. *If φ is a permutation of U in M, then $e = \{t \in U: \varphi(t) \neq t\}$ is a minimal support of φ.*

Proof. This is an easy consequence of the fact that for any finite subset e of U and any $\psi \in G$, $\psi(e) = e \to \psi \in \mathrm{fix}(e)$.

THEOREM 2.4. *In M, $2^U \leqslant U$!*

Proof. For any $b \in M$, let $S^0(b) = \{\varphi \in S(b): (\forall n \in b)(\varphi(n) \neq n)\}$. If $k \in \omega$, $|S^0(k)| - k!/e$ approaches 0 as k approaches ∞, so k can be chosen so that $(k+1)\cdot 2^{2k+1} < |S^0(k)|$. Choose such a k and let e be a set of $k(k^2+k)/2$ elements of U indexed as follows:

$$e = \{t^r(i,j): 1 \leqslant r \leqslant k,\ 1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant r\}\,.$$

For each r and i, $1 \leqslant r \leqslant k$ and $1 \leqslant i \leqslant k$, let $R^r(i) = \{t^r(i,j): 1 \leqslant j \leqslant r\}$ and let $R^r = \{t^r(i,j): 1 \leqslant i \leqslant k \text{ and } 1 \leqslant j \leqslant r\}$. It will be helpful if we put e in the following array which we will refer to as (*).

$$\begin{array}{l} t^1(1,1) \qquad\qquad t^1(2,1) \ldots\ldots\ldots\ldots t^1(k,1) \\ t^2(1,1)\,t^2(1,2) \qquad t^2(2,1)\,t^2(2,2) \ldots\ldots t^2(k,1)\,t^2(k,2) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ t^k(1,1)\,t^k(1,2) \ldots t^k(1,k)\ t^k(2,1)\,t^k(2,2) \ldots t^k(2,k) \ldots\ t^k(k,1) \ldots t^k(k,k) \end{array}$$

e will be the support of a function from $\mathscr{P}^M(U)$ 1-1 and into $S^M(U)$. We now proceed to define the function in several steps.

For each finite subset a of U, define

$$F(a) = \begin{cases} a & \text{if} \quad |a| \geqslant k\,, \\ a \cup R^n(i) & \text{if} \quad |a| = k-n \text{ and } i \text{ is the least natural} \\ & \qquad \text{number such that } R^n(i) \cap a = \emptyset\,, \end{cases}$$

i.e., if $|a| = k-n$, look at the nth row of the array (*) and add to a the first "block" of n elements which does not intersect a. The following four lemmas are consequences of the definition of F.

LEMMA 2.5. *$|F(a)| \geqslant k$ for every finite $a \subseteq U$.*

LEMMA 2.6. *If $|a| = k-n$ and $F(a) = b$, then $|a \cap R^r| = |b \cap R^r|$ for $r \neq n$ and $|a \cap R^n| + n = |b \cap R^n|$.*

LEMMA 2.7. *If $|b| = k$ and $|b \cap R^n| = j$, then there are at most j sets a such that $F(a) = b$ and $|a \cap R^n| < j$.*

LEMMA 2.8. *If $b \subseteq U$, there are at most $k+1$ sets a such that $F(a) = b$ (by Lemma 2.7).*

If $b \subseteq U$ and $|b| \geqslant k$, we let $F^{-1}[b] = \{a: F(a) = b\}$. Suppose $b \subseteq U$ is finite and $|b| \geqslant k$. We define

$$L(b) = \{A: A \subseteq U \,\&\, A \text{ has minimal support } a \text{ for some } a \in F^{-1}[b]\}\,.$$

Then by Lemmas 2.2 and 2.8 $|L(b)| \leqslant (k+1)\cdot 2^{2k+1}$. So by the choice of k, $|L(b)| < |S^0(b)|$.

LEMMA 2.9. *If $\varphi \in S^0(b)$ then φ has minimal support b. Hence for all $\psi \in G$, $\psi(\varphi) = \varphi \leftrightarrow \psi(b) = b$.*

Proof. This lemma follows from Lemma 2.3.

LEMMA 2.10. *If $A \in L(b)$ and $\psi \in \mathrm{fix}(e)$, then $\psi(A) = A \leftrightarrow \psi(b) = b$.*

Proof. Suppose A has minimal support a; then since $A \in L(b)$, $F(a) = b$. Hence $a \cup e' = b$ for some $e' \subseteq e$.

Now suppose $\psi(A) = A$. Then $\psi(a) = a$ by Lemma 2.1, hence $\psi(b) = b$. (Since $\psi \in \mathrm{fix}(e)$.)

Conversely suppose $\psi(b) = b$. Then $\psi(a) = a$, hence $\psi(A) = A$.

COROLLARY 2.11. *If $\varphi \in S^0(b)$ and $A \in L(b)$ then for all $\psi \in \mathrm{fix}(e)$*

$$\psi(\varphi) = \varphi \leftrightarrow \psi(A) = A\,.$$

LEMMA 2.12. *If $b \neq b'$ where b and b' are finite subsets of U such that $|b|, |b'| \geqslant k$, then $L(b) \cap L(b') = \emptyset$ and $S^0(b) \cap S^0(b') = \emptyset$. (Here and in what follows we suppose that $S^0(b)$ has been embedded in $S(U)$ in the natural way for each finite subset b of U.)*

Proof. The first part of the conclusion follows from the uniqueness of minimal supports and the definition of $L(b)$. The second part follows from the definition of S^0.

LEMMA 2.13. *If $b, b' \subseteq U$ are finite and $|b|, |b'| \geqslant k$ and if $A \in L(b)$ and $\varphi \in S^0(b)$, then for $\psi \in \mathrm{fix}(e)$ the following are equivalent:*

(i) $\psi(b) = b'$,
(ii) $\psi(A) \in L(b')$,
(iii) $\psi(\varphi) \in S^0(b')$.

Proof. (i) $\Leftrightarrow$ (iii) is clear using the fact that for any $\eta \in G$, $\eta(a)$ is a minimal support of $\eta(x)$ whenever a is a minimal support of x.

We prove (i) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (i). Suppose $\psi(b) = b'$ and that a is a minimal support for A; then $F(a) = a \cup e' = b$ where $e' \subseteq e$. We also have that $b' = \psi(F(a)) = \psi(a) \cup e' = F(\psi(a))$ using the definition of F and the fact that $\psi \in \mathrm{fix}(e)$. Hence $b' = F(\psi(a))$, therefore $\psi(A) \in L(b')$.

Suppose now that $\psi(A) \in L(b')$. Then $\psi(a)$ is a minimal support of $\psi(A)$ and hence $F(\psi(a)) = b'$, i.e., $\psi(a) \cup e' = b'$ where $e' \subseteq e$. Since $A \in L(b)$, $a \cup e' = b$ so that

$$\psi(b) = \psi(a \cup e') = \psi(a) \cup e' = b'.$$

This completes the proof of the lemma.

We now define an equivalence relation $\sim$ on $\{b \subseteq U: b \text{ is finite and } |b| \geqslant k\}$ by

$$b \sim b' \leftrightarrow (\exists \psi \in \mathrm{fix}(e))(\psi(b) = b')\,.$$

Let $\mathfrak{G}$ be the set of equivalence classes. For each $c \in \mathfrak{G}$ choose $b_c \in c$ and let W_{b_c} be a 1-1 function from $L(b_c)$ into $S^0(b_c)$. This is possible since $|L(b_c)| < |S^0(b)|$. Let

$$W = \bigcup \{\psi(W_{b_c}): c \in \mathfrak{G} \text{ and } \psi \in \mathrm{fix}(e)\}\,.$$

Claim. W is a 1-1 function from $\mathscr{P}^M(U)$ into $S^M(U)$ and W has support e.

That W has support e and that Range$(W) \subseteq S^M(U)$ follow from the definition of W. It remains to show:

1. W is a function. Suppose $(\psi(A), \psi(W_{b_c}(A)))$ and $(\psi'(A'), \psi'(W_{b_{c'}}(A')))$ are in W, where $A \in L(b_c)$ and $A' \in L(b_{c'})$ and $\psi, \psi' \in \mathrm{fix}(e)$, and suppose $\psi(A) = \psi'(A')$; then $\psi'^{-1}\psi(A) = A'$. Hence by Lemma 2.13

$$\psi'^{-1}\psi(b_c) = b_{c'},$$

so $b_c \sim b_{c'}$, which implies $b_c = b_{c'}$. Hence by Lemma 2.10

$$\psi'^{-1}\psi(A) = A \ (= A').$$

So by Corollary 2.11

$$\psi'^{-1}\psi(W_{b_c}(A)) = W_{b_c}(A) = W_{b_{c'}}(A').$$

Hence W is a function.

2. W is 1-1. As in 1, suppose $(\psi(A), \psi(W_{b_c}(A)))$ and $(\psi'(A), \psi'(W_{b_{c'}}(A')))$ are in W, where $A \in L(b_c)$ and $A' \in L_{b_{c'}}$ and $\psi, \psi' \in \mathrm{fix}(e)$. Now suppose

$$\psi(W_{b_c}(A)) = \psi'(W_{b_{c'}}(A'));$$

then

(1) $$\psi'^{-1}\psi(W_{b_c}(A)) = W_{b_{c'}}(A'),$$

whence by Lemma 2.13

(2) $$\psi'^{-1}\psi(b_c) = b_{c'}.$$

I.e., $b_c \sim b_{c'}$, which implies $b_c = b_{c'}$. Rewriting (2) we get $\psi'^{-1}\psi(b_c) = b_c$. Then applying Lemma 2.10

(3) $$\psi'^{-1}\psi(A) = A$$

and

(4) $$\psi'^{-1}\psi(W_{b_c}(A)) = W_{b_c}(A).$$

Combining (1), (4) and $b_c = b_{c'}$ gives

$$W_{b_c}(A) = W_{b_c}(A').$$

Hence $A = A'$ since W_{b_c} is 1-1. By this and (3) we obtain $\psi'^{-1}\psi(A) = A'$, so $\psi(A) = \psi'(A')$ and hence W is 1-1.

3. The domain of W is $\mathscr{P}^M(U)$. Choose $A \in \mathscr{P}^M(U)$ and suppose that A has minimal support a. Let $F(a) = b$ and suppose that $\psi(b_c) = b$ where $\psi \in \mathrm{fix}(e)$. Then $\psi^{-1}(b) = b_c$, so by Lemma 2.13 $\psi^{-1}(A) \in L(b_c)$. Hence

$$(\psi^{-1}(A), W_{b_c}(\psi^{-1}(A))) \in W_{b_c}$$

and so

$$\psi((\psi^{-1}(A), W_{b_c}(\psi^{-1}(A)))) \in W;$$

that is

$$(A, (W_{b_c}(\psi^{-1}(A)))) \in W.$$

Therefore A is in the domain of W.

This completes the proof of the claim and hence the proof of the theorem.

THEOREM 2.14. *In M, $2^U \neq U$!.*

Proof. Suppose $F \in M$ is a 1-1 correspondence between $\mathscr{P}^M(U)$ and $S^M(U)$ and suppose F has minimal support e. Choose a set $a = \{t_1, t_2, \ldots, t_k\}$ of urelements so that $a \cap e = \emptyset$ (where k is chosen so that $n \geqslant k \rightarrow 2^{2n+1} < |S^0(n)|$).

If $A \in \mathscr{P}^M(U)$ and A has minimal support $a \cup e$ where $e' \subset e$, then $F(A)$ must have minimal support $a \cup e''$ for some $e'' \subseteq e$. (Otherwise there will be some $\psi \in \mathrm{fix}(e)$ such that either $\psi(A) = A$ and $\psi(F(A)) \neq F(A)$, or else $\psi(F(A)) = F(A)$ and $\psi(A) \neq A$, contradicting the fact that F is 1-1 and has support e.) Similarly if $\varphi \in S^M(U)$ and φ has minimal support $a \cup e'$ for some $e' \subseteq e$, then $F^{-1}(\varphi)$ must have minimal support $a \cup e''$ for some $e'' \subseteq e$. Therefore if we let

$$X = \{A \subseteq U\colon A \text{ has minimal support } a \cup e' \text{ for some } e' \subseteq e\}$$

and

$$Y = \{\varphi \in S^M(U)\colon \varphi \text{ has minimal support } a \cup e' \text{ for some } e' \subseteq e\}$$

then $F \restriction X$ is a 1-1 correspondence between X and Y.

To show this is impossible, it suffices to show that for each $e' \subseteq e$, $|X_{e'}| < |Y_{e'}|$ where

$$X_{e'} = \{A \subseteq U\colon A \text{ has minimal support } a \cup e'\}$$

and

$$Y_{e'} = \{\varphi \in S^M(U)\colon \varphi \text{ has minimal support } a \cup e'\}.$$

So choose $e' \subseteq e$ and suppose $|a \cup e'| = n$. Then $n \geqslant k$, so $2^{2n+1} < |S^0(n)|$. But by Lemma 2.3, $|S^0(n)| = |Y_{e'}|$, and by Lemma 2.2, $|X_{e'}| \leqslant 2^{2n+1}$. Therefore $|X_{e'}| < |Y_{e'}|$ and the proof is complete.

We now construct a model of ZFU with set of urelements U in which U! and 2^U are incomparable.

Let M' be a model of ZFU+AC with a countable set U of urelements. Let G be the group of all permutations of U. For each $e \subseteq U$, let

$$\mathrm{fix}(e) = \{\psi \in G\colon (\forall t \in e)(\psi(t) = t)\}$$

and let $\mathfrak{F}$ be the filter of subgroups generated by the set $\{\mathrm{fix}(e)\colon e \subseteq U \text{ and } e \text{ is finite}\}$.

Finally let M be the permutation model determined by U and $\mathfrak{F}$.

LEMMA 2.15. *If $A \subseteq U$ and $A \in M$, then A is either finite or cofinite.*

Proof. Suppose $\mathrm{fix}(e)$ fixes A (i.e., for all ψ in $\mathrm{fix}(e)$, $\psi(A) = A$). Then if $t \in A$ for some $t \notin e$, we have $t' \in A$ for every $t' \notin e$. This follows because the permutation $(t; t')$ is in $\mathrm{fix}(e)$ and hence t', being the image of t under this permutation, must

be in A. Thus if $A \cap$ complement $(e) \neq \emptyset$, A must contain the complement of e and hence is cofinite. On the other hand, if $A \subseteq e$, then A is finite.

Using a similar argument one can show the following.

LEMMA 2.16. *If $\varphi \in S^M(U)$, then $\{t \in U: \varphi(t) \neq t\}$ is finite.*

THEOREM 2.17. *In M, $U! \not\leqslant 2^U$ and $2^U \not\leqslant U!$.*

Proof. Suppose first F is a 1-1 function in M from $S^M(U)$ into $\mathscr{P}^M(U)$ and suppose $\mathrm{fix}(e)$ fixes F where $e \subseteq U$ is finite. Choose t_1, t_2 and $t_3 \in U$ so that

$$\{t_1, t_2, t_3\} \cap e = \emptyset$$

and let $\varphi = (t_1; t_2; t_3)$. Suppose $F(\varphi) = A$.

If A is finite, then $\{t_1, t_2, t_3\} \subseteq A$. (Otherwise choose $t \notin \{t_1, t_2, t_3\} \cup e \cup A$ and suppose $t_3 \notin A$. Then $\psi = (t; t_3)$ is an element of $\mathrm{fix}(e)$. Further, $\psi(A) = A$ but $\psi(\varphi) \neq \varphi$, which contradicts the fact that $\mathrm{fix}(e)$ fixes F.) But now if $\psi' = (t_1; t_2)$, then ψ' fixes A and moves φ. Since $\psi' \in \mathrm{fix}(e)$ we have contradicted our assumption that $\mathrm{fix}(e)$ fixes F.

If A is cofinite, then $\{t_1, t_2, t_3\} \cap A = \emptyset$ (by an argument similar to the one above). But this again means that $\psi' = (t_1; t_2)$ fixes A and moves φ, a contradiction. Hence no such F exists.

Now suppose H is a 1-1 function from $\mathscr{P}^M(U)$ into $S^M(U)$ and that $\mathrm{fix}(e)$ fixes H. Let $a = \{t_1, t_2, t_3\}$ where $a \cap e = \emptyset$. If $H(a) = \varphi$, then $\varphi(t_i) \neq t_i$, $1 \leqslant i \leqslant 3$. (If not we can assume without loss of generality that $\varphi(t_3) = t_3$. Then choose $t \notin a \cup e$ such that $\varphi(t) = t$, so that $\psi = (t_3; t)$ fixes φ and moves a, a contradiction since $\psi \in \mathrm{fix}(e)$.)

We now consider two cases: If $\varphi(t_i) \in a$ for $1 \leqslant i \leqslant 3$, then when φ is written as the product of disjoint cycles either $(t_1; t_2; t_3)$ or $(t_1; t_3; t_2)$ must be one of the cycles. In either case $\psi' = (t_1; t_2)$ fixes a and moves φ. Since $\psi' \in \mathrm{fix}(e)$, "$H$ is fixed by $\mathrm{fix}(e)$" is contradicted.

On the other hand, if $\varphi(t_i) \notin a$ for some i, $1 \leqslant i \leqslant 3$, we assume without loss of generality that $\varphi(t_3) \notin a$ and proceed as follows: Let $\psi'' = (t_2; t_3)$. Then ψ'', moves φ and fixes a while $\psi'' \in \mathrm{fix}(e)$, a contradiction. Therefore no such H exists, completing the proof of Theorem 2.17.

In our last permutation model we will show that $U! < 2^U$ where U is the set of urelements. In some sense this model is obtained from the ordered Mostowski model by adding lots of new subsets of U but no new permutations.

Suppose M' is a model of ZFU+AC and the set U of urelements of M' is countable and indexed as follows:

$$U = \{t(i, r): r \text{ rational and } i < \omega\}.$$

Define a partial ordering on U by

$$t(i, r) < t(j, s) \leftrightarrow i = j \quad \text{and} \quad r < s.$$

Then for each $i < \omega$, let $T^i = \{t(i, r): r \text{ rational}\}$. Let G be the following group of permutations of U:

$$G = \{\psi: (\forall i \in \omega)(\psi(T^i) = T^i \text{ and } (\forall s)(\forall r)(\psi(t(i, r)) < \psi(t(i, s)) \leftrightarrow t(i, r) < t(i, s))\}.$$

For each finite $e \subseteq U$, let

$$\mathrm{fix}(e) = \{\psi \in G: (\forall t \in e)(\psi(t) = t)\}.$$

Let $\mathfrak{F}$ be the filter of subgroups of G generated by the set $\{\mathrm{fix}(e): e \subseteq U \text{ and } e \text{ is finite}\}$. Let M be the permutation model determined by U and $\mathfrak{F}$. We leave to the reader the verification that $\mathfrak{F}$ is closed under conjugation by elements of G and the verification of the following two lemmas:

LEMMA 2.18. *If $\psi \in \mathrm{fix}(e \cap e')$, then there is an $n \in \omega$ and permutations $\psi_1, \ldots, \psi_n \in G$ such that $\psi = \psi_1 \ldots \psi_n$ and $\psi_i \in \mathrm{fix}(e)$ or $\psi_i \in \mathrm{fix}(e')$ for $1 \leqslant i \leqslant n$.*

LEMMA 2.19. *If $x \in M$, $\mathrm{fix}(e)$ fixes x and $\mathrm{fix}(e')$ fixes x, then $\mathrm{fix}(e \cap e')$ fixes x.*

(Lemma 2.18 follows from the fact that the same lemma holds in the ordered Mostowski model, and 2.19 is an easy consequence of 2.18.) As a consequence of Lemma 2.19 we get:

LEMMA 2.20. *Every $x \in M$ has a unique minimal support.*

LEMMA 2.21. *If e is a minimal support of x, then $\varphi(x) = x$ implies $\varphi(e) = e$.*

Proof. Suppose $\varphi(e) \neq e$ and that $\varphi(x) = x$. Then since $\varphi(e)$ is a support of $\varphi(x)$, $\varphi(e) \cap e$ is a support of x and $\varphi(e) \cap e \subsetneq e$, contradicting the minimality of e.

LEMMA 2.22. *If $e \subseteq U$ and $|e| = n < \omega$, then there are at most $n!$ permutations with minimal support e.*

This follows from:

LEMMA 2.23. *If $\varphi \in M$ is a permutation of U, then $\{t \in U: \varphi(t) \neq t\}$ is finite and is a minimal support of φ.*

LEMMA 2.24. *If $e \subseteq U$ is finite, then there are at least $2^{\aleph_0}$ subsets of U with minimal support e.*

Proof. Suppose $e \subseteq U$ and e is finite, and let $R = \{i \in \omega: T^i \cap e = \emptyset\}$. $R \in M$ and $|R| = \aleph_0$ (in M). Each set of the form $e \cup (\bigcup_{i \in J} T^i)$ where $J \subseteq R$ has minimal support e, and there are $2^{\aleph_0}$ such sets.

THEOREM 2.25. *In M, $U! < 2^U$.*

Proof. We first prove $U! \leqslant 2^U$. The proof is similar to the proof of Theorem 2.4. Define an equivalence relation $\sim$ on $\{b: b \subseteq U \text{ and } b \text{ is finite}\}$ by

$$b \sim b' \Leftrightarrow (\exists \psi)(\psi \in G \,\&\, \psi(b) = b').$$

Let $\mathfrak{G}$ be the set of equivalence classes and choose $b_c \in c$ for each $c \in \mathfrak{G}$. Then for each $c \in \mathfrak{G}$ let F_c be a 1-1 function from the set

$$\{\varphi: \varphi \text{ is a permutation of } U \text{ in } M \text{ with minimal support } b_c\}$$

into the set

$$\{A\colon A\subseteq U \,\&\, A \text{ has minimal support } b_c\}.$$

This is possible by Lemmas 2.22 and 2.24.

Now let

$$F = \bigcup \{\psi(F_c)\colon c\in\mathfrak{G} \text{ and } \psi\in G\}.$$

As in Theorem 2.4 we claim F is a 1-1 function from $S^M(U)$ into $\mathscr{P}^M(U)$ with support $\emptyset$. The proof is similar to the proof of the similar claim in Theorem 2.4. We show only that F is a function. Suppose $\big(\psi(\varphi), \psi(F_c(\varphi))\big)$ and $\big(\psi'(\varphi'), \psi'(F_{c'}(\varphi'))\big)$ are in F, where φ has minimal support b_c and φ' has minimal support $b_{c'}$ and $\psi, \psi'\in G$. Suppose further that $\psi(\varphi) = \psi'(\varphi')$. Then $\psi'^{-1}\psi(\varphi) = \varphi'$, whence by Lemma 2.21, $\psi'^{-1}\psi(b_c) = b_{c'}$. Thus $b_c\sim b_{c'}$ and it follows that $c = c'$. Therefore

$$(*)\qquad \psi'^{-1}\psi(b_c) = b_c$$

so $\psi'^{-1}\psi(\varphi) = \varphi$ and hence $\varphi = \varphi'$. By $(*)$, $\psi'^{-1}\psi\big(F_c(\varphi)\big) = F_c(\varphi)$, that is $\psi'^{-1}\psi\big(F_c(\varphi)\big) = F_{c'}(\varphi')$. Hence $\psi\big(F_c(\varphi)\big) = \psi'\big(F_{c'}(\varphi')$ and F is a function.

Now we prove that $U! \neq 2^U$ in M. Suppose $U! = 2^U$ in M and that H is a 1-1 correspondence between $S^M(U)$ and $\mathscr{P}^M(U)$ with minimal support e.

If $\varphi\in S^M(U)$ has minimal support $\subseteq e$, then $H(\varphi)$ must have minimal support $\subseteq e$. (Otherwise some $\psi\in\operatorname{fix}(e)$ moves $H(\varphi)$ and fixes φ, contradicting the fact that H is a 1-1 function with support e.) Similarly if $A\subseteq U$ has minimal support $\subseteq e$, then $H^{-1}(A)$ must have minimal support $\subseteq e$.

Therefore $F\restriction\{\varphi\in S^M(U)\colon \varphi \text{ has minimal support } \subseteq e\}$ is a 1-1 correspondence between that set and

$$\{A\in\mathscr{P}^M(U)\colon A \text{ has minimal support } e\},$$

which is impossible by Lemmas 2.22 and 2.24. This completes the proof of the theorem. Pincus has observed that the ZF-analogue of 2.25 can also be obtained by using the Halpern-Lévy model of [3].

As mentioned in the introduction, all of the foregoing consistency results carry over directly to ZF. This is a consequence of the Jech-Sochor Embedding Theorem ([4], p. 85), since our results involve only the set U of urelements and hence (unlike the independence result of Pincus [6] mentioned earlier) depend only on a proper initial segment of the given permutation models.

References

[1] N. Bourbaki, *Éléments de Mathémetique, Théorie des Ensembles*, Paris 1968.

[2] J. D. Halpern, *The independence of the axiom of choice from the Boolean prime ideal theorem*, Fund. Math. 55 (1964), pp. 57–66.

[3] — and A. Lévy, *The Boolean prime ideal theorem does not imply the axiom of choice*, in *Axiomatic Set Theory*, Proc. Symp. Pure Math. 13 (1) (Am. Math. Soc., Providence 1967).

[4] T. Jech, *The Axiom of Choice*, Amsterdam 1973.

[5] A. Mostowski, *Über die Unabhängigkeit des Wohlordnungssatzes vom Ordnungsprinzip*, Fund. Math. 32 (1939), pp. 201–252.

[6] D. Pincus, *A note on the cardinal factorial*, to appear.

[7] H. Rubin and J. Rubin, *Equivalents of the Axiom of Choice*, Amsterdam 1963.

[8] W. Sierpiński, *Cardinal and Ordinal Numbers*, Warszawa 1965.

PENNSYLVANIA STATE UNIVERSITY
University Park, Pennsylvania
EASTERN MICHIGAN UNIVERSITY
Ypsilanti, Michigan

Accepté par la Rédaction le 14. 11. 1974