PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 27, Number 1, January 1971

CHOICES FROM FINITE SETS AND CHOICES OF FINITE SUBSETS

MARTIN M. ZUCKERMAN

ABSTRACT. In set theory without the axiom of choice we prove a consistency result involving certain "finite versions" of the axiom of choice. Assume that it is possible to select a nonempty finite subset from each nonempty set. We determine sets Z, of integers, which have the property that $n \in Z$ is a necessary and sufficient condition for the possibility of choosing an element from every n-element set. Given any nonempty set P of primes, the set Z_p, consisting of integers which are not "linear combinations" of primes of P, is such a set Z.

1. **Introduction.** Let σ be the system of set theory of [4]. This is a system of the Gödel-Bernays type which permits the existence of urelemente (objects in the domain, but not the range of the ϵ-relation) and which does not include among its axioms the axiom of choice.

By AC (the axiom of choice) we mean the statement of σ: "For every nonempty set X of nonempty sets there is a function f defined on X such that $f(x) \in x$ for each $x \in X$." We consider various "finite versions" of the axiom of choice. Let FS be the statement: "For every nonempty set X of nonempty sets there is a function f defined on X such that $f(x)$ is a nonempty finite[1] subset of x for each $x \in X$." Identify nonnegative integers with finite Von Neumann ordinals. For each positive integer n let $C(n)$ be the statement: "For every nonempty set X of n-element sets there is a function f defined on X such that $f(x) \in x$ for each $x \in X$." Thus $C(1)$ is a (trivial) theorem of σ. For a subset $Z = \{z_0, z_1, \cdots, z_{k-1}\}$ of integers $\geqq 2$, let $C(Z)$ be the conjunction of the statements $C(z_i)$, $i \in k$.

We are concerned with the following problem. Assume σ is consistent. For which sets Z of integers $\geqq 2$ is the set of axioms

$$(1) \qquad \sigma \cup \{\neg \mathrm{AC}, \mathrm{FS}, (\forall n \geqq 2)(C(n) \leftrightarrow n \in Z)\}$$

also consistent. Let $\mathcal{Z}$ be the set of sets Z for which (1) holds.

Received by the editors March 14, 1969.

AMS 1970 *subject classifications*. Primary 02K05, 02K20, 02A20, 02A25; Secondary 05A05.

Key words and phrases. Axiom of choice for n-element sets, multiple choice axioms, Fraenkel-Mostowski models, relative consistency.

[1] A set A is *finite* iff every nonempty set of subsets of A has a maximal element with respect to inclusion; otherwise, A is infinite.

Copyright © 1971, American Mathematical Society

For each positive integer n, let I_n be the set of integers $\geqq n$. Theorem 6 of [2] shows that $I_2 \in \mathcal{Z}$; Theorem 1 of [6] implies that 0 (the empty set) is in $\mathcal{Z}$. If P is any nonempty set of primes, let Lin Comb P be the set of positive integers of the form $k_0p_0 + k_1p_1 + \cdots + k_{s-1}p_{s-1}$, where $s \in I_1$ and for each $i \in s$, $k_i \in I_0$ and $p_i \in P$. The main result of the present paper shows that if P is any (nonempty) set of primes and if $Y = I_2 \backslash$Lin Comb P, then $Y \in \mathcal{Z}$.[2] It is well known that if P contains more than two primes and if p and q are the two smallest primes of P, then $I_{(p-1)(q-1)} \subseteq$Lin Comb P. Thus we need only consider finite sets of primes.

We prove our theorem by constructing a Fraenkel-Mostowski model of set theory; we employ a variation of the technique used in [2] and [6]. As an immediate corollary of our theorem we have a direct proof of the necessity of Mostowski's condition (M) (defined below) for an implication of the form $C(Z) \rightarrow C(n)$ to be provable in σ.

2. The model.

THEOREM. *Assume σ is consistent. Let P be any nonempty finite set of primes and let $Y = I_2 \backslash$Lin Comb P. Then there is a model of*

$$\sigma \cup \{\neg \mathrm{AC}, \mathrm{FS}, (\forall n \geqq 2)(C(n) \leftrightarrow n \in Y)\}.^{3}$$

PROOF. Let σ^* be σ together with the axiom of choice and an axiom asserting the existence of a denumerable set of urelemente. σ^* is relatively consistent with σ (see [2, pp. 478–479]); we shall work within σ^*.

Let $\mathfrak{M}$ be a denumerable set of urelemente. Define $\mathfrak{M}_0$ to be $\mathfrak{M}$ and for each ordinal number $\eta > 0$, let $\mathfrak{M}_\eta = \mathfrak{M} \cup \bigcup \{\mathcal{P}(\mathfrak{M}_\mu) : \mu \in \eta\}$.

Let $\mathcal{G}_0$ be the group of all one-one transformations of $\mathfrak{M}$ onto itself. By transfinite induction, if $x \in \mathfrak{M}_\eta \backslash \bigcup \mathfrak{M}_\zeta$ $(\zeta \in \eta)$ for some $\eta > 0$ and if $\phi \in \mathcal{G}_0$, we "extend" ϕ by letting $\phi(x) = \{\phi(y) : y \in x\}$.

Let $P = \{p_0, p_1, \cdots, p_{s-1}\}$. Let T be the subset of $I_0 \times I_0$ consisting of all ordered pairs $\langle i, t\rangle$, where i ranges over I_0 and where $t \in p_j$ if $i \equiv j \pmod{s}$. Since T is denumerable, there is a one-one correspondence between T and $\mathfrak{M}$. With respect to any such one-one correspondence, let $\mathfrak{m}_{i,t}$ be the member of $\mathfrak{M}$ which corresponds to $\langle i, t\rangle$.

[2] This result was also obtained, independently, by D. Pincus.

[3] It was remarked in [2, p. 478] that using Mendelson's technique of [3], Theorem 6 of [2] can be proved with "Gödel's system A, B, C" replacing "σ" in the hypothesis or conclusion. The same remark applies to Theorem 1 of [6] and to our present theorem.

For each $i \in I_0$ and $j \in s$, let $q_i = p_j$ if $i \equiv j \pmod{s}$ and let $\mathfrak{M}^{(i)} = \{\mathfrak{m}_{i,t} : t \in q_i\}$. Then $\mathfrak{M}$ is the pairwise disjoint union of the $\mathfrak{M}^{(i)}$, $i \in I_0$. Let χ_i be the element of $\mathcal{G}_0$ which maps $\mathfrak{m}_{j,t}$ into itself for $j \neq i$, and which maps $\mathfrak{m}_{i,t}$ into $\mathfrak{m}_{i,u}$ for $t, u \in q_i$ and $u \equiv t+1 \pmod{q_i}$. Let $\mathcal{G}_1$ be the subgroup of $\mathcal{G}_0$ generated by $\{\chi_i : i \in I_0\}$. If Z is a finite set of integers and if $\phi \in \mathcal{G}_1$; then ϕ is said to be *Z-identical* if $\phi(\mathfrak{m}_{i,t}) = \mathfrak{m}_{i,t}$ for every pair $\langle i, t\rangle$ for which $i \in Z$. If $x \in \mathfrak{M}_\eta$ for some ordinal number η, then x is said to be *Z-symmetric* if $\phi(x) = x$ for every Z-identical $\phi \in \mathcal{G}_1$.

For each ordinal number η, we define $\mathcal{K}_\eta$ by transfinite induction: $\mathcal{K}_0 = \mathfrak{M} \cup \{0\}$, and for each $\eta > 0$,

$$x \in \mathcal{K}_\eta \leftrightarrow (\forall y \in x)(\exists \xi \in \eta)(y \in \mathcal{K}_\xi)$$
$$\wedge\ (x \text{ is } Z\text{-symmetric with respect to some finite set } Z \subset I_2).$$

x is said to be an *$\mathfrak{M}$-element* if there exists an ordinal number η such that $x \in \mathcal{K}_\eta$. A class X is called an *$\mathfrak{M}$-class* if every element of X is an $\mathfrak{M}$-element and if there is a finite set Z of integers with the property that for every Z-identical $\phi \in \mathcal{G}_1$, $\phi(y) \in X$ for every $y \in X$. If X and Y are classes, define $X \in_{\mathfrak{M}} Y$ to be true iff X is an $\mathfrak{M}$-element, Y is an $\mathfrak{M}$-class and $X \in Y$. Then, if we interpret σ in σ^* by replacing the primitive notions "element," "class," "$\in$," and "0" by the notions "$\mathfrak{M}$-element," "$\mathfrak{M}$-class," "$\in_{\mathfrak{M}}$," and "0," respectively, all of the axioms and theorems of σ will become theorems of σ^*.

For a discussion of Fraenkel-Mostowski models, and in particular for a verification of some of the axioms in these models, see [4] and [5]. [2] and [6] discuss absoluteness in these models. The verification of FS (called "$Z(\infty)$") is carried out in [2] and applies to the present model.

We now show that if $n \in \text{Lin Comb } P$, then $C(n)$ is false in the model. For each such n, let $k_0, k_1, \cdots, k_{s-1}$ be any integers for which $n = k_0p_0 + k_1p_1 + \cdots + k_{s-1}p_{s-1}$. Delete the zero terms and write this sum as

$$n = k_{i_0}p_{i_0} + k_{i_1}p_{i_1} + \cdots + k_{i_v}p_{i_v}, \qquad 0 \leqq i_0 < i_1 < \cdots < i_v < s.$$

Let

$$x_n = \left\{ \bigcup_{j=0}^{v} \bigcup_{l=mk_{i_j}}^{(m+1)k_{i_j}-1} \mathfrak{M}^{(i_j+ls)} : m \in I_0 \right\}.$$

Then x_n is a set of n-element sets. Clearly, $x_n \in \mathfrak{M}_2$; moreover, x_n is 0-symmetric, and it is, consequently, in $\mathcal{K}_2$. Suppose that f is a choice function on x_n. Then f must be Z-symmetric for some finite $Z\subset I_0$. For $m\in I_0$, let

$$R_m = \{i_j + ls : l = mk_{i_j}, mk_{i_j} + 1, \cdots, (m+1)k_{i_j} - 1; \quad j = 0, 1, \cdots, v\}.$$

Let m_0 be the smallest integer m for which $Z\cap R_m = 0$. Then for each $r\in R_{m_0}$, χ_r is Z-identical and, hence, $\chi_r(f) = f$. Let

$$(x_n)_{m_0} = \bigcup_{j=0}^{v} \bigcup_{l=m_0k_{i_j}}^{(m_0+1)k_{i_j}-1} \mathfrak{M}^{(i_j+ls)}.$$

Now since $f((x_n)_{m_0}) = (x_n)_{m_0}$ and since the $\mathfrak{M}^{(j)}$ are pairwise disjoint, it follows that $f((x_n)_{m_0}) \in \mathfrak{M}^{(r)}$ for some unique $r\in R_{m_0}$, and, consequently, that $f((x_n)_{m_0}) = \mathfrak{m}_{r,t}$ for some $t\in q_r$. Thus $\langle (x_n)_{m_0}, \mathfrak{m}_{r,t}\rangle \in f$. But then $\langle (x_n)_{m_0}, \chi_r(\mathfrak{m}_{r,t})\rangle = \chi_r(\langle (x_n)_{m_0}, \mathfrak{m}_{r,t}\rangle) \in \chi_r(f) = f$; since $\chi_r(\mathfrak{m}_{r,t}) \neq \mathfrak{m}_{r,t}$, f cannot be a function.

It remains to show that if $n\notin$ Lin Comb P, then $C(n)$ is true in the model. Let X be a nonempty $\mathfrak{M}$-set of n-element sets x. Then $X \in \mathcal{K}_{\alpha+1}\setminus\mathcal{K}_\alpha$ for some $\alpha \geqq 1$, and X is Z-symmetric for some finite $Z\subset I_0$. Let $\mathcal{G}^Z$ be the subgroup of $\mathcal{G}_1$ consisting of all Z-identical maps. Then for each $\phi\in\mathcal{G}^Z$, $X = \phi(X) = \{\phi(x) : x\in X\}$.

We first show that

(2) for each $x\in X$, there is an $a\in x$ with the property that whenever $\phi, \psi \in \mathcal{G}^Z$ and $\phi(x) = \psi(x)$, then $\phi(a) = \psi(a)$.

Equivalently, we show that for each $x\in X$ there is an $a\in x$ with respect to which $\phi\in\mathcal{G}^Z$ and $\phi(x) = x$ together imply $\phi(a) = a$.

Suppose $X\in\mathcal{K}_2\setminus\mathcal{K}_1$ and $x\in X$. Then the elements of x are in $\mathcal{K}_0$. If $0\in x$, then $\phi(0) = 0$ for every $\phi\in\mathcal{G}^Z$; if $\mathfrak{m}_{i,t}\in x$ for some $i\in Z$, then $\phi(\mathfrak{m}_{i,t}) = \mathfrak{m}_{i,t}$ for every $\phi\in\mathcal{G}^Z$. Otherwise, x consists of n urelemente in $\mathfrak{M}_0\setminus\bigcup_{i\in Z}\mathfrak{M}^{(i)}$. Now each $\mathfrak{M}^{(j)}$ consists of q_j elements for some $q_j\in P$, whereas $n\notin$ Lin Comb P. Thus for some j, $x\cap\mathfrak{M}^{(j)}$ is a nonempty proper subset of $\mathfrak{M}^{(j)}$. Pick any such j and any $\mathfrak{m}_{j,t}\in x$. For any $\phi\in\mathcal{G}^Z\setminus\mathcal{G}^{\{j\}}$, if $\phi(\mathfrak{m}_{j,t}) \neq \mathfrak{m}_{j,t}$, then $\phi(\mathfrak{m}_{j,t}) = \mathfrak{m}_{j,u}$ for some $u\in s\setminus\{t\}$. Thus $\phi(x\cap\mathfrak{M}^{(j)}) = \{\mathfrak{m}_{j,v}$: some $\mathfrak{m}_{j,w}\in x$ and $v - w \equiv u - t \pmod{q_j}\} \neq x\cap\mathfrak{M}^{(j)}$, and since $\phi(x\setminus\mathfrak{M}^{(j)})\cap\mathfrak{M}^{(j)} = 0$, it follows that $\phi(x)\neq x$.

For any $\mathfrak{M}$-set Y, let $\Sigma_0(Y) = Y$ and for ordinal numbers $\xi > 0$ let $\Sigma_\xi(Y) = Y\cup\{y$: for some $\eta<\xi$ and some $z\in\Sigma_\eta(Y)$, $y\in z\}$. (Properties of the $\Sigma_\xi(Y)$ are discussed in [4].)

Let $\Sigma(Y)=\{z:z\in\Sigma_\xi(Y)$ for some ordinal number $\xi\}$.

An element of $\mathcal{K}_0\cap\Sigma(Y)$ will be called a *progenitor of* Y.

A transfinite induction argument shows that for any $\phi\in\mathcal{G}^Z$ and $\mathfrak{M}$-set Y, a necessary condition that $\phi(Y)=Y'$ is that Y and Y' have the same number of progenitors in each $\mathfrak{M}^{(j)}$, $j\in I_0$.

Now let $X\in\mathcal{K}_{\alpha+1}\setminus\mathcal{K}_\alpha$ for $\alpha>1$, and let $x\in X$. We may assume that either $x\cap\mathcal{K}_0=0$ or else that the number of elements of $x\cap\mathcal{K}_0$ is in Lin Comb P; otherwise, the previous argument applies. Suppose that for $\phi\in\mathcal{G}^Z$ we have $\phi(x)=x$ but $\phi(a)\neq a$ for every $a\in x$. Let $a_1\in x\setminus\mathcal{K}_0$. Then, surely, for some progenitor $\mathfrak{m}_{i,t}$ of a_1 (and hence of x), $\phi(\mathfrak{m}_{i,t})\neq\mathfrak{m}_{i,t}$. Now for every $a\in x$, $\phi(a)\in x$. Thus for some positive integer h_{i_1}, $x\setminus\mathcal{K}_0$ must contain $h_{i_1}\,q_{i_1}$ elements, with progenitors in $\mathfrak{M}^{(i_1)}$, which are cyclically permuted by ϕ. Since $n\notin$Lin Comb P, and x contains n elements, there must be an element a_2 in $x\setminus\mathcal{K}_0$ distinct from these $h_{i_1}\,q_{i_1}$ elements. Repeat the above argument for a_2 and obtain $h_{i_2}\,q_{i_2}$ elements of $x\setminus\mathcal{K}_0$ for $q_{i_2}\in P$, $h_{i_2}\geqq 1$. These new elements are distinct from the previous ones; again, these $h_{i_1}\,q_{i_1}+h_{i_2}\,q_{i_2}$ elements cannot exhaust $x\setminus\mathcal{K}_0$. Clearly, in a finite number, r, of steps we will obtain $\sum_{j=1}^r h_{i_j}\,q_{i_j}$ distinct elements of $x\setminus\mathcal{K}_0$, where for $j=1, 2,\cdots,r$, $h_{i_j}\geqq 1$ and the q_{i_j} are (not necessarily distinct) primes of P, and where $\sum_{j=1}^r h_{i_j}\,q_{i_j}>n$. This contradicts the assumption that x has n elements and completes the proof of (2).

Define the relation R on X by $x_1\,R\,x_2$ iff there is some $\phi\in\mathcal{G}^Z$ for which $\phi(x_1)=x_2$. R is obviously an equivalence relation on X. Choose an element x_C from each cell C of the partition X/R; choose an element a_C in each such chosen x_C with the property that whenever $\phi(x_C)=\psi(x_C)$, ϕ, $\psi\in\mathcal{G}^Z$, then $\phi(a_C)=\psi(a_C)$. Let $f_C=\{\langle\phi(x_C),\ \phi(a_C)\rangle:\phi\in\mathcal{G}^Z\}$. Each such f_C is a function with domain C. Clearly $f_C\in\mathfrak{M}_{\alpha+3}$. Moreover, f_C is Z-symmetric because for $\psi\in\mathcal{G}^Z$, $\psi(f_C)=\{\langle\psi\phi(x_C),\ \psi\phi(a_C)\rangle:\phi\in\mathcal{G}^Z\}=f_C$. Thus $f_C\in\mathcal{K}_{\alpha+3}$. Let $f=\bigcup_{C\in X/R} f_C$; f is also Z-symmetric and is in $\mathcal{K}_{\alpha+3}$. f is the desired choice function for X.

A finite subset $Z\subset I_2$ and an integer $n\in I_2$ are said to satisfy *condition* (M) iff for every finite set P of primes, $n\in$Lin Comb P implies $Z\cap$Lin Comb $P\neq 0$.

In [5], Mostowski proves the necessity of condition (M) for the implication $C(Z)\to C(n)$ to hold in σ by first considering the following condition (K), which we proceed to define.

For $n\geqq 1$, let $\mathcal{S}_n$ be the symmetric group on $\{1, 2,\cdots,n\}$. If $\mathcal{G}$ is a subgroup of $\mathcal{S}_n$, if $1\leqq k\leqq n$, and if $\phi(k)=k$ for every $\phi\in\mathcal{G}$, we say that k is a *fixed-point of* $\mathcal{G}$. For any group $\mathcal{G}$, let $\mathcal{G}^\omega$ denote the group whose elements are those infinite sequences, $\langle g_1,\ g_2,\cdots\rangle$, whose terms belong to $\mathcal{G}$ and which are such that almost all of the g_n are equal to the unity of $\mathcal{G}$; multiplication in $\mathcal{G}^\omega$ is defined by termwise multiplication in $\mathcal{G}$. A finite subset Z of I_1 and an $n \in I_1$ satisfy *condition* (K) if for every subgroup $\mathcal{G}$ of $\mathcal{S}_n$ without fixed-points there is a group $\mathcal{K} \subset \mathcal{G}^\omega$ and a finite number r of (not necessarily different) proper subgroups $\mathcal{L}_1, \mathcal{L}_2, \cdots, \mathcal{L}_r$ of $\mathcal{K}$ such that

$$\sum_{i=1}^{r} \operatorname{Ind}(\mathcal{K}/\mathcal{L}_i) \in Z.$$

The model constructed in [5] proves that (K) is necessary for $C(Z) \to C(n)$ to hold in σ; it is then shown that if Z and n satisfy (K) they also satisfy (M).

As an immediate consequence of our theorem we obtain:

COROLLARY 1. *Condition* (M) *is necessary for the implication* $(\mathrm{FS} \wedge C(Z)) \to C(n)$ *to hold in* σ.

By taking P to consist of a single prime we obtain:

COROLLARY 2. *For each prime p, there is a model for*

$$\sigma \cup \{\neg \mathrm{AC}, \mathrm{FS}, (\forall n \geqq 2)(C(n) \leftrightarrow (n \textit{ is not a multiple of } p))\}.$$

Thus there is a model $\mathfrak{M}$ in which the set Z of integers n for which $C(n)$ is true in $\mathfrak{M}$ as well as the set Y of n for which $C(n)$ is false in $\mathfrak{M}$, are both infinite.

REFERENCES

1. K. Gödel, *The consistency of the axiom of choice and of the generalized continuum hypothesis with the axioms of set theory*, 6th ed., Ann. of Math. Studies, no. 3, Princeton Univ. Press, Princeton, N. J., 1964.

2. A. Lévy, *Axioms of multiple choice*, Fund. Math. **50** (1962), 475–483.

3. E. Mendelson, *The independence of a weak axiom of choice*, J. Symbolic Logic **21** (1956), 350–366. MR **18**, 864.

4. A. Mostowski, *Über die Unabhängigkeit des Wohlordnungssätzes vom Ordnungsprinzip*, Fund. Math. **32** (1939), 201–252.

5. ———, *Axiom of choice for finite sets*, Fund. Math. **33** (1945), 137–168. MR **8**, 3.

6. M. M. Zuckerman, *Multiple choice axioms*, Proc. Sympos. Pure Math., vol. 13, Amer. Math. Soc., Providence, R. I., 1970.

CITY COLLEGE OF THE CITY UNIVERSITY OF NEW YORK, NEW YORK, NEW YORK 10031