PACIFIC JOURNAL OF MATHEMATICS
Vol. 28, No 1, 1969

A UNIFYING CONDITION FOR IMPLICATIONS AMONG THE AXIOMS OF CHOICE FOR FINITE SETS

MARTIN M. ZUCKERMAN

For $n \geq 1$, let $C(n)$ be the axiom of choice restricted to sets of n-element sets. We define a condition, (Z), which is sufficient to assure the provability of an implication

$$(C(m_1)\ \&\ C(m_2)\ \&\ \cdots\ \&\ C(m_s)) \longrightarrow C(n)$$

in set theory. We compare condition (Z) with various other conditions related to the above implication.

1. Notation and preliminaries. Let σ be the set theory of [3]; this is a set theory of the Gödel-Bernays type which permits the existence of urelemente (objects, other than the null set, which are in the domain, but not the range, of the $\in$-relation) and which does include the axiom of choice among its axioms. Our independence statements will assume that σ is consistent; this is equivalent to the assumption that Gödel's system A, B, C, of [2], is consistent. Our logical framework is the first-order predicate calculus with identity.

By the nonnegative integers we mean the Von-Neumann integers, i.e., 0 is the empty set, $1 = \{0\}, 2 = 1 \cup \{1\}, 3 = 2 \cup \{2\}$, etc. For each such n, we let I_n be the set of all integers $\geqq n$ and we let J_n be the relative complement of I_{n+1} in I_1, $I_1 \backslash I_{n+1}$. We let Π represent the set of prime numbers, and we let $\Pi_n = \Pi \cap I_n$.

If there is a function (which is itself a set) which maps the set x one-one onto the positive integer n, then x is called an *n-element set*; in this case we let $n(x)$ denote the unique integer n for which such a mapping exists.

DEFINITION 1. For $n \in I_1$ let $C(n)$ denote the following statement of set theory: "For every set x of n-element sets there is a function f defined on x such that for each $y \in x, f(y) \in y$. The statements $C(n)$ are called the *axioms of choice for n-element sets* or simply the *axioms of choice for finite sets*.

For any set x let $\mathscr{P}(x)$ denote the power set of x and let $\mathscr{P}^{\#}(x)$ designate the set consisting of 0 together with the set of all n-element subsets of x for $n \in I_1$. For $Z \in \mathscr{P}^{\#}(I_1)$, let $C(Z)$ be the conjunction of the statements $C(z), z \in Z$. Since a positive integer is not a subset of I_1, no confusion will result from our usage of $C(n)$ instead of $C(\{n\})$.

We shall be concerned with implications of the form

$$(1) \qquad C(Z) \longrightarrow C(n)$$

which are provable in the set theory σ; when this is the case we shall let (1) abbreviate the statement "The implication (1) is provable in σ." (In general, we shall omit the phrase, "is provable in σ.")

In [4], Mostowski introduces the following condition which he shows to be necessary for (1):

DEFINITION 2. $Z(\in \mathscr{P}^*(I_1))$ together with $n(\in I_1)$ satisfy *condition* (M) if for any decomposition of n into a sum of (not necessarily distinct) primes,

$$n = p_1 + p_2 + \cdots + p_s ,$$

there are $r_1, r_2, \cdots, r_s$ in I_0 such that

$$r_1p_1 + r_2p_2 + \cdots + r_sp_s \in Z .$$

In § 23 of [4] Mostowski states four lemmas with the aid of which, in Theorem IX, he proves the sufficiency of condition (M) for the implication (1) in certain special cases. The first three of these lemmas (13, 14, and 15) are sufficiently powerful to yield all but one of the numerical implications given in [5], [6], pp. 97–103, and in [7],[1] as well as several of the cases of Theorem IX of [4]. Moreover, various implicational results which were proved by other methods in [4] and [5] could have been proved by means of Lemmas 13, 14, and 15. We define condition (Z) inductively in terms of these three lemmas; this condition will have all of the above properties and will be intermediate in strength between conditions (M) and (S) (see Definition 5, below).

2. Condition (Z).

We first state the three lemmas in question, modifying the notation and wording.

(2) ([4], Lemma 13) $(\forall n, k \in I_1)(C(nk) \longrightarrow C(k))$.[2]

(3) ([4], Lemma 14) *If* $\boldsymbol{n}(A) = m(\in I_1)$,

$\boldsymbol{n}(B) = n(\in I_1)$, $A \cap B = 0$, *and if we know how to realize the proposition* $C(km + ln)$, *where* $k, l \in I_0$ *and* $k + l \in I_1$, *then we can choose an element from* $A \cup B$.

---

[1] Except for some minor revisions, the section in **[6]** is a translation of **[5]**. The exception noted is $C(\{3, 7\}) \to C(9)$; this is proved by different methods in **[4]** and **[5]**. A third proof is given by J. H. Conway (unpublished). Each of these proofs utilizes something in addition to Lemmas 13, 14, and 15 and apparently cannot be proved on the basis of our condition (Z). However, we remark that condition (Z) is sufficient in the case of the implication $C(\{3, 13\}) \to C(9)$.

We note that the implication $C(\{2, 3, 13\}) \to C(14)$ (**[5]**, p. 98) is false. (Undoubtedly, this is a misprint; in **[6]**, p. 102, this is replaced by the (valid) implication $C(\{2, 3, 7\}) \to C(14)$.) Further, the implication $C(\{2, 3, 5, 17, 13\}) \to C(32)$ (**[6]**, p. 103, Example 3), is false as is stated and, most likely, was intended as $C(\{2, 3, 5, 7, 13\}) \to C(32)$.

[2] The proof of this lemma, which is attributed to A. Tarski, is given in **[6**, p. 99**]**.

(4) ([4], Lemma 15)[3] *If* $p \in \Pi$, $\boldsymbol{n}(A) = mp$ *for* $m \in I_2$, *and if we know how to realize the proposition* $C(p)$, *then we can define effectively a decomposition of* A *into a union of two disjoint, nonempty sets.*

DEFINITION 3. For $Z \in \mathscr{P}^{\#}(I_1)$ and $n \in I_1$, n is a *Z-number* provided either $(\mathrm{i})_{\mathrm{a}}$ & $(\mathrm{i})_{\mathrm{b}}$ or else (ii) holds:

$(\mathrm{i})_{\mathrm{a}}$ There is a $z \in Z$ such that $(n, z) > 1$.

$(\mathrm{i})_{\mathrm{b}}$ Whenever $n = n_1 + n_2$, $n_1, n_2 \in I_2$, then there are r_1, r_2 in I_0 such that $r_1 n_1 + r_2 n_2 \in Z$.

(ii) $n = 1$.

DEFINITION 4. $Z(\in \mathscr{P}^{\#}(I_1))$ and $n(\in I_1)$ satisfy *condition* (Z) if either (i) or else $(\mathrm{ii})_{\mathrm{a}}$ & $(\mathrm{ii})_{\mathrm{b}}$ holds:

(i) n is a Z-number.

$(\mathrm{ii})_{\mathrm{a}}$ There is a $z \in Z$ such that $(n, z) > 1$.

$(\mathrm{ii})_{\mathrm{b}}$ Whenever $n = n_1 + n_2$, $n_1, n_2 \in I_2$, either Z and n_1 satisfy (Z) or else Z and n_2 satisfy (Z).

If $Z(\in \mathscr{P}^{\#}(I_1))$ and $n(\in I_1)$ satisfy $(\mathrm{ii})_{\mathrm{a}}$ and $(\mathrm{ii})_{\mathrm{b}}$, but not (i), of Definition 4, we shall say that Z and n properly satisfy condition (Z).

We note that if n is a Z-number and $n = n_1 + n_2$, $n_1, n_2 \in I_2$, it does not follow that either Z and n_1 or Z and n_2 satisfy (Z); for instance, let $Z = \{25\}$ and $n = 5$.

LEMMA 1. *If* $n \in \Pi \cup \{1, 4, 6\}$ *and* $Z \in \mathscr{P}^{\#}(I_1)$, *then* Z *and* n *satisfy condition* (Z) *if and only if* n *is a* Z*-number.*

LEMMA 2. *If* n *is an even integer and if* $Z(\in \mathscr{P}^{\#}(I_1))$ *contains only odd integers, then* Z *and* n *fail to satisfy condition* (Z).

Proof. Let Z be a nonempty, finite set of odd integers. $n = 2$ fails to meet condition $(\mathrm{i})_{\mathrm{a}}$ of Definition 3 and, thus, by Lemma 1, Z and 2 cannot satisfy (Z). For $n(\text{even}) \in I_4$, $2s_1 + (n-2)s_2$ is even for all $s_1, s_2 \in I_0$; hence condition $(\mathrm{i})_{\mathrm{b}}$ of Definition 3 fails. The proof that Z and $n = 2k$, $k \in I_1$, cannot satisfy (Z) follows by a routine induction on k.

THEOREM 1. *Condition* (Z) *is sufficient for the implication* $C(Z) \to C(n)$.

[3] The proof of Lemma 15 in [**4**] erroneously refers to divisibility by p, instead of by np, in each of the first two lines on p. 165. The proof is correctly carried out in [**5**, pp. 99-100].

Proof. (by induction on n).

The result is immediate for $n = 1$ since, in fact, $C(1)$ is a (trivial) theorem of set theory. Suppose for all $k < n$ and for all $Z' \in \mathscr{P}^{\#}(I_1)$ that whenever Z' and k satisfy (Z), then $C(Z') \to C(k)$.

Case 1. n is a Z-number:

By $(\mathrm{i})_{\mathrm{a}}$ of Definition 3 and (2), $C(p)$ is true if p is the smallest prime divisor of (n, z) as z ranges over all elements of Z for which $(n, z) > 1$. If n is prime, we are finished.

Otherwise, let X be a nonempty set of pairwise disjoint n-element sets, let $X_{(p)}$ be the set of p-element subsets of elements of X, and let f by any choice function on $X_{(p)}$. Then, by (4), in terms of f we can define a function F on X such that for each $x \in X$, $F(x) = \{x_1, x_2\}$, where x_1 and x_2 are nonempty, disjoint sets whose union is x. Define the following equivalence relation on X: $x \approx x'$ if an element of $F(x)$ is equipotent with an element of $F(x')$. Let Y be the corresponding partition on X. For each $y \in Y$ define a choice function g_y on y as follows: if for each $x \in y$, $f(x)$ contains a unit set $\{a\}$ (it can contain only one such), let $g_y(x) = a$; otherwise, y is such that for each $x \in y$ and each $x_i \in F(x)$, $\boldsymbol{n}(x_i) \in I_2$.

Using $(\mathrm{i})_{\mathrm{b}}$ of Definition 3, let s_1 and s_2 be any nonnegative integers such that for all $x \in y$ and $x_1, x_2 \in F(x)$, $s_1 \cdot \boldsymbol{n}(x_1) + s_2 \cdot \boldsymbol{n}(x_2) \in Z$. By (3), there is a function g_y defined on y such that $g_y(x) \in x$ for each $x \in y$. Then $G = \bigcup g_y(y \in Y)$ is a choice function on X; hence $C(n)$ is true.

Case 2. Z and n properly satisfy condition (Z):

The first two paragraphs of Case 1 apply here with the exception that n cannot be prime (by Lemma 1). In the present case, if y is such that for each $x \in y$ and each $x_i \in F(x)$, $\boldsymbol{n}(x_i) \in I_2$, then either Z and $\boldsymbol{n}(x_1)$ satisfy (Z) or else Z and $\boldsymbol{n}(x_2)$ satisfy (Z).

If $\boldsymbol{n}(x_1)$ and $\boldsymbol{n}(x_2)$ are distinct and if $\{i, j\} = \{1, 2\}$, let $x_3 = x_i$ if Z and $\boldsymbol{n}(x_i)$ satisfy (Z) but Z and $\boldsymbol{n}(x_j)$ do not, or if Z and $\boldsymbol{n}(x_j)$ (as well as Z and $\boldsymbol{n}(x_i)$) satisfy (Z) but $\boldsymbol{n}(x_i) < \boldsymbol{n}(x_j)$. In this case let $A_y = \{x_3 : x_3 \subset x \in y\}$. By the inductive hypothesis, there is a function G_y defined on A_y such that $G_y(x_3) \in x_3$, $x_3 \in A_y$; hence there is a function g_y defined on y such that $g_y(x) \in x$, $x \in y$.

Now if $\boldsymbol{n}(x_1) = \boldsymbol{n}(x_2)$, then $n = \boldsymbol{n}(x_1) + \boldsymbol{n}(x_2)$ is even; by Lemma 2, Z must contain an even integer, z_0. Thus $C(2)$ is true; we can select one of the sets x_1 or x_2, and proceed as in the preceding paragraph.

Finally, we again have $G = \bigcup g_y(y \in Y)$ as a choice function on X.

Theorem 1 provides a convenient alternative proof of various theorems, as well as a unified method of obtaining certain results which depend on Lemmas 13, 14 and 15 of [4]. We give some examples:

(i) $C(2) \to C(4)$. (4 is a $\{2\}$-number.)[4]

(ii) $C(J_m) \to C(J_n)$ if there is no prime p such that $m < p \leqq n$.[5] (Using Bertrand's postulate, [8, pp. 51–64], we see that each $k \in J_n$ is a J_m-number.)

(iii) For any $n \in I_1$, let T_n be the set of composites of J_n. Then $C(\Pi \cap J_p) \to C(T_{2n+1})$ if there is no prime q satisfying $p < q \leqq n$.[6] ($\Pi \cap J_p$ together with each $k \in T_{2n+1}$ satisfy (Z).)

$(\mathrm{iv})_a$ $C(\{3, 13\}) \to C(9)$. (9 is a $\{3, 13\}$-number.)

$(\mathrm{iv})_b$ $C(\{2, 3, 7\}) \to C(14)$.[7] ($\{2, 3, 7\}$ and 14 (properly) satisfy (Z).)

(v) For any $Z \in \mathscr{P}^{\#}(I_1)$, condition (M) is sufficient for an implication of the form $C(Z) \to C(n)$, whenever $n \in \Pi \cup \{4, 6, 8, 10, 12, 18, 30\}$.[8] (Whenever Z and n satisfy (M), they also satisfy (Z).)

In connection with example (v), we see that although (Z) is necessary for an implication $C(Z) \to C(n)$ whenever $n \in \Pi \cup \{4,6,8,10,12,18,30\}$, (Z) is not necessary for such an implication in the general case. In fact, $\{2, 5, 11, 13, 17\}$ and 20 satisfy (M), and, hence, by Rubin's extension of Theorem IX of [4],[9] $C(\{2, 5, 11, 13, 17\}) \to C(20)$, but they fail to satisfy (Z). (The successive decompositions—$20 = 6 + 14$; $6 = 3 + 3$, $14 = 7 + 7$—indicate the failure of (Z).) Similarly, counterexamples exist for $n = 9, 14, 16, 24$, and 42.[10]

The preceding example further illustrates that condition (Z) is also weaker than the combined strength of the sufficiency conditions implicit in the lemmas (13, 14, and 15 of [4]) upon which (Z) is based.[11] Using $C(2)$, we could choose a 3-element set (in the second decomposition) and using $C(17)$ we could pick an element from among the remaining elements. Our condition makes no provision for either of these devices. Another example will be afforded by Theorem 5 of [10].

3. (Z) in relation to other conditions.

We consider two other conditions, each of which is sufficient for the implication (1).

DEFINITION 5. $Z(\in \mathscr{P}^{\#}(I_1))$ together with $n(\in I_1)$ satisfy *condition* (S) if for any decomposition of n into a sum of (not necessarily distinct) primes,

---

[4] Compare with Tarski's proof in [**4**, p. 138].

[5] This is half of [**4**, Theorem VIII].

[6] This is [**6**, p. 101, Theorem 3]; it will be extended in [**11**].

[7] $(\mathrm{iv})_a$ and $(\mathrm{iv})_b$ follow by the sufficiency of condition (M) (Theorem IX of [**4**]).

[8] This includes most of the cases of Theorem IX of [**4**], augmented by one of H. Rubin's cases (see [**9**, § 4]).

[9] See [**9**, § 4].

[10] $C(\{3, 7\}) \to C(9)$; $C(\{2, 7, 11\}) \to C(14)$; $C(\{2, 11, 13\}) \to C(16)$; $C(\{11, 12, 17, 19\}) \to C(24)$; $C(\{2, 3, 7, 13, 17, 19, 31, 37\}) \to C(42)$.

[11] Lemmas 13, 14, and 15 also yield the last implication of footnote 10.

$$n = p_1 + p_2 + \cdots + p_s ,$$

there is some $r \in I_1$ and some p_i, $i \in J_s$, such that $rp_i \in Z$.[12]

DEFINITION 6. $Z(\in \mathscr{P}^{\#}(I_1))$ together with $n(\in I_1)$ satisfy *condition* (SS) if for any decomposition of n into a sum of (not necessarily distinct) primes,

$$n = p_1 + p_2 + \cdots + p_s ,$$

there is some p_i, $i \in J_s$, which is in Z.[13]

Each of the conditions (M), (Z), (S), and (SS) induces a relation in $\mathscr{P}^{\#}(I_1) \times \mathscr{P}^{\#}I_1$ defined by $Z_1 R_X Z_2$ if and only if for each $n \in Z_2$, Z_1 and n satisfy condition (X) (X being M, Z, S, or SS). (Again, we omit the classifier in case Z_1 or Z_2 is a unit set.)

THEOREM 2. $R_{SS} \subset R_S \subset R_Z \subset R_M$.

Proof. We first note that any $Z \in (\mathscr{P}^{\#}(I_1))$ together with 1 satisfy all four conditions (SS), (S), (Z), and (M).

It follows from example (v), above, that in order to show that (M) is a stronger condition than (Z), we need only show that (M) is a consequence of (Z). Suppose $Z(\in \mathscr{P}^{\#}(I_1))$ and $n(\in I_2)$ satisfy (Z). Let

$$n = p_1 + p_2 + \cdots + p_m \tag{5}$$

be any decomposition of n into primes; we must find $r_1, r_2, \cdots, r_m \in I_0$ such that $r_1p_1 + r_2p_2 + \cdots + r_mp_m \in Z$.

If $n \in \Pi$, then n is a Z-number (Lemma 1) and consequently Z contains kn for some $k \in I_0$. Let $r_1 = r_2 = \cdots = r_m = k$ in (5); it follows that Z and n satisfy (M).

For composite n assume that for all $j < n$ and all $Z \in \mathscr{P}^{\#}(I_1)$, whenever Z and j satisfy (Z), they also satisfy (M). If n is a Z-number, then since n is composite, m must be $\geqq 2$ in (5), and by $(\mathrm{i})_{\mathrm{b}}$ of Definition 3, there exists s_1 and s_2 in I_0 such that

$$s_1p_1 + s_2(p_2 + \cdots + p_m) \in Z .$$

Let $r_1 = s_1$ and $r_2 = \cdots = r_m = s_2$. Finally, if Z and n properly satisfy (Z), then either Z and p_1 or else Z and $n' = p_2 + \cdots + p_m$ must satisfy (Z). In the former case $k'p_1 \in Z$ for some $k' \in I_1$, and we let $r_1 = k'$,

[12] This is [**4**, Definition 4]; it is the same as condition (S') of [**6**], and it is equivalent to condition (Σ) of [**1**]. Different proofs of the sufficiency of (S) for (1) are given in (1), Theorem 8, in (4), Theorem II, and (7), Theorem 2.

[13] cf. [**7**, Theorem 1].

$r_2 = \cdots = r_m = 0$. In the latter case by the inductive hypothesis, Z and n' satisfy (M). Now $p_2 + \cdots + p_m$ is already a prime decomposition of n'. Thus there are $t_2, \cdots, t_m \in I_0$ such that $t_2p_2 + \cdots + t_mp_m \in Z$; let $r_1 = 0, r_2 = t_2, \cdots, r_m = t_m$.

If Z and n satisfy (S), then whenever (5) holds, there is a $k'' \in I_0$ such that $k''p_i \in Z$ for some $i \in J_m$. In particular, if $n = lp$, $l \in I_1$, there is a prime decomposition of n consisting solely of p's. Thus for some $k''' \in I_0$, $k'''p \in Z$ and $(k'''p, n) > 1$. If n is prime, as above, n must be a Z-number. Otherwise, $n \geqq 4$; we assume that for all $j' < n$, whenever $Z(\in \mathscr{P}^{\sharp}(I_1))$ and j' satisfy (S), they also satisfy (Z). Assume Z and n satisfy (S), and let $n = n_1 + n_2$, $n_1, n_2 \in I_2$. Let $n_1 = p_1 + p_2 + \cdots + p_u$ and $n_2 = q_1 + q_2 + \cdots + q_v$ be any prime decompositions of n_1 and n_2; then $n = p_1 + p_2 + \cdots + p_u + q_1 + q_2 + \cdots + q_v$ is a prime decomposition of n. By (S), there is a $k^* \in I_1$ such that either k^*p_i, $i \in J_l$, or k^*q_j, $j \in J_m$, is in Z; hence either Z and n_1 or else Z and n_2 satisfy (S), and consequently (Z), by the inductive hypothesis. This proves that Z and n satisfy (Z).

[12], (1.15) and the examples following it guarantee the inclusion $R_{SS} \subset R_S$; the second example also serves to assure the proper inclusion $R_S \subset R_Z$.

We note the following additional properties of the relations R_X:

(i) If $Z_1R_XZ_2$ and if $Y_1(\in \mathscr{P}^{\sharp}(I_1))$ is any superset of Z, and Y_2 is any subset of Z_2, then $Y_1R_XY_2$, $X = M, Z, S$, or SS.

(ii) R_M and R_Z are reflexive; R_S and R_{SS} are not (by [9], (30)).

(iii) None of the R_X are symmetric; for $X = M, Z$, or S, R_X is also not anti-symmetric ($2R_X4$ and $4R_X2$).

(iv) For $k, n \in I_1$ and $Z \in \mathscr{P}^{\sharp}(I_1)$, $ZR_Xkn \to ZR_Xn$. For $X = M, S$ or SS, this is immediate. For $X = Z$, this will be shown in Lemma 4.

(v) Each of the R_X is transitive. For $X = S$ or SS this is immediate; for $X = M$ this is seen as follows: Suppose $Z_1R_MZ_2$ and Z_2R_MY. Then for any $n \in Y$ and any prime decomposition, $n = p_1 + p_2 + \cdots + p_s$, there are $k_1, k_2, \cdots, k_s \in I_0$ such that $k_1p_1 + k_2p_2 + \cdots + k_sp_s = z_0 \in Z_2$. Since Z_1 and z_0 satisfy (M) and since

$$\underbrace{p_1 + \cdots + p_1}_{k_1} + \underbrace{p_2 + \cdots + p_2}_{k_2} + \cdots + \underbrace{p_s + \cdots + p_s}_{k_s}$$

is a prime decomposition of z_0, there are $l_1, l_2, \cdots, l_{k_1+k_2+\cdots+k_s} \in I_0$ such that

$$\begin{aligned}
&l_1p_1 + l_2p_1 + \cdots + l_{k_1}p_1 + l_{k_1+1}p_2 + l_{k_1+2}p_2 + \cdots + l_{k_1+k_2}p_2 \\
&\quad + \cdots + l_{k_1+k_2+\cdots+k_{s-1}+1}p_s + l_{k_1+k_2+\cdots+k_{s-1}+2}p_s + \cdots + l_{k_1+k_2+\cdots+k_s}p_s \\
&= (l_1 + l_2 + \cdots + l_{k_1})p_1 + (l_{k_1+1} + l_{k_1+2} + \cdots + l_{k_1+k_2})p_2 + \cdots \\
&\quad + (l_{k_1+k_2+\cdots+k_{s-1}+1} + l_{k_1+k_2+\cdots+k_{s-1}+2} + \cdots + l_{k_1+k_2+\cdots+k_s})p_s \in Z_1 \,.
\end{aligned}$$

Thus Z_1 and n satisfy (M), and, consequently, $Z_1 R_M Y$. The transitivity of R_Z will follow from Theorem 3.

LEMMA 3. *If Z and n satisfy (Z) and if p is a prime factor of n, then Z contains a multiple of p.*

Proof. Assume that the hypothesis of the lemma holds.

First, suppose that n is a Z-number. If Z contains a multiple of n, it contains a multiple of p. Otherwise, n is composite, by $(\mathrm{i})_a$ of Definition 3, and by $(\mathrm{i})_b$, there are $s_1, s_2 \in I_0$, at least one of which is in I_1, such that $s_1 p + s_2(lp) \in Z$ for some $l \in I_1$. Thus $kp \in Z$ for $k = s_1 + s_2 l$.

Suppose that for all $m < n$ and for all $Z \in \mathscr{P}^*(I_1)$, whenever Z and m satisfy (Z) and q is a prime factor of m, then Z contains a multiple of q.

Let Z and n properly satisfy (Z); by Lemma 1, n is composite. Again, $n = p + lp$ for some $l \in I_1$, and by $(\mathrm{ii})_b$ of Definition 4, Z together with either p or lp satisfy (Z). The result follows from the inductive hypothesis.

COROLLARY. *If $YR_Z Z$ and $ZR_Z n$, then Y contains a multiple of each prime factor of n.*

Proof. Under this hypothesis, if p is a prime factor of n, then, by Lemma 3, $kp \in Z$ for some $k \in I_1$. Since p is a prime factor of an element of Z, again $k'p \in Y$ for some $k' \in I_1$.

LEMMA 4. $(\forall k, n \in I_1)(\forall Z \in \mathscr{P}^*(I_1))(ZR_Z kn \rightarrow ZR_Z n)$. *Moreover, if kn is a Z-number, so is n.*

Proof. This is trivial for $n = 1$ and k, Z arbitrary, and, also, for $k = 1$ and n, Z arbitrary. Let $n > 1$ and $k > 1$ and assume that for all $k' < k$ and all $Z \in \mathscr{P}^*(I_1)$ that $ZR_Z k'n \rightarrow ZR_Z n$. Now, if kn is a Z-number, then for $l_1, l_2 \in I_0$, $l_1 n + l_2(k-1)n \in Z$. Hence

$$(n, l_1 n + l_2(k-1)n) = n > 1 ,$$

and if $n = n_1 + n_2$, $n_1, n_2 \in I_2$, then

$$(l_1 + l_2(k-1))n_1 + (l_1 + l_2(k-1))n_2 = l_1 n + l_2(k-1)n \in Z .$$

It follows that n is a Z-number. If Z and kn properly satisfy (Z), then either $ZR_Z n$ or $ZR_Z(k-1)n$; by the inductive hypothesis, we are finished.

THEOREM 3. $(\forall n \in I_1)(\forall Y, Z \in \mathscr{P}^*(I_1))((YR_Z Z \,\&\, ZR_Z n) \rightarrow YR_Z n)$.

Proof. For $n \in I_1$ and $Y, Z \in \mathscr{P}^{\sharp}(I_1)$ assume that

$$YR_Z Z \,\&\, ZR_Z n \; . \tag{6}$$

For $n = 1$, by (ii) of Definition 3, we have $YR_Z 1$. For $n \in \Pi$, by the corollary to Lemma 3, Y contains a multiple of n; hence n is a Y-number.

For composite n, assume that for all $k < n$ and all $Z \in \mathscr{P}^{\sharp}(I_1)$, $(YR_Z Z \,\&\, ZR_Z k) \rightarrow YR_Z k$. (6) together with the corollary to Lemma 3, yield the existence of a $y \in Y$ such that $(n, y) > 1$. Suppose that

$$n = n_1 + n_2, n_1, n_2 \in I_2 \; . \tag{7}$$

Case 1. n is a Z-number.

There are $s_1, s_2 \in I_0$ for which $s_1 n_1 + s_2 n_2 \in Z$. If either s_1 or $s_2 = 0$, then $s_i n_i \in Z$ for $i = 1$ or 2; hence n_i is a Z-number and, by the inductive hypothesis, $YR_Z n_i$. It follows that $YR_Z n$. If neither s_1 nor $s_2 = 0$, then either

$$t_1 s_1 n_1 + t_2 s_2 n_2 \in Y \qquad \text{for } t_1, t_2 \in I_0 \; , \tag{8}$$

or else

$$\text{either } Y \text{ and } s_1 n_1 \text{ or } Y \text{ and } s_2 n_2 \text{ satisfy } (Z) \; . \tag{9}$$

In case (9) holds, Lemma 4 assures that Y and n_1 or Y and n_2 satisfy (Z); in either instance, (8) or (9), $YR_Z n$.

Case 2. Z and n properly satisfy (Z):

Then, by (7) and $(\mathrm{ii})_b$ of Definition 4, $ZR_Z n_1$ or $ZR_z n_2$; by the inductive hypothesis, $YR_Z n_1$ or $YR_2 n_2$. Therefore $YR_Z n$.

We remark that if n is a Z-number and if each $z \in Z$ is a Y-number, it does not follow that n is a Y-number. A counter-example is afforded by the case in which $n = 8$, $Z = \{3, 4\}$, and $Y = \{2, 3\}$.

References

1. M. N. Bleicher, *Multiple choice axioms and axioms of choice for finite sets*, Fund. Math. **57** (1965), 247-252.

2. K. Gödel, *The consistency of the axiom of choice and of the generalized continuum-hypothesis with the axioms of set theory*, 6th ed., Annals of Math. Studies **3**, Princeton Univ. Press, Princeton, 1964.

3. A. Mostowski, *Über die Unabhängigkeit des Wohlordnungssatzes vom Ordnungsprincip*, Fund. Math. **32** (1939), 201-252.

4. ———, *Axiom of choice for finite sets*, Fund. Math. **33** (1945), 137-168.

5. W. Sierpinski, *L'axiome du choix pour les ensembles finis*, **10** (1955), 92-99.

6. ———, *Cardinal and ordinal numbers*, 1st, ed., Monografe Matematyczne **34**, Pańtswome Wydawnictwo Naukowe, Warszawa, 1958.

7. W. Szmielew, *On choices from finite sets*, Fund. Math. **34** (1947), 75-80.
8. P. L. Tchebychef, *Oeuvres*, tome 1, Publiees par les soins de A. Markoff and N. Sonin, Chelsea Publ. Co., New York, 1962.
9. M. Zuckerman, *Bertrand's Postulate and conditions (M) and (S) for the axiom of choice for finite sets* (to appear in Illinois J. Math.).
10. ———, *Some theorems on the axiom of choice for finite sets* (to appear in Z. Math. Logik Grundlagen Math.).

Received September 8, 1967. The preparation of this paper was supported in part by the U.S. Air Force and in part by a National Science Foundation Science Faculty Fellowship. This research formed part of the author's Ph. D. thesis (Yeshiva University, 1967) under the supervision of Professor Martin Davis of New York University.

11. ———, *On a theorem of Sierpenski* (to appear).
12. ———, *Finite versions of the axiom of choice*, Ph. D. Thesis, Dept. of Math., Yeshiva University, New York (1967).

NEW YORK UNIVERSITY
THE CITY COLLEGE OF THE CITY UNIVERSITY OF NEW YORK