NUMBER THEORETIC RESULTS RELATED TO THE AXIOMS OF CHOICE FOR FINITE SETS

BY

Martin M. Zuckerman[1]

1. Introduction

Definition 1. For each positive integer n, let $C(n)$ be the following statement of set theory: "For every nonempty set X whose elements are n-element sets, there is a function f with domain X such that $f(x) \in x$ for each $x \in X$."

The axioms $C(n)$ ($[n]$ in the original notation) were introduced by Mostowski in [8]; we shall refer to these as the *axioms of choice for finite sets*. Mostowski investigates implications of the form

$$(1) \qquad (C(m_1) \ \& \ C(m_2) \ \& \ \cdots \ \& \ C(m_k)) \rightarrow C(n)$$

which are valid in set theory (without the axiom of choice). He finds an upper bound on n in terms of the maximum of the set $\{m_1, m_2, \cdots, m_k\}$ under the assumption that (1) is provable in set theory (ibid., Theorem V); he obtains this result by utilizing *Bertrand's postulate* [12, pp. 51–64]:

(2) For $x > 7/2$ there is a prime p satisfying $x < p < 2x - 2$.

By considering (2) as well as a modified version of this classical number theoretic result in connection with Mostowski's necessary condition (M) for (1) we strengthen some of Mostowski's conclusions. We also utilize Bertrand's postulate to prove a theorem concerning the sufficiency condition (S) for (1) (due to Szmielew and Mostowski) as well as to obtain an independence result for a specific case of this implication.

2. Preliminaries

The system of set theory within which we shall work will be the one introduced by Mostowski in [7]; this is a system of the Gödel-Bernays type which does not include the axiom of choice among its axioms and which permits the existence of urelements (objects, other than the empty set, which are in the domain but not the range of the ϵ-relation). Throughout the metamathematical part of this paper we shall assume that this system of set theory is consistent; this is equivalent to the assumption that Gödel's system

Received August 31, 1967.

[1] 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. The work was supported in part by the U. S. Air Force.

The author wishes to thank the referee for various suggestions and in particular, for shortening the proofs of Theorems 4 and 5.

A, B, C (of [3]) is consistent. (See the discussion in [6, pp. 478–479].) The first-order predicate calculus with identity will serve as the logical framework for set theory.

Let 0 be the empty set, let $1 = \{0\}$, let $2 = 1 \cup \{1\}$, let $3 = 2 \cup \{2\}$, etc. For any such (nonnegative) integer n and any set X, we say that X *is an n-element set* if there is a 1-1 mapping of X onto n.

For sets X and Y, we shall use $X \backslash Y$ to denote the relative complement of Y in X; we note that in case X and Y are both integers with $0 < Y < X$ (i.e., $0 \in Y \in X$), then $X \backslash Y \neq X - Y$ (here, "$-$" is the usual arithmetic operation). Furthermore, we let $\mathcal{P}^{\#}(X)$ designate the set of finite[2] subsets of X and $\mathcal{P}^{*}(X) = \mathcal{P}^{\#}(X)\backslash\{0\}$.

For $n = 1, 2, \cdots$, let I_n denote the set of all integers $\geq n$, and let $J_n = \{1, 2, \cdots, n\}$. Let Π represent the set of prime numbers. The letters $i, j, k, l, m, n, p, q, r, s, t, z, N$ will always refer to integers.

For $Z \in \mathcal{P}^{*}(I_1)$ we let $C(Z)$ denote the conjunction of the statements $C(z)$ for $z \in Z$; since positive integers are not subsets of I_1, no confusion will ensue if we write $C(z)$ in lieu of $C(\{z\})$ for $z \in I_1$. (We shall also omit the braces in various conditions to be defined.)

We shall write an implication such as "$C(Z) \rightarrow C(n)$" when we intend the metamathematical statement " '$C(Z) \rightarrow C(n)$' is a theorem of set theory."

3. The function $\mathfrak{y}(n)$

We begin by introducing several notions.

DEFINITION 2. Let $s \geq 1$ and let $m_1, m_2, \cdots, m_s$ be distinct integers ≥ 2. For $j \in 2$ define Lin Comb$^j(m_1, m_2, \cdots, m_s)$ to be the set of all integers ≥ 2 of the form $z_1m_1 + z_2m_2 + \cdots + z_sm_s$ where each $z_i \geq j$ for $i \leq s$.

We shall write Lin Comb$^j(M)$, $j \in 2$, for Lin Comb$^j(m_1, m_2, \cdots, m_s)$ when $M = \{m_1, m_2, \cdots, m_s\} \in \mathcal{P}^{*}(I_1)$. Clearly, for each $M \in \mathcal{P}^{*}(I_1)$, Lin Comb$^1(M) \subseteq$ Lin Comb$^0(M)$, and if $\mathbf{n}(M) > 1$, this inclusion is proper.

DEFINITION 3. For $n \geq 1$ and $P \in \mathcal{P}^{*}(\Pi)$, we say that P is a *prime decomposition of n* if $n \in$ Lin Comb$^1(P)$; we let $\pi(n)$ be the set of prime decompositions of n.

Clearly $\pi(n)$ is finite for each $n \geq 1$; $\pi(n) = 0$ iff $n = 1$. Moreover,

$$\pi(n) \subseteq \pi(kn) \qquad \text{for all } k, n \geq 1. \tag{3}$$

DEFINITION 4. $Z(\in \mathcal{P}^{\#}(I_1))$ and $n(\in I_1)$ satisfy *condition* (M) if for every $P \in \pi(n)$, $Z \cap$ Lin Comb$^0(P) \neq 0$.

Using group theoretic as well as set theoretic techniques, Mostowski shows

[2] 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. For the relationship between various definitions of "finiteness" in set theory without the axiom of choice, see [5].

condition (M) to be necessary for any implication of the form $C(Z) \rightarrow C(n)$ [8, Theorem IV].

Definition 5. Let $\mu(1) = 1$; for $n \geq 2$, let

$$\mu(n) = \max \{\min P: P \in \pi(n)\}.$$

Thus for $n \geq 2$, $\mu(n)$ is the greatest prime p such that n is expressible as the sum of primes not less than p.

The second formulation of this definition (with dom $\mu = I_2$) is due to Mostowski; he introduces it because various cases of the implication $C(Z) \rightarrow C(n)$ can be expressed in terms of $\mu(n)$. In particular, he shows ([8], p. 163, (1)) that

$$(4) \qquad (C(J_m) \rightarrow C(n)) \leftrightarrow (m \geq \mu(n)), \qquad m, n \in I_2 .$$

We note that

(5) if $C(Z) \rightarrow C(n)$ and if $m = \max (Z)$, then $C(J_m) \rightarrow C(n)$ and $m \geq \mu(n)$.

Mostowski mentions the following additional properties of the function $\mu(n)$ (ibid., (2), (3), (4); we modify these to suit our definition at $n = 1$).

$$(6) \qquad \sqrt{(n/2)}/2 < \mu(n) \leq n, \qquad n \geq 1.$$

(7) Let $n \geq 2$; then $\mu(n) \in \Pi$, and $\mu(n) = n$ iff $n \in \Pi$.

(8) If $n \neq 1, 2$, or 4, then $\mu(n) > 2$.

The aim of this section is to obtain further estimates of $\mu(n)$.

Lemma 1. *For $n_1, n_2 \geq 1$, $\mu(n_1 + n_2) \geq min \{\mu(n_1), \mu(n_2)\}$.*

Theorem 1. *If $m(\geq 2)$ is such that $\mu(k) > p$ for $m \leq k < 2m$,* then *$\mu(n) > p$ for all $n \geq m$.*

Proof. Suppose $\mu(k) > p$ for $m \leq k < 2m$ and let $n \geq 2m$. Then $n = (m + t) + sm$, where $s \geq 1$ and $0 \leq t < m$. Using (3) and Lemma 1, we conclude that $\mu(n) > p$.

We observe that Theorem 1 yields an alternative proof that $\mu(n) = 2$ only if $n = 2$ or 4 (because $\mu(n) > 2$ for $5 \leq n < 10$).

Theorem 2. (a) *If n is composite, then $2 \leq \mu(n) \leq n/2$.*

(b) *For $n \geq 2$, $2 < \mu(n) < n/2$ iff n is neither a prime nor twice a prime; if n is twice a prime, then $\mu(n) = n/2$.*

(c) *If n is odd and composite, then $3 \leq \mu(n) \leq n/3$.*

In addition,

(i) *if n is not thrice a prime, then $3 < \mu(n) < n/3$;*

(ii) *if n is thrice a prime, then $\mu(n) = n/3$.*

Proof. (a) If n is composite, $p \epsilon P \epsilon \pi(n)$, and $p > n/2$, then there must be some $q \epsilon P$ such that $q < n/2$.

(b) follows from (7), (8), part (a), and the observation that $\{n/2\} \epsilon \pi(n)$ iff $n/2$ is prime.

(c) follows from similar considerations. Here we note that if n is an odd composite, then there must be a prime decomposition consisting solely of at least three (not necessarily distinct) odd primes, at least one of which is less than or equal to $n/3$. Moreover, by theorem 1, $\mu(n) > 3$ if $n > 9$; hence if n is odd but is neither a prime nor twice a prime, then $\mu(n) > 3$.

Theorem V of [8] together with (5), above, assert that $n < 8\mu(n)^2$. This result depends upon the form (2), above, of Bertrand's postulate. In order to reduce this upper bound on n we note that the prime number theorem [4, pp. 229–263] has the following consequence.

LEMMA 2. *For every $\rho > 1$, there is an $N(\rho)$ such that for $x \geq N(\rho)$, there is always a prime between x and ρx.*

Much of the explicit computation of $N(\rho)$ has been carried out in [9].

LEMMA 3. *For every $\rho > 1$, $n < \rho\mu(n)^2$ with finitely many exceptions.*

Proof. Given $\rho > 1$, let $\sigma = \sqrt[3]{\rho}$, and let $N(\sigma)$ be as in Lemma 2. By (6), for n sufficiently large, $n \geq \mu(n) \geq N(\sigma)$. Suppose that for any such n, $n \geq \rho\mu(n)^2$.

We apply Mostowski's method of Theorem V of [8], but with the stronger version of Bertrand's postulate given in Lemma 2, above.

There are primes p and q such that

$$\mu(n) < p < \sigma\mu(n) < q < \sigma^2\mu(n) \tag{9}$$

and there are integers s and t such that $ps + qt = 1$. Let $k = sn$ and let $l = tn$. Then $pk + ql = n$.

k and l cannot both be negative. Suppose, for example, that $k > 0$ and $l < 0$. Let z be the least positive integer such that $l + zp \geq 0$. Then $0 \leq l + zp < p$. If $k - zq \leq 0$, then

$$n = p(k - zq) + q(l + zp) \leq q(l + zp) < pq < \rho\mu(n)^2,$$

contradicting the hypothesis. Hence $k - zq > 0$, and nonnegative integers k' $(= k - zq)$ and l' $(= l + zp)$ exist which satisfy $pk' + ql' = n$. Thus $\mu(n) \geq p$; this contradicts (9).

THEOREM 3. *For all $n \geq 1$, $n < 1.178\ \mu(n)^2$.*

Proof. $N(1.056) = 212$ in Lemma 2 (for details, see [13, pp. 33–38]); by Lemma 3, $n < 1.178\ \mu(n)^2$ for $\mu(n) \geq 212$. Now $\mu(n) > 211$

for $672 \leq n < 1344$; by Theorem 1, $\mu(n) > 211$ for all $n \geq 672$. For $n < 672$ the inequality indicated in the statement of the theorem can readily be calculated. (See Table 1 of [13].)

COROLLARY. *For all* $n \geq 1$, $\mu(n) > .93\sqrt{n}$.

Other properties of $\mu(n)$ and of a related prime-valued function are given in [13].

4. Condition (S)

DEFINITION 6. $Z(\epsilon\, \mathcal{P}^{\#}(I_1))$ and $n(\geq 1)$ satisfy *condition* (S) if for every $P \epsilon\, \pi(n)$ there is some $p \epsilon P$ and $r \geq 1$ such that $rp \epsilon Z$.

Condition (S) is sufficient for the implication $C(Z) \rightarrow C(n)$.[3] Clearly, for any $Z \epsilon\, \mathcal{P}^{*}(I_1)$ and $n \geq 1$, if Z and n satisfy (S), then they satisfy (M). Moreover, the direction of this implication cannot be reversed; take $n = 5$, $P = \{2, 3\}$, and $Z = \{5\}$. This, of course shows that condition (S) is not necessary for the implication $C(Z) \rightarrow C(n)$; (S) is "almost totally unnecessary" in a sense which will be explained in the corollary of Theorem 4, below.

LEMMA 4. *Let m and n be relatively prime integers* ≥ 2. *Then* $I_{mn+1} \subset$ Lin Comb^1 (m, n) (*equivalently*, $I_{(m-1)(n-1)} \subseteq$ Lin Comb^0 (m, n)).

(This is a well-known result which is mentioned in [2].)

LEMMA 5. *For all $n, k \geq 1$, $C(nk) \rightarrow C(k)$.*

(A proof of this lemma is given in [10, p. 99, Theorem 2].)

Henceforth, we let $\mathbf{P}(n)$ be the set of prime factors of n.

THEOREM 4. *For every $n = 5$ or $n \geq 7$ there are distinct primes p, q which are not factors of n for which $\{p, q\} \epsilon\, \pi(n)$.*

Proof. Let $n \geq 5$, let

$$q_1 = \min(\Pi \backslash \mathbf{P}(n)) \quad \text{and} \quad q_2 = \min(\Pi \backslash (\mathbf{P}(n) \cup \{q_1\})).$$

Then, in fact, if $n \epsilon I_5 \backslash \{6, 18, 30\}$, we have $\{q_1, q_2\} \epsilon\, \pi(n)$. For $n > q_1 q_2$, this follows from Lemma 4; otherwise, $n \leq q_1 q_2 \leq 77$ and there are only finitely many cases to check. Finally, $\{7, 11\} \epsilon\, \pi(18)$ and $\{11, 19\} \epsilon\, \pi(30)$.

COROLLARY. *For every $n = 5$ or $n \geq 7$, condition* (S) *fails for* $C(n) \rightarrow C(n)$.

Remark. By Lemma 5, this implies that condition (S) fails also for implications $C(m) \rightarrow C(n)$, where $n = 5$ of $n \geq 7$, and where m is any multiple of n.

[3] Different proofs of the sufficiency of (S) are given in [1, Theorem 8], in [8, Theorem II], in [11, Theorem 2], and in [16, Theorems 1 and 2].

5. An independence theorem

From Lemma 5 it follows that for all $n \geq 2$, $C(n) \to C(\mathbf{P}(n))$. Moreover, $C(\mathbf{P}(4)) \to C(4)$ (see [8, p. 138]) and $C(\mathbf{P}(6)) \to C(6)$ (ibid., Theorem VI). In contrast, we have the following.

THEOREM 5. *If n is a composite greater than* 6, *then $C(n)$ is independent of $C(\mathbf{P}(n))$.*

Proof. Let $n(> 6)$ be composite and let p be the greatest prime divisor of n. In the first two cases we show that condition (M) fails for $\mathbf{P}(n)$ and n.

Case 1. n is odd. By (2), there is a prime q satisfying $p < q < 2p$; hence $q - 1 < n$. Thus $n \in \text{Lin Comb}^0(2, q)$, by Lemma 4, whereas $\mathbf{P}(n) \cap \text{Lin Comb}^0(2, q) = 0$.

Case 2. n is even and square-free. Then $n = 2kp$ and $p \geq 5$. Let q_1 be a prime such that $p < q_1 < 2p - 2$. It follows that $n - q_1 > 1$; let q_2 be a prime divisor of $n - q_1$. q_2 cannot divide n because then q_2 would also divide q_1—hence would equal q_1. But as a prime divisor of n, q_2 would be $\leq p < q_1$. Thus $\mathbf{P}(n) \cap \text{Lin Comb}^0(q_1, q_2) = 0$, whereas obviously $n \in \text{Lin Comb}^0(q_1, q_2)$.

Case 3. $n = 8$ or 12. $\mathbf{P}(8) = J_2$, $\mu(8) = 3$; $\mathbf{P}(12) = J_3$, $\mu(12) = 5$. The result follows from (4).

By Lemma 5, these are the only cases which need be considered.

Applications of this theorem are made in [14] and in [16].

BIBLIOGRAPHY

1. M. N. BLEICHER, *Multiple choice axioms and axioms of choice for finite sets*, Fund. Math., vol. 57 (1965), pp. 247-252.
2. A. BRAUER, *On a problem of partitions*, Amer. J. Math., vol. 64 (1942), pp. 299-312.
3. 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 Mathematics Studies, no. 3, Princeton, Princeton, 1964.
4. W. J. LEVEQUE, *Topics in number theory*, vol. 2, Addison-Wesley, Reading, Massachusetts, 1956.
5. A. LÉVY, *The independence of various definitions of finiteness*, Fund. Math., vol. 46 (1958), pp. 1-13.
6. ———, *Axioms of multiple choice*, Fund. Math., vol. 50 (1962) pp. 475-483.
7. A. MOSTOWSKI, *Über die Unabhängigkeit des Wohlordnungssatzes vom Ordnungsprinzip*, Fund. Math., vol. 32 (1939), pp. 201-252.
8. ———, *Axiom of choice for finite sets*, Fund. Math., vol. 33 (1945), pp. 137-168.
9. J. B. ROSSER AND L. SCHOENFELD, *Approximate formulas for some functions on prime numbers*, Illinois J. Math., vol. 6 (1962), pp. 64-94.
10. W. SIERPINSKI, *Cardinal and ordinal numbers*, 1st ed., Monografie Matematyczne, 34, Państwowe Wydawnictwo Naukowe, Warszawa, 1958.
11. W. SZMIELEW, *On choices from finite sets*, Fund. Math., vol. 34 (1947), pp. 75-80.
12. P. L. TCHEBYCHEF, *Oeuvres*, tome 1, Publiées par les soins de A. Markoff et N. Sonin, Chelsea Publ. Co., New York, 1962.
13. M. M. ZUCKERMAN, *Finite versions of the axiom of choice*, Ph.D. Thesis, Dept. of Math., Yeshiva University, New York, 1967.

14. ———, *Some theorems on the axiom of choice for finite sets*, Z. Math. Logik Grundlagen Math., to appear.

15. ———, *Multiple choice axioms*, (Axiomatic Set Theory) Proc. Sympos. Pure Math., vol. 13 (1969).

16. ———, *A unifying condition for implications among the axioms of choice for finite sets*, Pacific J. Math., vol. 28, (1969), pp. 233–242.

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