On the axiom of choice for families of finite sets

by

K. Wiśniewski (Warszawa)

The investigation of the axiom of choice for families of finite sets was initiated by Mostowski [4]. Further mathematical investigations of this topic are due to Szmielew [6] and Sierpiński [5], and metamathematical ones — to Zuckerman [8] and Gauntt [1]. In the present paper we prove that some forms of the axiom of choice for families of finite sets are independent of others forms. This paper is a continuation of [7].
The writer thanks Professor Mostowski for his kind help in the preparation of this paper and Professor Ryll-Nardzewski for his valuable suggestions and criticism.

In this paper we consider the set theory ZF′, which differs from ZF by containing the constant Ø for the empty set, and the axiom stating the existence of an infinite set of individuals. The axiom of extensionality in ZF′ is restricted only to sets (1).

We consider the following propositions:

$[n]$: *For every family of n-element sets there exists a choice function*;

$[n]^0$: *For every linearly ordered family of n-element sets there exists a choice function*;

$[n]^\omega$: *For every denumerable family of n-element sets there exists a choice function.*

Let G be a group and $\mathfrak{A}$ — a family of proper subgroups of G. Consider the set $S_i = \{(xH, i)\colon H \in \mathfrak{A} \ \&\ x \in G\}$ $(i \in \omega)$. The group Γ_i of permutations $\pi_y^{(i)}$ of the set S_i which are defined by the formula

$$\pi_y^{(i)} = \begin{pmatrix} (xH, i) \\ ((yx)H, i) \end{pmatrix}_{H \in \mathfrak{A}}$$

(1) The restriction to ZF′ set theory is inessential. We may use the Fraenkel–Mostowski method for the other set theories, e.g. the set theory of the Gödel–Bernays type with classes and individuals or set theories in which unfounded sets are allowed (cf. [2]). The results of the present paper are valid for the "ordinary" set theory i.e. the set theory with no individuals and with the axiom of regularity. This can be shown by the Cohen method modified by Marek [3].

is a representation of G. The sets $T_H^{(i)} = \{(xH, i): x \in G\}$ are the orbits of the group G. The length of $T_H^{(i)}$ is $[G:H]$ for $H \in \mathfrak{A}$. Γ_i is a faithful representation of G; there exists a subgroup $H \in \mathfrak{A}$ containing no non-trivial normal subgroup of G.

Let $S = S^{(0)} = \bigcup_{i \in \omega} S_i$. Let Γ^ω be a weak product of groups Γ_i. We assign to every element π of the group Γ^ω a permutation of the set S defined by the formula $\pi(a) = \pi^{(i)}(a)$ for $a \in S_i$. In the sequel we consider the group Γ^ω as the group of permutations of the set S which are defined above.

Now we shall define for ordinal numbers $\xi > 0$ the sets $S^{(\xi)}$ and extend the permutation $\pi \in \Gamma^\omega$ to those sets. Suppose that for $\eta < \xi$ we have defined the set $S^{(\eta)}$ and that $\pi(x)$ is defined for $x \in \bigcup_{\eta<\xi} S^{(\eta)}$. For $x \in P(\bigcup_{\eta<\xi} S^{(\eta)}) - \bigcup_{\eta<\xi} S^{(\eta)}$ we put $\varphi(x) = \{\varphi(y): y \in x\}$. We define the set $S^{(\xi)}$ as the subset of the set $P(\bigcup_{\eta<\xi} S^{(\eta)}) \cup \bigcup_{\eta<\xi} S^{(\eta)}$ consisting of those elements x for which there exists a $q \in \omega$ such that for arbitrary $\pi \in \Gamma^\omega$ the equalities $\pi^{(0)} = \ldots = \pi^{(q)} = 1$ imply $\pi(x) = x$. Let $M = M(G, \mathfrak{A})$ be the class consisting of those elements x for which there exists an ordinal number ξ such that $x \in S^{(\xi)}$. The class M is a model of ZF'.

THEOREM 1. *Let P be an additive semigroup of positive integers generated by a set Z of prime numbers. Then there exists a model M of ZF' in which every proposition $[n]$ for $n \notin P$ is true and every proposition $[n]^\omega$ for $n \in P$ is false.*

Proof. Let $G = \prod_{r \in Z} C_r$ (C_r being the cyclic group of order r); let $\mathfrak{A}$ be the set of all proper subgroups of the group G and $M = M(G, \mathfrak{A})$. If $n \in P$ then $n = \sum_{i=1}^{s} p_i k_i$, where $p_i \in Z$ and k_i are positive integers. Let $H_1, \ldots, H_s$ be subgroups of G such that $[G:H_i] = p_i$. Then in the model M there exists no choice function for the set

$$\{\bigcup_{i=1}^{s} (T_{H_i}^{(j)} \times \underline{k}_i): j \in \omega\},$$

where $\underline{k}_i$ denotes the k_ith number of von Neumann. Thus $[n]^\omega$ is false in M.

Suppose that $n \notin P$. Let $x \in S^{(\xi)}$ be a family of disjoint n-element sets. Then there exists an integer q such that $\pi(x) = x$ provided $\pi \in \Gamma^\omega$ and $\pi^{(0)} = \ldots = \pi^{(q)} = 1$. Let $\Delta = \{\pi \in \Gamma^\omega: \pi^{(0)} = \ldots = \pi^{(q)} = 1\}$. If $u, v \in x$ then $u \sim v \equiv (E\pi)_\Delta \pi(u) = v$. From every equivalence class of the relation $\sim$ we choose exactly one element e_A.

Let $\theta_A = \{\pi \in \Delta: \pi(e_A) = e_A\}$. If for every $z \in e_A$ there existed a permutation $\pi \in \theta_A$ such that $\pi(z) \neq z$, then the group θ_A would have a representation which is a group of permutations of the set e_A with no fixed point, and thus of degree n, which is impossible. Thus there exists an element $f_A \in e_A$ such that $\pi(f_A) = f_A$ for every permutation $\pi \in \theta_A$. The set

$$w = \bigcup \{\{\pi(f_A): \pi \in \Delta\}: A \text{ is an equivalence class of relation } \sim\}$$

is a selector for the set x and belongs to M [2].

THEOREM 2. *Let G be a finite group, $Q(G)$—the additive semigroup of positive integers generated by indices of proper subgroups of the group G, and $R(G)$—the additive semigroup of positive integers generated by orders of non-trivial (i.e. $\neq 1$) elements of the group G. Then there exists a model M of ZF' in which propositions $[n]^0$ for $n \notin Q(G)$ are true and propositions $[n]$ for $n \notin R(G)$ and $[n]^\omega$ for $n \in Q(G)$ are false.*

LEMMA 1. *Let $G_1, \ldots, G_r$ be finite groups and $K_1, \ldots, K_r$—sets of positive integers such that index of each proper subgroup of the group G_i is divisible at least by one of the numbers of the set K_i. Then the index of each proper subgroup of the group $\prod_{i=1}^{r} G_i$ is divisible at least by one of the numbers of the set $\bigcup_{i=1}^{r} K_i$* [3].

The proof of lemma is inductive (with respect to r) and the following simple fact is used:

If G_1 and G_2 are finite groups and H—a subgroup of $G_1 \times G_2$, then

$$[G_1 \times G_2 : H] = [G_1 : G_1'] \cdot [G_2 : G_2'] \cdot [G_1' : H_1] = [G_1 : G_1'] \cdot [G_2 : G_2'] \cdot [G_2' : H_2],$$

where

$$G_1' = \{x \in G_1: (Ey)(x, y) \in H\}, \quad G_2' = \{y \in G_2: (Ex)(x, y) \in H\},$$
$$H_1 = \{x \in G_1: (x, 1) \in H\}, \quad H_2 = \{y \in G_2: (1, y) \in H\}.$$

Proof of theorem 2. Let $M = M(G, \mathfrak{A})$, where $\mathfrak{A}$ is the set of all proper subgroups of the group G.

Let $n \notin Q(G)$ and $x \in S^{(\xi)}$ be a family of n-element sets which is linearly ordered by $\prec \in M$. Thus there exists a positive integer q such that $\pi(x) = x$ and $\pi(\prec) = \prec$ provided $\pi^{(0)} = \ldots = \pi^{(q)} = 1$ and $\pi \in \Gamma^\omega$. Let $\Delta = \{\pi \in \Gamma^\omega: \pi^{(0)} = \ldots = \pi^{(q)} = 1\}$. If $u \in x$ then $\pi(u) = u$ for $\pi \in \Delta$. Suppose that there exists a $\pi \in \Delta$ such that $\pi(u) \neq u$. Let θ be the cyclic group generated by π. The finiteness of G implies that θ is finite. Thus the set $v = \{\varphi(u): \varphi \in \theta\}$ is finite and has at least 2 elements. This implies that $u \prec \pi(u) \prec \ldots \prec u$ or $u \succ \pi(u) \succ \ldots \succ u$; therefore $\prec$ is not an ordering relation.

---

[2] The proof given above is a slight modification of the proof in Mostowski's paper [4].

[3] This lemma and its proof have been given by Prof. Mostowski.

Let u be an arbitrary element of the family x. For every $z \in u$ q_z is the least positive integer such that $\pi \in \Gamma^\omega$ and $\pi^{(0)} = \ldots = \pi^{(q_z)} = 1$ imply $\pi(z) = z$. Put $q(u) = \max\{q_z\colon z \in u\}$. If $q(u) \leqslant q$ then for every $z \in u$ and $\pi \in \Delta$ we have $\pi(z) = z$. If $q(u) > q$ then for every $z \in u$ and $\varphi \in \Delta$ we have $\varphi(z) = \varphi_{q,q(u)}(z)$, where $\varphi^{(i)}_{q,q(u)} = \varphi^{(i)}$ for $i < q(u)$ and $\varphi^{(q(u)+i)}_{q,q(u)} = 1$. Let $\Xi = \{\pi \in \Delta\colon (i)\,\pi^{(q(u)+i)} = 1\}$. If for every $z \in u$ there existed a permutation $\pi \in \Delta$ such that $\pi(z) \neq z$, then the group Ξ would have a representation of degree n. Since Ξ is isomorphic with the product of q copies of G and $n \notin Q(G)$, we obtain a contradiction. Thus, for every $u \in x$ there exists an $e_u \in u$ such that $\pi(e_u) = e_u$ for $\pi \in \Delta$. The set $\{(u, e_u)\colon u \in x\}$ is a choice function for the family belonging to M; therefore $[n]^0$ is true in M.

Now let $n \in R(G)$, i.e., $n = \sum_{i=1}^{s} r_i k_i$, where r_i are the orders of non-trivial elements of the group and k_i are positive integers. Without loss of generality we may assume that r_i are prime numbers. Let $H \in \mathfrak{A}$ contain no non-trivial normal subgroup of the group G. Consider the set

$$a = \bigcup_{i \in \omega} \{ \bigcup_{l=1}^{s} (x_l \times \underline{k}_l)\colon \bigwedge_{l=1}^{s} x_l \in P^{(r_l)}(T_H^{(l+is-1)})\}\,,$$

where $P^{(q)}(A)$ denotes the family of all q-element subsets of the set A. It is clear that a belongs to the model. We must show that in M there exists no choice function. Suppose that such a function exists. Let w be a choice function for a. Then there exists a positive integer $q(w)$ such that if $\pi \in \Gamma^\omega$ and $\pi^{(0)} = \ldots = \pi^{(q(w))} = 1$ then $\pi(w) = w$. Let $q > q(w)$ be a number divisible by s. Further, let φ_l be a permutation of order r_l of the group Γ_{q+l-1} $(1 \leqslant l \leqslant s)$. We have $\psi_l = \varphi_l | T_H^{(q+l-1)} \neq 1$. Let $b_1, \ldots, b_s$ be the sets of elements of fixed cycles of permutations $\psi_1, \ldots, \psi_l$. Evidently, $b = \bigcup_{i=1}^{s} (b_i \times \underline{k}_i) \in a$. We define the element φ of the group putting $\varphi^{(i)} = 1$ for $i < q$, $\varphi^{(q+l-1)} = \varphi_l$ for $1 \leqslant l \leqslant s$ and for $i \geqslant q+s$, say $\varphi^{(i)} = 1$. Let $(b, x) \in w$. Then

$$\varphi\big((b, x)\big) \in \varphi(w) \equiv \big(\varphi(b), \varphi(x)\big) \in w \equiv \big(b, \varphi(x)\big) \in w\,.$$

Hence we get $x = w(b) = \varphi(x)$, which is impossible, because $x \neq \varphi(x)$. Therefore the proposition $[n]$ is false in the model M. At last, if $n \notin Q(G)$ then $n = \sum_{j=1}^{s} i_j k_j$, where i_j is the index of the proper subgroup of the group G and k_j is a positive integer. Let $H_1, \ldots, H_s \in \mathfrak{A}$ satisfy equalities $[G\colon H_j] = i_j$ for $1 \leqslant j \leqslant s$. Then in the model there is no choice function for

$$\{ \bigcup_{j=1}^{s} (T_{H_j}^{(l)} \times \underline{k}_j)\colon l \in \omega\}\,.$$

Thus the proposition $[n]^\omega$ is false in M, q.e.d.

LEMMA 2. *If p and q are prime numbers such that $p_1 = (p^q-1)/(p-1)$ is a prime number, then there exists a group G such that the indices of its proper subgroups are divisible by p_1 or p^q.*

Proof. Let p and q be prime numbers such that p_1 is a prime number. Let A be an elementary Abelian group of order p^q. Then the order of its automorphism group is divisible by p_1. In virtue of the Cauchy theorem there exists an automorphism α of the group A of the order p_1. Consider the set of pairs (a^s, x), where $x \in A$. This set becomes a group if we define multiplication by the formula

$$(a^s, x)(a^i, y) = \big(a^{s+i}, a^i(x)y\big)\,.$$

Denote this group by $G(p, q)$. The order of $G(p, q)$ is $p_1 p^q$. The set of elements of the form $(1, y)$ is a subgroup of the group $G(p, q)$ and its index is equal to p_1; the set of elements of the form $(a^s, 1)$ its a subgroup of index p^q. Let H be a subgroup of the group $G(p, q)$ such that is index is divisible neither by p_1 nor p^q. Thus the order of H is of the form $p_1 p^a$, where $0 < a < q$. By the Cauchy theorem there exist elements $u, v \in H$ of the orders p_1 and p, respectively. It is easy to see that $u = (a^s, x)$ and $v = (1, y)$, where x, y are elements of the group A and $p_1 \nmid s$.

Let $p_1 \nmid s$. We consider the automorphism a^s of the group A as a permutation of the set $A - \{1\}$. It is easy to see that a^s its a permutation with no fixed points, whence it is the product of $p-1$ cycles of the length p_1. If $w \in A - \{1\}$, $k \neq l$ and $p_1 \nmid kl$, then the elements w^k and w^l belong to different cycles of permutation a^s. If this were not the case (without loss of generality we may assume that $l = 1$), then the elements $w, w^k, w^{k^2}, \ldots$ would form a cycle of the length $\leqslant p-1$ of a non-identity permutation a^r, which is impossible because the order a^r is equal to p_1. Therefore, for arbitrary $w \in A - \{1\}$ the elements $w, w^2, \ldots, w^{p-1}$ belong to different cycles of permutation a^s. The elements of the form $u^k v^l u^{-k}$ are all elements of the group $G(p, q)$ of the form $(1, w)$. Thus there exist integers k_0 and l_0 such that $(1, x^{-1}) = u^{k_0} v^{l_0} u^{-k_0}$. Hence we get $(a^s, 1) = u^{k_0+1} v^{l_0} u^{-k_0}$. Thus all elements of the group $G(p, q)$ are of the form $(u^{k_0+1} v^{l_0} u^{-k_0})^r u^k v^l u^{-k}$, whence $G = H$.

THEOREM 3. *Let p and q be prime numbers such that $p_1 = (p^q-1)/(p-1)$ is a prime number. Then there exists a model M for ZF′ in which the propositions $[n]^0$, where n is of the form $kp_1 + lp^q$, are true, the propositions $[n]$, where n is of the form $kp + lq$, are false and the propositions $[n]^\omega$ for n of the form $kp_1 + lp^q$ are false.*

Proof. It is sufficient to put $G = G(p, q)$ in Theorem 2.

THEOREM 4. *If for every prime number p there exist infinitely many prime numbers of the form $(p^q-1)/(p-1)$, then there exists a model of* ZF′

in which every sentence $[n]^0$ *is true and every sentence* $[n]$ *for* $n>1$ *is false* (4).

Proof. Let A and B be arbitrary finite sets of positive integers and $\min B>1$. We shall show that there exists a model M for $\mathrm{ZF}' \cup \cup \{[n]^0\colon n \in A\} \cup \{\neg[n]\colon n \in B\}$. Let $p_1, \ldots, p_k$ be prime numbers such that every element of the set B is divisible by at least one of these numbers. From the assumption it follows that there exist prime numbers $q_1, \ldots, q_k$ such that $(p_i^{q_i}-1)/(p_i-1)$ are prime numbers greater than the numbers of the set A. By lemma 2 there exist groups $G_1, \ldots, G_k$ such that the index of every proper subgroup of the group G_i is divisible by at least one of the numbers of the set $C_i = \{p_i^{q_i}, (p_i^{q_i}-1)/(p_i-1)\}$. Let $G = \prod_{i=1}^{k} G_i$. Using lemma 1, we infer that the index of every proper finite subgroup of the group G is divisible by at least one of the numbers of the set $\bigcup_{i=1}^{k} C_i$. In virtue of theorem 2 there exists a model in which the propositions $[n]^0$ for $n \in A$ are true and the propositions $[n]$ for $n \in B$ are false. Using the compactness theorem we obtain the assertion of theorem 4.

(4) The famous conjecture on the existence of infinitely many Mersenne primes (i.e. the numbers 2^n-1) is a particular case of the conjecture stated in the assumption of the theorem.

References

[1] J. R. Gauntt, *Some restricted versions of axiom of choice* (Abstract 68T–176), Notices Amer. Math. Soc. 15 (1968), p. 351.

[2] A. Lévy, *The Fraenkel–Mostowski method for independence proofs in set theory. The theory of models*, Proceedings of the 1963 International Symposium at Berkeley, pp. 221–228.

[3] W. Marek, *Permutation models for* ZF*-set theory without individuals*, Warsaw University, Warsaw 1968 (doctoral dissertation).

[4] A. Mostowski, *Axiom of chöice for finite sets*, Fund. Math. 33 (1945), pp. 137–168.

[5] W. Sierpiński, *L'axiom du choix pour les ensembles finis*, Matematiche (Catania) 10 (1955), pp. 92–99.

[6] W. Szmielew, *On choice from finite sets*, Fund. Math. 34 (1947), pp. 75–80.

[7] K. Wiśniewski, *Weakened forms of the axiom of choice for finite sets*, Bull. Acad. Polon. Sci., Sér. Sci. Math., Astr. et Phys. 16 (1968), pp. 615–620.

[8] M. M. Zuckerman, *Finite versions of the axiom of choice*, Yeshiva University, New York 1967 (doctoral dissertation).

Reçu par la Rédaction le 27. 1. 1970

Some properties of convex metric spaces

by

B. Krakus (Stockholm)

1. Introduction. A point x of a metric space (X, ϱ) is said to be a *frontier point* (see [6]) if there exists a point $y \in X$ such that for every point $z \in X\backslash\{x\}$ we have

$$\varrho(y, x)+\varrho(x, z) > \varrho(y, z)\,.$$

The aim of this paper is to give a topological characterization of a frontier point of a compact strongly convex (1) finite-dimensional metric space (X, ϱ) without ramifications (2) (denoted by $(X, \varrho) \in \mathrm{SCWR}$). Holsztyński and Kuperberg have proved (see [4]) that every frontier point of a space $(X, \varrho) \in \mathrm{SCWR}$ is a labile point in X (3). It follows from [3] that the set of the frontier points of a space $(X, \varrho) \in \mathrm{SCWR}$ is a boundary set (see [8] too). In the present note it is shown that this set is compact. I give some remarks concerning the set of the stable points (3) of the SCWR-spaces.

2. Property of a ball. Let $(X, \varrho) \in \mathrm{SCWR}$. Then there exists exactly one function $\lambda\colon X\times X\times I \to X$ where $I = \langle 0, 1\rangle$ such that

$$\varrho\big(x, \lambda(x, y, t)\big) = t\varrho(x, y) \quad \text{and} \quad \varrho\big(y, \lambda(x, y, t)\big) = (1-t)\varrho(x, y)\,.$$

It is not difficult to see that the function λ defined above is continuous. Let us write $|x, y| = \lambda\big((x, y)\times I\big)$. This means that $z \in |x, y|$ if and only if

$$\varrho(x, z)+\varrho(z, y) = \varrho(x, y)\,.$$

(1) A metric space (X, ϱ) is said to be *strongly convex* (see [1]) if for every two points $x, y \in X$ there exists exactly one point $z \in X$ such that $\varrho(x, z) = \varrho(y, z) = \frac{1}{2}\varrho(x, y)$.

(2) A metric space (X, ϱ) is said to be *without ramifications* if for all points $x, y, z, s \in X$ the conditions $\varrho(x, y)+\varrho(y, z) = \varrho(x, z)$, $\varrho(x, y)+\varrho(y, s) = \varrho(x, s)$, $\varrho(x, z) = \varrho(x, s)$ imply $z = s$ (see [6]).

(3) A point p of topological space X is said to be a *labile point* in X if for any neighbourhood U of p there exists a homotopy $h\colon X\times I \to X$ such that the following conditions hold: (i) $h(x, 0) = x$ for every $x \in X$, (ii) $h(x, t) = x$ for every $x \in X\backslash U$, $t \in I$, (iii) $h(x, t) \in U$ for every $x \in U$, $t \in I$, (iv) $h(x, 1) \neq p$ for every $x \in X$ (see [2]). A point of topological space X is said to be a *stable point* in X if is not a labile point.