Bull. Aust. Math. Soc. **95** (2017), 177–182
doi:10.1017/S0004972716000757

A FINITE-TO-ONE MAP FROM THE PERMUTATIONS ON A SET

NATTAPON SONPANOW and PIMPEN VEJJAJIVA✉

(Received 30 June 2016; accepted 6 August 2016; first published online 19 October 2016)

Abstract

Forster ['Finite-to-one maps', *J. Symbolic Logic* **68** (2003), 1251–1253] showed, in Zermelo–Fraenkel set theory, that if there is a finite-to-one map from $\mathcal{P}(A)$, the set of all subsets of a set A, onto A, then A must be finite. If we assume the axiom of choice (AC), the cardinalities of $\mathcal{P}(A)$ and the set $S(A)$ of permutations on A are equal for any infinite set A. In the absence of AC, we cannot make any conclusion about the relationship between the two cardinalities for an arbitrary infinite set. In this paper, we give a condition that makes Forster's theorem, with $\mathcal{P}(A)$ replaced by $S(A)$, provable without AC.

2010 *Mathematics subject classification*: primary 03E10; secondary 03E25.

Keywords and phrases: finite-to-one map, permutation, axiom of choice.

1. Introduction

Intuitively, the *cardinality* of a set is the number of all elements of the set. We will denote the cardinality of a set A by $|A|$. There are many interesting facts concerning the relationship between the cardinalities of the set of all subsets of a set A and the set of all permutations on A, denoted by $\mathcal{P}(A)$ and $S(A)$, respectively. In Zermelo–Fraenkel set theory (ZF), we know, from Cantor's theorem, that $|\mathcal{P}(A)|$ is always greater than $|A|$. In [1], Dawson and Howard showed, in ZF, that $|S(A)|$ is also greater than $|A|$ for any set A such that $|A| \geq 3$. Moreover, they showed that, if we assume the axiom of choice (AC), then $|\mathcal{P}(A)|$ and $|S(A)|$ are equal for any infinite set A. However, without AC, we cannot make any conclusion about the relationship between the two cardinalities for an arbitrary infinite set. It has been shown in [1] that the statement 'there exists a set A such that $|\mathcal{P}(A)|$ is greater than $|S(A)|$' is consistent with ZF while the opposite conclusion is consistent with ZF as well. It is also consistent with ZF that 'there is some set A such that $|\mathcal{P}(A)|$ and $|S(A)|$ are not comparable'. As a result, any relationship of these two cardinalities for an arbitrary infinite set cannot be proved from ZF.

In [3], Forster showed, in ZF, that if there is a finite-to-one map from $\mathcal{P}(A)$ onto a set A, then A must be finite. Thus, in the absence of AC, we can ask whether or not

Forster's theorem still holds if we replace $\mathcal{P}(A)$ in the statement by $S(A)$. In this paper, we give a condition that makes the theorem provable without AC.

2. Preliminaries

We use $a, b, c, \ldots, A, B, C, \ldots$ for sets. Let ${}^{B}A$, $F \upharpoonright A$ and $F[A]$ denote the set of all functions from B into A, the *restriction* of a function F to A and the *image* of A under F, respectively. All other standard concepts in set theory and their notations will be used in the usual way. Proofs of all theorems in this section will be omitted. The details can be found in any set theory text book, for example [2].

We say that A is *equinumerous* to B, denoted by $A \approx B$, if there is a bijection from A onto B. Since the *cardinality* of a set represents the number of all elements of the set, it is defined so that for any sets A and B,

$$|A| = |B| \quad \text{if and only if} \quad A \approx B.$$

We call $|A|$ a *cardinal* (number).

Natural numbers are constructed as follows:

$$0 = \emptyset, 1 = \{0\}, 2 = \{0, 1\}, \ldots, n + 1 = \{0, 1, \ldots, n\}, \ldots,$$

and ω denotes the set of all natural numbers. A set is said to be *finite* if it is equinumerous to a (unique) natural number and this natural number is the cardinality of the set. A set which is not finite is said to be *infinite*.

Cardinal arithmetic is defined as follows. For cardinals $\mathfrak{m} = |M|$ and $\mathfrak{n} = |N|$, define $\mathfrak{m} + \mathfrak{n} = |M \cup N|$, where $M \cap N = \emptyset$, $\mathfrak{m} \cdot \mathfrak{n} = |M \times N|$ and $\mathfrak{m}^{\mathfrak{n}} = |{}^{N}M|$.

We say that M is *dominated* by N, written $M \preceq N$, if there is an injection from M into N. We define $|M| \leq |N|$ if $M \preceq N$ and say that $|M| < |N|$ if $|M| \leq |N|$ but $|M| \neq |N|$. It is easy to see that $\leq$ is reflexive and transitive. It is antisymmetric by the Schröder–Bernstein theorem.

A *well-ordering* R on A is a linear ordering on A such that every nonempty subset of A has an R-least element. A set is *well-ordered* if there is a well-ordering on it.

A set A is *transitive* if each element of A is a subset of A. An *ordinal* is a transitive set which can be well-ordered by $\in$. Note that every natural number and ω are ordinals. Every member of an ordinal is also an ordinal. The class of ordinals can be well-ordered by $\in$, which we sometimes write $<$ instead. We will use $\alpha, \beta, \gamma, \ldots$ for ordinals.

The *successor* of α, denoted by $\alpha + 1$, is defined by $\alpha + 1 = \alpha \cup \{\alpha\}$. An ordinal α is a *successor ordinal* if $\alpha = \beta + 1$ for some ordinal β. An ordinal $\alpha \neq 0$ which is not a successor ordinal is called a *limit ordinal*.

An important property of well-ordered sets is that if $<$ is a well-ordering on A, then $(A, <)$ is isomorphic to a unique ordinal. Such an ordinal will be denoted by $\mathrm{type}(A, <)$. We may drop A and simply write $\mathrm{type}(<)$, which means that $<$ is a well-ordering on its field. We define the cardinality of a well-ordered set as the least ordinal equinumerous to it. Note that every natural number and ω are cardinals.

https://doi.org/10.1017/S0004972716000757 Published online by Cambridge University Press

The cardinal number of an infinite well-ordered set is called an *aleph*. We have $\aleph + \aleph = \aleph \cdot \aleph = \aleph$ for any aleph $\aleph$. If A is a set of alephs, then $\bigcup A$ is also an aleph and it is the supremum of A.

Hartogs' theorem states that for any cardinal $\mathfrak{m}$, there exists a least aleph, denoted by $\aleph(\mathfrak{m})$, such that $\aleph(\mathfrak{m}) \not\leq \mathfrak{m}$.

We define ω_α (or $\aleph_\alpha$) inductively as follows:

$$\begin{aligned} \omega_0 &= \omega, \\ \omega_{\alpha+1} &= \aleph(\omega_\alpha), \\ \omega_\alpha &= \bigcup\{\omega_\xi : \xi < \alpha\} \quad \text{if } \alpha \text{ is a limit ordinal.} \end{aligned}$$

Every aleph is equal to ω_α for some α. We write $\omega_\alpha^{<\omega}$ for $\bigcup\{\omega_\alpha^n : n < \omega\}$. Note that $\omega_\alpha^{<\omega} \approx \omega_\alpha$.

The axiom of choice (AC) states that every set can be well-ordered. Thus, under AC, every infinite cardinal is an aleph. There are many equivalent statements of AC, such as the comparability of cardinals and Zorn's lemma. Without AC, we cannot choose an arbitrary object from each nonempty set in an infinite collection. Therefore, in ZF, all proofs that require infinite processes must be constructive. Without AC, cardinal comparability holds for alephs, but not for arbitrary cardinals in general. Therefore, we cannot guarantee that there is an injection from ω into an arbitrary infinite set. A set A is *Dedekind-infinite* if $\omega \preceq A$ or, equivalently, A has a denumerable subset. For more details on the axiom of choice, see [4].

We write $A \preceq^* B$ or $|A| \leq^* |B|$ if A is empty or there is a surjection from B onto A. It is easy to see that, for any cardinals $\mathfrak{m}$ and $\mathfrak{n}$, $\mathfrak{m} \leq \mathfrak{n}$ implies that $\mathfrak{m} \leq^* \mathfrak{n}$. But the converse does not necessarily hold without AC. Analogous to Hartogs' theorem, for any cardinal $\mathfrak{m}$, there exists an aleph $\aleph$ such that $\aleph \not\leq^* \mathfrak{m}$.

All work in this paper is done in ZF without AC.

3. Main theorem

In this section we give our main result. We start with some relevant definitions.

Definition 3.1. For any set A, define $S(A) = \{f : f \text{ is a bijection on } A\}$.

Definition 3.2. A function $F : A \to B$ is *finite-to-one* if $F^{-1}[\{b\}]$ is finite for all $b \in \operatorname{ran} F$.

Notation 3.3. We write $F : A \twoheadrightarrow B$ if F is a surjection from A onto B and write id_A for the identity function on A.

Definition 3.4. We say that A is *even* if there is a set B such that $A \approx 2 \times B$ and A is *almost even* if there is a function f on A which has no fixed point and $f \circ f = \mathrm{id}_A$.

Note that if A is even, then A is almost even since if $g : A \to 2 \times B$ is a bijection, then $f = g^{-1} \circ h \circ g$, where $h : 2 \times B \to 2 \times B$, defined by $h(0, x) = (1, x)$ and $h(1, x) = (0, x)$, has no fixed point and $f \circ f = \mathrm{id}_A$.

https://doi.org/10.1017/S0004972716000757 Published online by Cambridge University Press

Since '$\mathfrak{m} = 2\mathfrak{m}$ for all infinite cardinals $\mathfrak{m}$' is a weaker form of AC (see [5]) and it implies that every infinite set is even and thus almost even, these consequences are weaker than AC as well.

PROPOSITION 3.5. *If A is almost even, then there is a partition of A each of whose members has exactly two elements.*

PROOF. Assume that A is almost even. Then there is a function f on A which has no fixed point and $f \circ f = \mathrm{id}_A$. Let $\Pi = \{\{x, f(x)\} \mid x \in A\}$. Since $f \circ f = \mathrm{id}_A$, Π is a partition of A. Note that, since f has no fixed point, each member of Π is of cardinality 2. □

DEFINITION 3.6. We call the partition Π constructed above an *a.e.-partition* of A (induced by f).

PROPOSITION 3.7. *If A is almost even and Π is an a.e.-partition of A, then we can construct an injection from $\mathcal{P}(\Pi)$ into $S(A)$. Thus, a surjection from $S(A)$ onto $\mathcal{P}(\Pi)$ can be constructed as well.*

PROOF. Let Π be an a.e.-partition of A induced by f. An injection $G\colon \mathcal{P}(\Pi) \to S(A)$ is defined by

$$G(\Sigma) = \left(f \restriction \bigcup \Sigma\right) \cup \mathrm{id}_{A - \bigcup \Sigma}.$$

Define a surjection from $S(A)$ onto $\mathcal{P}(\Pi)$ by

$$h \mapsto \begin{cases} G^{-1}(h) & \text{if } h \in \operatorname{ran} G, \\ \emptyset & \text{otherwise.} \end{cases}$$

□

The proofs of the lemmas below as well as the main theorem are modified from those in [3].

LEMMA 3.8. *Suppose that there exists a finite-to-one map $F\colon S(A) \to A$ and A is infinite. If A is almost even, then an a.e.-partition of A is Dedekind-infinite.*

PROOF. Let Π be an a.e.-partition of A induced by f. Define $G\colon A \to \Pi$ by $G(x) = \{x, f(x)\}$. Then G is finite-to-one and onto. So $H = G \circ F\colon S(A) \to \Pi$ is also finite-to-one. For each natural number $m \geq 2$, define

$$X_m = \{g \in S(A) : |\{x \in A : g(x) \neq x\}| = m\}.$$

Note that these X_m are pairwise disjoint and nonempty. As a result, since H is finite-to-one, for each n, there are only finitely many m such that $H[X_m] = H[X_n]$. Hence, $T = \{H[X_m] : 2 \leq m < \omega\}$ is a denumerable set.

Define $\Gamma\colon T \to S(A)$ by $\Gamma(B) = (f \restriction \bigcup B) \cup \mathrm{id}_{A - \bigcup B}$. Clearly Γ is one-to-one, so $\operatorname{ran}\Gamma$ is a denumerable subset of $S(A)$. Since H is finite-to-one, $H[\operatorname{ran}\Gamma]$ is a denumerable subset of Π. Thus, Π is Dedekind-infinite. □

https://doi.org/10.1017/S0004972716000757 Published online by Cambridge University Press

LEMMA 3.9. *Let A be almost even and Π be an a.e.-partition of A. Suppose that there exists a finite-to-one and onto map $H\colon S(A) \twoheadrightarrow \Pi$, where A is infinite. Then we can construct:*

(1) *a surjection from Π onto ω_α from a surjection $h\colon S(A) \twoheadrightarrow \omega_\alpha$;*
(2) *a surjection from $S(A)$ onto $\omega_{\alpha+1}$ from a surjection $g_\alpha\colon \Pi \twoheadrightarrow \omega_\alpha$;*
(3) *a surjection from $S(A)$ onto ω_λ from a collection $\{g_\alpha\colon \alpha < \lambda\}$, where $g_\alpha\colon \Pi \twoheadrightarrow \omega_\alpha$ for all $\alpha < \lambda$ and λ is a limit ordinal.*

PROOF. (1) Suppose that $h\colon S(A) \twoheadrightarrow \omega_\alpha$. Define $g\colon \Pi \to \mathcal{P}(\omega_\alpha)$ by $g(P) = h[H^{-1}[\{P\}]]$. Since H is finite-to-one, each $g(P)$ is a finite subset of ω_α, so $\bigcup \operatorname{ran} g \subseteq \omega_\alpha$. Since we can regard each $g(P)$ as a finite sequence of ordinals less than ω_α, $\operatorname{ran} g$ can be well-ordered by the lexicographic order and thus $|\operatorname{ran} g|$ is an aleph. Since h is onto and $h(f) \in h[H^{-1}[\{H(f)\}]] = g(H(f))$ for all $f \in S(A)$, $\omega_\alpha \subseteq \bigcup \operatorname{ran} g$. Then $|\bigcup \operatorname{ran} g| = \aleph_\alpha$. Since each member of $\operatorname{ran} g$ is a finite set of ordinals, $|\operatorname{ran} g| \geq \aleph_\alpha$. Then, by recursion, we can construct an injection from ω_α into $\operatorname{ran} g$. Since there is a canonical injection from $\operatorname{ran} g$ into $\bigcup\{\omega_\alpha^n : n < \omega\} = \omega_\alpha^{<\omega}$, by using the canonical bijection from $\omega_\alpha^{<\omega}$ onto ω_α, we can construct an injection from $\operatorname{ran} g$ into ω_α. Therefore, we can construct a bijection ρ from $\operatorname{ran} g$ onto ω_α by the Schröder–Bernstein theorem. Thus, $\rho \circ g$ is a surjection from Π onto ω_α.

(2) Suppose that $g_\alpha\colon \Pi \twoheadrightarrow \omega_\alpha$. Then the map $\Sigma \mapsto g[\Sigma]$ is a surjection from $\mathcal{P}(\Pi)$ onto $\mathcal{P}(\omega_\alpha)$. Similarly, from the canonical bijection from ω_α onto $\omega_\alpha \times \omega_\alpha$, we can construct a bijection from $\mathcal{P}(\omega_\alpha)$ onto $\mathcal{P}(\omega_\alpha \times \omega_\alpha)$. By Lemma 3.7, there is a surjection from $S(A)$ onto $\mathcal{P}(\Pi)$. Thus, we obtain a surjection from $S(A)$ onto $\mathcal{P}(\omega_\alpha \times \omega_\alpha)$. In order to have a surjection from $S(A)$ onto $\omega_{\alpha+1}$, it is enough to construct a surjection from $\mathcal{P}(\omega_\alpha \times \omega_\alpha)$ onto $\omega_{\alpha+1}$.

Define a function from $\mathcal{P}(\omega_\alpha \times \omega_\alpha)$ into $\omega_{\alpha+1}$ by

$$R \mapsto \begin{cases} \operatorname{type}(R) & \text{if } R \subseteq \omega_\alpha \times \omega_\alpha \text{ is a well-ordering,} \\ 0 & \text{otherwise.} \end{cases}$$

The above map is surjective since if $\gamma < \omega_{\alpha+1}$, then $|\gamma| \leq \omega_\alpha$, so there exists an injection $h\colon \gamma \to \omega_\alpha$. Thus, we can define the well-ordering $R \subseteq \omega_\alpha \times \omega_\alpha$ induced by this h.

(3) Suppose that λ is a limit ordinal and we have a collection $\{g_\alpha : \alpha < \lambda\}$, where $g_\alpha\colon \Pi \twoheadrightarrow \omega_\alpha$ for all $\alpha < \lambda$. Consider each $\beta < \omega_\lambda$, that is, $\beta < \omega_\alpha$ for some $\alpha < \lambda$. Notice that, since g_α is onto, $\{\alpha < \lambda : \beta \in \operatorname{ran} g_\alpha\} \neq \emptyset$. Define $\mu_\beta = \min\{\alpha < \lambda : \beta \in \operatorname{ran} g_\alpha\}$ and $\Pi_\beta = g_{\mu_\beta}^{-1}[\{\beta\}]$. Let $B = \{\Pi_\beta : \beta < \omega_\lambda\}$. Then $|B| \leq \aleph_\lambda$. Note that if $\alpha < \lambda$ and $\omega_\alpha < \beta < \gamma < \omega_{\alpha+1}$, then

$$\mu_\beta = \min\{\xi < \lambda : \beta < \omega_\xi\} = \alpha + 1 = \min\{\xi < \lambda : \gamma < \omega_\xi\} = \mu_\gamma$$

and so $\Pi_\beta \neq \Pi_\gamma$. Thus, $|B| \geq \aleph_\alpha$ for all $\alpha < \lambda$, which implies that $|B| \geq \aleph_\lambda$. Hence, $|B| = \aleph_\lambda$. Thus, we may assume that for all distinct subscripts $\alpha, \beta < \omega_\lambda$, $\Pi_\alpha \neq \Pi_\beta$ and so there is an obvious bijection ρ from B onto ω_λ.

https://doi.org/10.1017/S0004972716000757 Published online by Cambridge University Press

Define a surjection from $\mathcal{P}(\Pi)$ onto ω_λ by

$$\Sigma \mapsto \begin{cases} \rho(\Sigma) & \text{if } \Sigma \in B, \\ 0 & \text{if } \Sigma \notin B. \end{cases}$$

By Lemma 3.7, we can construct a surjection from $S(A)$ onto $\mathcal{P}(\Pi)$. So we have a surjection from $S(A)$ onto ω_λ. □

Now we are ready to prove the main result.

THEOREM 3.10. *Suppose that A is almost even and there exists a finite-to-one and onto map $F\colon S(A) \twoheadrightarrow A$. Then A is finite.*

PROOF. Suppose to the contrary that A is infinite. Let Π be an a.e.-partition of A. By Lemma 3.8, $\aleph_0 \leq |\Pi|$. So we have a surjection $g_0\colon \Pi \twoheadrightarrow \omega_0$.

For each ordinal α, define g_α recursively as follows. Define $g_{\alpha+1}\colon \Pi \twoheadrightarrow \omega_{\alpha+1}$ from $g_\alpha\colon \Pi \twoheadrightarrow \omega_\alpha$ by (2) and (1) of Lemma 3.9, and $g_\lambda\colon \Pi \twoheadrightarrow \omega_\lambda$ from $\{g_\alpha : \alpha < \lambda\}$ by (3) and (1) of Lemma 3.9, where λ is a limit ordinal. Then, for any ordinal α, $\aleph_\alpha \leq^* |\Pi|$, which contradicts the fact that there is an aleph $\aleph$ such that $\aleph \not\leq^* |\Pi|$. □

We can see from the proofs that, in order to relate subsets of A to permutations on A, we need the condition that A is almost even to have a partition of A each of whose members is finite with cardinality at least 2 and also a fixed permutation f on A with no fixed point such that $f \restriction P$ is also a permutation on P for all members P of the partition. Thus, more generally, the theorem also holds when there are a natural number $n \geq 2$ and a bijection f on A such that f has no fixed point and $\underbrace{f \circ \ldots \circ f}_{n \text{ copies}} = \mathrm{id}_A$.

References

[1] J. W. Dawson Jr. and P. E. Howard, 'Factorials of infinite cardinals', *Fund. Math.* **93** (1976), 186–195.
[2] H. B. Enderton, *Elements of Set Theory* (Academic Press, New York, 1977).
[3] T. Forster, 'Finite-to-one maps', *J. Symbolic Logic* **68** (2003), 1251–1253.
[4] T. J. Jech, *The Axiom of Choice* (North-Holland, Amsterdam, 1973).
[5] G. Sageev, 'An independence result concerning the axiom of choice', *Ann. Math. Logic* **8** (1975), 1–184.

NATTAPON SONPANOW, Department of Mathematics and Computer Science,
Faculty of Science, Chulalongkorn University, Bangkok, Thailand
e-mail: chonattapon@gmail.com

PIMPEN VEJJAJIVA, Department of Mathematics and Computer Science,
Faculty of Science, Chulalongkorn University, Bangkok, Thailand
e-mail: Pimpen.V@chula.ac.th

https://doi.org/10.1017/S0004972716000757 Published online by Cambridge University Press