Consequences of arithmetic for set theory

Author(s):
Halbeisen, Lorenz; Shelah, Saharon

Publication date:
1994

Permanent link:
https://doi.org/10.3929/ethz-b-000423096

Originally published in:
The Journal of Symbolic Logic 59(1), https://doi.org/10.2307/2275247

THE JOURNAL OF SYMBOLIC LOGIC
Volume 59, Number 1, March 1994

CONSEQUENCES OF ARITHMETIC FOR SET THEORY

LORENZ HALBEISEN AND SAHARON SHELAH

Abstract. In this paper, we consider certain cardinals in ZF (set theory without AC, the axiom of choice). In ZFC (set theory with AC), given any cardinals $\mathscr{C}$ and $\mathscr{D}$, either $\mathscr{C} \leq \mathscr{D}$ or $\mathscr{D} \leq \mathscr{C}$. However, in ZF this is no longer so. For a given infinite set A consider $\operatorname{seq}^{1\text{-}1}(A)$, the set of all sequences of A without repetition. We compare $|\operatorname{seq}^{1\text{-}1}(A)|$, the cardinality of this set, to $|\mathscr{P}(\mathscr{A})|$, the cardinality of the power set of A. What is provable about these two cardinals in ZF? The main result of this paper is that $\mathrm{ZF} \vdash \forall A(|\operatorname{seq}^{1\text{-}1}(A)| \neq |\mathscr{P}(\mathscr{A})|)$, and we show that this is the best possible result. Furthermore, it is provable in ZF that if B is an infinite set, then $|\operatorname{fin}(B)| < |\mathscr{P}(B)|$ even though the existence for some infinite set B^* of a function f from $\operatorname{fin}(B^*)$ onto $\mathscr{P}(B^*)$ is consistent with ZF.

§0. Introduction, definitions, and basic theorems.

Introduction. In ZFC the cardinality of ordinal numbers plays an important role, since by AC each set has the cardinality of some ordinal.

We use "alephs" for the cardinalities of ordinals. Thus in ZFC each cardinal number is an aleph. However, this need not be the case in ZF.

If we have a model M of ZF in which the axiom of choice fails, then we have more cardinals in M than in a model V of ZFC, even if we have fewer sets in M than in V. (This occurs when the choice-functions are not all in M.) This is because the ordinals are in M and, hence, the alephs as well.

In this paper we are interested in the relation between three cardinals arising in connection with a set S, namely,

(1) the cardinality of the power set of S,

(2) the cardinality of the finite subsets of S,

(3) the cardinality of the finite sequences without repetition of S.

This section contains definitions and basic theorems provable in ZF. In the next section we present two relative consistency proofs illustrating possible relations between these cardinals.

The last two sections contain three results provable in ZF. The proofs of these are based on the same idea originally from E. Specker, who used it to prove that the axiom of choice follows from the generalised continuum hypothesis [Sp1]. Assuming the existence of a function we derive a contradiction to Hartogs's Theorem.

Received November 9, 1992; revised February 8, 1993.

Parts of this work are of the first author's Diplomarbeit at the ETH Zürich. He is grateful to his supervisor, Professor H. Läuchli.

Research of the second author was partially supported by the Basic Research Fund, Israeli Academic; Publ. No. 488.

0022-4812/94/5901-0002/$02.10

Because we do not use AC, our proofs are constructive. But we will see that sometimes arithmetic is powerful enough for our constructions, making it an adequate substitute for AC.

CARDINALS. A *cardinal number* $\mathscr{C}$ is the equivalence class of all sets which have the *same size*. (Two sets are said to have the same size iff there is a bijection between them.)

ALEPHS. A cardinal number $\mathscr{C}$ is an *aleph* if it contains a well-ordered set.

We use calligraphic letters to denote cardinals and $\aleph$'s to denote the alephs.

We denote the cardinality of the set s by $|s|$.

RELATIONS BETWEEN CARDINALS. We say that the cardinal number $\mathscr{C}$ is less than or equal to the cardinal number $\mathscr{D}$ iff there are sets $c \in \mathscr{C}$, $d \in \mathscr{D}$ and a 1-1 function from c into d.

In this case we write $\mathscr{C} \leq \mathscr{D}$. We write $\mathscr{C} < \mathscr{D}$ for $\mathscr{C} \leq \mathscr{D}$ and $\mathscr{C} \neq \mathscr{D}$.

If $c \in \mathscr{C}$, $d \in \mathscr{D}$, and we have a function from d onto c, then we write $\mathscr{C} \leq^* \mathscr{D}$.

We also need some well-known facts provable in ZF.

HARTOGS'S THEOREM. *Given a cardinal $\mathscr{C}$ there is a least aleph $\aleph(\mathscr{C})$ such that $\aleph(\mathscr{C}) \not\leq \mathscr{C}$.*

PROOF. See [Je1, p. 25]. □

CANTOR-BERNSTEIN THEOREM. *If $\mathscr{C}$ and $\mathscr{D}$ are cardinals with $\mathscr{C} \leq \mathscr{D}$ and $\mathscr{D} \leq \mathscr{C}$, then $\mathscr{C} = \mathscr{D}$.*

PROOF. See [Je1, p. 23]. □

CANTOR NORMAL FORM THEOREM. *Any ordinal α can be written as*

$$\alpha = \sum_{i=0}^{j} \omega^{\alpha_i} \cdot k_i$$

with $\alpha \geq \alpha_0 > \alpha_1 > \cdots > \alpha_j \geq 0$, $1 \leq k_i < \omega$, $0 \leq j < \omega$.

PROOF. See [Ba, p. 57 ff.]. □

COROLLARY 1. *The Cantor Normal Form Theorem does not depend on AC.*

PROOF. The proof of the Cantor Normal Form Theorem requires no infinite choices. □

COROLLARY 2. *If $\alpha = \sum_{i=0}^{j} \omega^{\alpha_i} \cdot k_i$ is a Cantor normal form, then define $\overleftarrow{\alpha}$ by*

$$\overleftarrow{\alpha} := \sum_{i=j}^{0} \omega^{\alpha_i} \cdot k_i = \omega^{\alpha_0} \cdot k_0.$$

Then (in ZF) $|\alpha| = |\overleftarrow{\alpha}|$.

PROOF. See [Ba, p. 60]. □

COROLLARY 3. *For any ordinal α, ZF implies the existence of the following bijections:*

$$F^{\alpha}_{\mathrm{seq}^{1\text{-}1}} : \alpha \to \mathrm{seq}^{1\text{-}1}(\alpha) \qquad (=: \textit{finite sequences of } \alpha \textit{ without repetition}),$$

$$F^{\alpha}_{\mathrm{seq}} : \alpha \to \mathrm{seq}(\alpha) \qquad (=: \textit{finite sequences of } \alpha),$$

$$F^{\alpha}_{\mathrm{fin}} : \alpha \to \mathrm{fin}(\alpha) \qquad (=: \textit{finite subsets of } \alpha).$$

PROOF. Use the Cantor Normal Form Theorem, Corollary 2, order the finite subsets of α, and then use the Cantor-Bernstein Theorem. □

§1. **Consistency results.** In this section we work in the Mostowski permutation model to derive some relative consistency results. The permutation models are models of ZFA, set theory with atoms (see [Je2, p. 44 ff.]).

The atoms $x \in A$ may also be considered to be sets which contain only themselves. This means $x \in A \Rightarrow x = \{x\}$ (see [Sp2, p. 197] or [La, p. 2]). Thus, the permutation models are models for ZF without the axiom of foundation. However, the Jech-Sochor Embedding Theorem (see [Je, p. 208 ff.]) implies consistency results for ZF.

In the permutation models we have a set of atoms A and a group $\mathscr{G}$ of permutations of A. Let $\mathscr{F}$ be a normal filter on $\mathscr{G}$ (see [Je1, p. 199]). We say that x is *symmetric* if the group $\mathrm{sym}_{\mathscr{G}}(x) := \{\pi \in \mathscr{G} : \pi(x) = x\}$ belongs to $\mathscr{F}$.

Let us further assume that $\mathrm{sym}_{\mathscr{G}}(a) \in \mathscr{F}$ for every atom a, that is, all atoms are symmetric (with respect to $\mathscr{G}$ and $\mathscr{F}$), and let $\mathscr{B}$ be the class of all hereditarily symmetric objects. The class $\mathscr{B}$ is both a permutation model and a transitive class: all atoms are in $\mathscr{B}$ and $A \in \mathscr{B}$. Moreover, $\mathscr{B}$ is a transitive model of ZFA.

Given a finite set $E \subset A$, let $\mathrm{fix}_{\mathscr{G}}(E) := \{\pi \in \mathscr{G} : \pi a = a \text{ for all } a \in E\}$ and let $\mathscr{F}$ be the filter on $\mathscr{G}$ generated by $\{\mathrm{fix}_{\mathscr{G}}(E) : E \subset A \text{ is finite}\}$. $\mathscr{F}$ is a normal filter and x is symmetric iff there is a finite set of atoms E_x such that $\pi(x) = x$ whenever $\pi \in \mathscr{G}$ and $\pi a = a$ for each $a \in E_x$. Such an E_x is called a support for x.

Now the Mostowski model is constructed as follows (see also [Je2, p. 49 ff.]):

(1) The set of atoms A is infinite.

(2) R is an order-relation on A.

(3) With respect to R, A is a dense linearly ordered set without end points.

(4) Let Aut_R be the group of all permutations of A such that for all atoms x, $y \in A$ and each $\pi \in \mathrm{Aut}_R$, if Rxy then $R\pi(x)\pi(y)$.

(5) Let $\mathscr{F}$ be generated by $\{\mathrm{fix}(E) : E \subset A \text{ is finite}\}$.

We will write $x < y$ instead of Rxy.

The subsets of A (in the Mostowski model) are symmetric sets. Hence, each subset of A has a finite support.

If $x \subseteq A$ (in the Mostowski model) and x has nonempty support E_x, then an $a \in E_x$ may or may not belong to x.

FACT. *If $b \neq x \cup E_x$ and there are two elements $a_0, a_1 \in E_x$ with $a_0 < b < a_1$ such that $\forall c(a_0 < c < a_1 \to c \notin E_x)$, then $\forall c(a_0 < c < a_1 \to c \notin x)$.*

Proof. Otherwise, we construct a $\pi \in \mathrm{Aut}_R$ such that $\pi a_i = a_i$ for all $a_i \in E_x$ and $\pi c = b$. Then $\pi(x) \neq x$, which is a contradiction.

We can similarly show that if $a_0 < b < a_1$ and $b \in x \setminus E_x$, then $\forall c(a_0 < c < a_1 \to c \in x)$. The cases when $\neg\exists a_1(a_1 \in E_x \wedge b < a_1)$ or $\neg\exists a_0(a_0 \in E_x \wedge b > a_0)$ are similar.

Hence, given a finite set $E \subset A$ ($|E| := n$), we can construct $2^n \cdot 2^{n+1} = 2^{2n+1}$ subsets $x \subseteq A$ such that E is a support of x.

Given a finite subset E of A, consider the set $\mathscr{E}$ of subsets of A with support E. We use R to order $\mathscr{E}$ as follows. Given $E_1 = \{a_1, \ldots, a_n\}$ and $E_2 =$

$\{a_1, \ldots, a_n, \ldots, a_{n+k}\}$ with $a_i < a_j$ whenever $i < j$ are given $x \in \mathscr{E}$, if x is the lth subset with support E_1, then x is also the lth subset with support E_2.

Finally, we define the function

$$F : \operatorname{fin}(A) \to \mathscr{P}(A) \text{ by}$$
$$E \mapsto |E|\text{th subset of } A \text{ constructible with support } E.$$

It is easy to see that F is onto.

If $E \subset A$ is finite, then use R to order the subsets of E and use the corresponding lexicographic order on the set of permutations of subsets of E. The set of permutations of subsets of E is isomorphic to $\operatorname{seq}^{1\text{-}1}(E)$. In fact, we can order $\operatorname{seq}^{1\text{-}1}(E)$ for each finite $E \subset A$.

For each subset $x \subseteq A$ there is exactly one smallest support $E_x (=: \operatorname{supp}(x))$.

If $|\operatorname{supp}(x)| = n$, then put $\overline{x} := |\{y \subseteq A : \operatorname{supp}(y) = \operatorname{supp}(x)\}| \leq 2^{2n+1}$ and for $l \leq \overline{x}$ define as above the lth element of $\{y \subseteq A : \operatorname{supp}(y) = \operatorname{supp}(x)\}$. We say that: "$y \subseteq A$ is the lth subset of A with support $\operatorname{supp}(x)$".

Now choose 24 distinct elements $a_0, \ldots, a_{23} \in A$ and define $A_{24} := \{a_0, \ldots, a_{23}\}$. A simple calculation shows that

$$(*) \qquad \text{if } n \geq 12, \text{ then } 2 \cdot 2^{2n+1} < n!$$

Take a finite subset E of A, and let $y \subseteq A$ be the lth subset of A with $\operatorname{supp}(y) = E$. Put $D := \operatorname{supp}(y) \Delta A_{24}$ (where Δ denotes symmetric difference) and $d := |D|$. Define the function $\operatorname{Seq}_A : \mathscr{P}(A) \to \operatorname{seq}^{1\text{-}1}(A)$ by

$$\operatorname{Seq}_A(y) := \begin{cases} \text{the } l\text{th permutation of } \operatorname{supp}(y) & \text{if } |\operatorname{supp}(y)| \geq 12, \\ \text{the } (d! - l - 1)\text{th permutation of } \operatorname{supp}(y) & \text{otherwise.} \end{cases}$$

Seq_A is well defined because of $(*)$ and $d \geq 13$.

It is easy to see that Seq_A is 1-1. If there is a bijection between $\mathscr{P}(A)$ and $\operatorname{seq}^{1\text{-}1}(A)$, then we find an ω-sequence$^{1\text{-}1}$ in A using an analogous construction. But this is a contradiction (see §3).

Even more is true in the Mostowski model ($\mathscr{A} := |\text{Atoms}|$);

$$\mathscr{A} < \operatorname{fin}(\mathscr{A}) < \mathscr{P}(\mathscr{A}) < \operatorname{seq}^{1\text{-}1}(\mathscr{A}) < \operatorname{fin}(\operatorname{fin}(\mathscr{A})) < \operatorname{seq}(\mathscr{A}) < \mathscr{P}(\mathscr{P}(\mathscr{A})).$$

(We omit the proof.)

Our interest there is in the following result.

THEOREM 1. *The following theories are equiconsistent*:

(i) *ZF*,

(ii) $ZF + \exists \mathscr{A}(\mathscr{P}(\mathscr{A}) < \operatorname{seq}^{1\text{-}1}(\mathscr{A}))$,

(iii) $ZF + \exists \mathscr{A}(\mathscr{P}(\mathscr{A}) \leq^* \operatorname{fin}(\mathscr{A}))$.

PROOF. It was shown above that in the Mostowski model there is a cardinal $\mathscr{A}$; namely, the cardinality of the set of atoms, for which both (ii) and (iii) hold.

Unfortunately, the Mostowski model is only a model of ZFA. But it is well known that $\operatorname{Con}(ZF) \Rightarrow \operatorname{Con}(ZFC)$, and the Jech-Sochor Embedding Theorem provides a model of (ii) and (iii). □

THEOREM 2. *The following theories are equiconsistent*:

(i) *ZF*,

(ii) $ZF + \exists \mathscr{A}(\mathrm{seq}(\mathscr{A}) < \mathrm{fin}(\mathscr{A}))$.

PROOF. By the Jech-Sochor Embedding Theorem it is enough to construct a permutation model $\mathscr{B}$ in which there is a set A, such that

(a) there is a 1-1 function from $\mathrm{seq}(A)$ into $\mathrm{fin}(A)$,

(b) there is no bijection between $\mathrm{seq}(A)$ and $\mathrm{fin}(A)$.

We construct, by induction on $n \in \omega$, the following:

(α) $A_0 := \{\{\varnothing\}\}$; $Sq_0(\{\varnothing\})$:=the empty sequence; G_0 := the group of all permutations of A_0.

Let k_n be the number of elements of G_n, and let $\mathscr{E}_n$ be the set of sequences of A_n in length less than or equal to n which are not in range(Sq_n). Then

(β) $A_{n+1} := A_n \cup \{(n+1, \zeta, i) : \zeta \in \mathscr{E}_n \text{ and } i < k_n + k_n\}$.

(δ) Sq_{n+1} is a function from A_{n+1} to $\mathrm{seq}(A_n)$ defined as follows:

$$Sq_{n+1}(x) = \begin{cases} Sq_n(x) & \text{if } x \in A_n, \\ \zeta & \text{if } x = (n+1, \zeta, i) \in A_{n+1} \setminus A_n. \end{cases}$$

(γ) G_{n+1} is the subgroup of the group of permutations of A_{n+1} containing all permutations h such that for some $g_h \in G_n$ and $j_h < k_n + k_n$ we have

$$h(x) = \begin{cases} g_h(x) & \text{if } x \in A_n, \\ (n+1, g_h(\zeta), i +_n j_h) & \text{if } x = (n+1, \zeta, i) \in A_{n+1} \setminus A_n, \end{cases}$$

where $g_n(\zeta)(m) := g_h(\zeta(m))$ and $+_n$ is the addition modulo $k_n + k_n$. Let $A := \bigcup\{A_n : n \in \omega\}$ and $Sq := \bigcup\{Sq_n : n \in \omega\}$. Then Sq is a function from A onto $\mathrm{seq}(A)$.

Further, define for each natural number n partial functions f_n from A to $A \cup \{\varnothing\}$ as follows. If $lg(x)$ denotes the length of $Sq(x)$ and $n < lg(x)$, then $f_n(x) := Sq(x)(n)$; otherwise, let $f_n(x) = \varnothing$.

Let $\mathrm{Aut}(A)$ be the group of all permutations of A. Then $\mathscr{G} := \{H \in \mathrm{Aut}(A) : \forall n \in \omega(H|_{A_n} \in G_n)\}$ is a group of permutations of A. Let $\mathscr{F}$ be the normal filter on $\mathscr{G}$ generated by $\{\mathrm{fix}(E) : E \subset A \text{ is finite}\}$, and let $\mathscr{B}$ be the class of all hereditarily symmetric objects.

Now $A \in \mathscr{B}$ and for each $n \in \omega$, $\mathrm{supp}(f_n) = \varnothing$; hence, f_n belongs to $\mathscr{B}$ too.

Now define on A an equivalence relation as follows:

$$x \sim y \quad \text{iff} \quad \forall n(f_n(x) = f_n(y)). \qquad \square$$

FACTS. (1) *Every equivalence class of A is finite.* (*Because of each A_n is finite; hence, each k_n*).

(2) $\mathrm{seq}(A) = \{\zeta_x : x \in A\}$, *where* $\zeta_x(n) := f_n(x)$ (*if* $f_n(x) \neq \varnothing$).

(3) *For every finite subset B of A there are finite subsets C, Y of A and a natural number $k > 1$ such that $B \subseteq C$, $\forall x \in A \setminus C(|\{H(x) : H \in \mathrm{fix}_{\mathscr{G}}(C)\}| > k)$ and $|\{H[Y] : H \in \mathrm{fix}_{\mathscr{G}}(C)\}| = k$. (Choose A_n $(n \geq 1)$ such that $B \subseteq A_n$, and let $C := A_n$. Let $k := k_n + k_n$ and $Y := \{(n+1, \zeta, i) \in A_{n+1} : i \text{ is even}\}$. Then Y has exactly two images under $\{h : h \in \mathrm{fix}_{\mathscr{G}}(C)\}$ and $\forall x \in A \setminus C(|\{h(x) : h \in \mathrm{fix}_{\mathscr{G}}(C)\}| \geq k_{n+1} + k_{n+1})$.)*

Now the function

$$\Psi\colon \operatorname{seq}(A) \to \operatorname{fin}(A)$$
$$\zeta \mapsto \{x\colon \zeta_x = \zeta\}$$

is a 1-1 function in $\mathscr{B}$ from $\operatorname{seq}(A)$ into $\operatorname{fin}(A)$ (by Facts 1 and 2). Hence, (a) holds in $\mathscr{B}$.

To prove (b) assume there is a 1-1 function $\Phi \in \mathscr{B}$ from $\operatorname{fin}(A)$ into $\operatorname{seq}(A)$. Let B be a support of Φ, and let C, Y, k be as in Fact 3.

If the sequence $\Phi(Y)$ belongs to $\operatorname{seq}(C)$, then for some $H \in \operatorname{fix}_{\mathscr{G}}(C)$, $H[Y] \neq Y$; hence, $\Phi(H[Y]) \neq \Phi(Y)$. But this contradicts the fact that H maps Φ to itself (by definition of C, Y, and H).

Otherwise, there exists an $m \in \omega$ such that $x := \Phi(Y)(m)$ does not belong to the set C.

Hence, $|\{H(x)\colon H \in \operatorname{fix}_{\mathscr{G}}(C)\}| > k$ and $|\{H[Y]\colon H \in \operatorname{fix}_{\mathscr{G}}(C)\}| = k$ (by Fact 3). Every $H \in \operatorname{fix}_{\mathscr{G}}(C)$ maps Φ to itself and, hence, $\Phi(Y)$ to $\Phi(H[Y])$. So we have a mapping from a set with k members onto a set with more than k members. But this is a contradiction. □

§2. **ZF** $\vdash (|\operatorname{fin}(S)| < |\mathscr{P}(S)|)$ **for any infinite set** S.

THEOREM 3. $ZF \vdash \operatorname{fin}(\mathscr{C}) < \mathscr{P}(\mathscr{C})$.

PROOF. Take $S \in \mathscr{C}$. The natural map from $\operatorname{fin}(S)$ into $\mathscr{P}(S)$ is a 1-1 function; hence, $|\operatorname{fin}(S)| \leq |\mathscr{P}(S)|$ is always true.

Assume that there is a bijective function $B\colon \operatorname{fin}(S) \to \mathscr{P}(S)$. Then given any ordinal α, we can construct an α-sequence$^{1\text{-}1}$ in $\operatorname{fin}(S)$. But this contradicts Hartogs's Theorem.

First, we construct an ω-sequence$^{1\text{-}1}$ in $\operatorname{fin}(S)$ as follows: $S \in \mathscr{P}(S)$ and because S is infinite, $S \notin \operatorname{fin}(S)$. But $B^{-1}(S) \in \operatorname{fin}(S)$. So put $s_0 := B^{-1}(S)$ and $s_{n+1} := B^{-1}(s_n)$ $(n \notin \omega)$. Then the set $\{s_i : i < \omega\}$ is an infinite set of finite subsets of S, and the sequence $\langle s_0, s_1, \ldots, s_n, \ldots\rangle_\omega$ is an ω-sequence$^{1\text{-}1}$ in $\operatorname{fin}(S)$.

If we have already constructed an α-sequence$^{1\text{-}1}$ $\langle s_0, s_1, \ldots, s_\beta, \ldots\rangle_\alpha$ in $\operatorname{fin}(S)$ (with $\alpha \geq \omega$), then we define an equivalence relation on S by

$$x \sim y \quad \text{iff} \quad \forall \beta < \alpha (x \in s_\beta \Leftrightarrow y \in s_\beta).$$

Take $x \in S$ and, suppose that $\mu < \alpha$. Define

$$D_{x,\mu} := \bigcap_{i<\mu} \{s_i\colon x \in s_i\},$$
$$g(x) := \{\mu < \alpha\colon x \in s_\mu \wedge (s_\mu \cap D_{x,\mu} \neq D_{x,\mu})\}.$$

FACT. *Given* $x, y \in S$, $g(x) = g(y) \Leftrightarrow x \sim y$. *(In other words,* $x^\sim = y^\sim$ *whenever* $g(x) = g(y)$.*) Hence, there is a bijection between* $\{x^\sim : x \in S\}$ *and* $\{g(x)\colon x \in S\}$. *Furthermore,* $g(x) \in \operatorname{fin}(\alpha)$.

Since $\{g(x)\colon x \in S\} \subseteq \operatorname{fin}(\alpha)$, apply F^α_{fin} to obtain $F^\alpha_{\text{fin}}[\{g(x)\colon x \in S\}] \subseteq \alpha$. Let γ be the order-type of $F^\alpha_{\text{fin}}[\{g(x)\colon x \in S\}]$. Then $\gamma \leq \alpha$ and for each $g(x)$ we obtain an ordinal number $\eta(g(x)) < \gamma$.

Each s_ι ($\iota < \alpha$) is the union of at most finitely many equivalence classes. Thus, there is a 1-1 function

$$h\colon \alpha \to \operatorname{fin}(\gamma)$$
$$\iota \mapsto \{\xi\colon \eta(g(x)) = \xi \wedge x \in s_\iota\}.$$

Since $F^\gamma_{\operatorname{fin}}$ is a bijection between $\operatorname{fin}(\gamma)$ and γ, $F^\gamma_{\operatorname{fin}} \circ h$ is a 1-1 function from α into γ, and because $\gamma \leq \alpha$, we also have a 1-1 function from γ into α.

The Cantor-Berstein Theorem yields a bijection between γ and α and, hence, a bijection G from $\{\eta(g(x))\colon x \in S\}$ onto $\{s_\iota : \iota < \alpha\}$.

Now consider the function $\Gamma\colon B \circ G \circ \eta \circ g$ from S into $\mathscr{P}(S)$:

$$\Gamma\colon S \xrightarrow{g} \{g(x)\colon x \in S\} \xrightarrow{\eta} \{\eta(g(x))\colon x \in S\} \xrightarrow{G} \{s_\iota\colon i < \alpha\} \xrightarrow{B} \mathscr{P}(S).$$

FACT. $S_\alpha := \{x \in S\colon x \notin \Gamma(x)\} \notin \{B(s_\iota)\colon i < \alpha\}$.

Proof. Otherwise, take $S_\alpha = B(s_\beta)$ (for some $\beta < \alpha$). We identify each $x^\sim$ with $g(x)$ using the bijection above. Then there is a $g(x)$ such that $G \circ \eta((g(x)) = s_\beta$. Now if $y \in x^\sim$, then $\Gamma(y) = S_\alpha$. But $y \in S_\alpha \Leftrightarrow y \notin \Gamma(y) \Leftrightarrow y \notin S_\alpha$, which is a contradiction.

But $S_\alpha \subseteq S$ and $B^{-1}(S_\alpha) =: s_\alpha \in \operatorname{fin}(S)$ with $s_\alpha \notin \{s_\iota\colon \iota < \alpha\}$, and we have an $(\alpha + 1)$-sequence$^{1\text{-}1}$ in $\operatorname{fin}(S)$; namely, $\langle s_0, s_1, \ldots, s_\beta, \ldots, s_\alpha\rangle_{\alpha+1}$. We now see that for an infinite set S there is no bijection between $\operatorname{fin}(S)$ and $\mathscr{P}(S)$, and this completes the proof.

We note the following *facts*.

Given a natural number n, $\mathbf{ZF} \vdash (n \times \operatorname{fin}(\mathscr{C}) = \mathscr{P}(\mathscr{C}) \to n = 2^k$ for a $k \in \omega)$.

Moreover, for each $k \in \omega$, $\operatorname{Con}(\mathrm{ZF}) \Rightarrow \operatorname{Con}(\mathrm{ZF} + \exists \mathscr{C}(2^k \times \operatorname{fin}(\mathscr{C}) = \mathscr{P}(\mathscr{C}))$. (If $k = 0$, then this is obvious for finite cardinals.)

Sketch of the proof of the facts. For the consistency result, consider the permutation model with an infinite set of atoms A and the empty relation. Then the automorphism group is the complete permutation group. It is not hard to see that any subset of A in this model is either finite or has a finite complement. Take a natural number k, and consider (in this model) the set $k \times A$. The cardinality of the set $\mathscr{P}(k \times A)$ is the same as that of the set $2^k \times \operatorname{fin}(A)$.

To prove the other fact, assume that n is a natural number which is not a power of 2 and that for some infinite set S there is a bijection B between $n \times \operatorname{fin}(S)$ and $\mathscr{P}(S)$. Use the function B to construct an ω-sequence$^{1\text{-}1}$ in $\operatorname{fin}(S)$. Then, using Theorem 3, $\omega \leq \operatorname{fin}(S) < \mathscr{P}(S)$ and it is easy to see that $n \times \operatorname{fin}(S) \leq \operatorname{fin}(S) \times \operatorname{fin}(S) =: \operatorname{fin}(S)^2$. Then $\omega < \mathscr{P}(S) = n \times \operatorname{fin}(S) \leq \operatorname{fin}(S)^2$ contradicts the fact that if $\aleph_0 \leq \mathscr{P}(\mathscr{C})$, then for any natural number n, $\mathscr{P}(\mathscr{C}) \not\leq \operatorname{fin}(\mathscr{C})^n$. (Here $\aleph_0$ denotes the cardinality of ω.) The proof of this fact is similar to the proof of Theorem 3. □

§3. $\operatorname{seq}^{1\text{-}1}(S)$, $\operatorname{seq}(S)$, and $\mathscr{P}(S)$ when S is an arbitrary set.

We show that $\mathbf{ZF} \vdash \operatorname{seq}^{1\text{-}1}(\mathscr{C}) \neq \mathscr{P}(\mathscr{C})$ for every cardinal $\mathscr{C} \geq 2$. But we first need the following result.

LEMMA. $ZF \vdash \aleph_0 \leq \mathscr{P}(\mathscr{C}) \to \mathscr{P}(\mathscr{C}) \not\leq \operatorname{seq}^{1\text{-}1}(\mathscr{C})$.

PROOF. Take $S \in \mathscr{C}$. Then because $\aleph_0 \leq \mathscr{P}(\mathscr{C})$, we have a 1-1 function $f_\omega\colon \omega \to \mathscr{P}(S)$.

Assume that there is a 1-1 function $J: \mathscr{P}(S) \to \mathrm{seq}^{1\text{-}1}(S)$. Then $J \circ f_\omega: \omega \to \mathrm{seq}^{1\text{-}1}(S)$ is also 1-1, and we get an ω-sequence$^{1\text{-}1}$ in $\mathrm{seq}^{1\text{-}1}(S)$. Using this ω-sequence$^{1\text{-}1}$ in $\mathrm{seq}^{1\text{-}1}$ in S we can easily construct an ω-sequence$^{1\text{-}1}$ in S. If we already have constructed an α-sequence$^{1\text{-}1}\langle s_0, s_1, \ldots, s_\beta, \ldots\rangle_\alpha$ $(\alpha \geq \omega)$ in S, put $T := \{s_\iota : \iota < \alpha\}$. This gives rise to bijective functions,

$$h_0: T \to \alpha,$$
$$h_1: \mathrm{seq}^{1\text{-}1}(\alpha) \to \mathrm{seq}^{1\text{-}1}(T).$$

Let J^{-1} be the inverse of J, and denote the inverse of F^α_{seq} by $\mathrm{inv}F^\alpha_{\mathrm{seq}}$. Further, define

$$\Gamma := J^{-1} \circ h_1 \circ \mathrm{inv}F^\alpha_{\mathrm{seq}} \circ h_0.$$

Note. $\mathrm{dom}(\Gamma) \subseteq T$ and $\mathrm{range}(\Gamma) \subseteq \mathscr{P}(S)$ (because J is 1-1). □

FACT. $S_\alpha := \{x \in S : x \notin \Gamma(x)\} \notin J^{-1}[\mathrm{seq}^{1\text{-}1}(T)]$.

Proof. Assume not; then $x \in S$ such that $J(S_\alpha) = h_1 \circ \mathrm{inv}F^\alpha_{\mathrm{seq}} \circ h_0(x)$ yields a contradiction. Because $J(S_\alpha) \notin \mathrm{seq}^{1\text{-}1}(T)$, the sequence $J(S_\alpha)$ has a first element which is not in T, say s_α. Finally, the sequence $\langle s_0, s_1, \ldots, s_\alpha\rangle_{\alpha+1}$ is an $(\alpha + 1)$-sequence$^{1\text{-}1}$ in S. So the existence of a 1-1 function $J: \mathscr{P}(S) \to \mathrm{seq}^{1\text{-}1}(S)$ contradicts Hartogs's Theorem.

THEOREM 4. *If $\mathscr{C} \geq 2$ is any cardinal, then $ZF \vdash (\mathrm{seq}^{1\text{-}1}(\mathscr{C}) \neq \mathscr{P}(C))$.*

PROOF. By the lemma it is enough to prove that if $\mathscr{C} \geq 2$, then $\mathrm{seq}^{1\text{-}1}(\mathscr{C}) = \mathscr{P}(\mathscr{C}) \Rightarrow \aleph_0 \leq \mathscr{C}$. For finite cardinals $\mathscr{C} \geq 2$ the statement is obvious. So let $S \in \mathscr{C}$ be an infinite set, and assume that there is a bijective function

$$B: \mathrm{seq}^{1\text{-}1}(S) \to \mathscr{P}(S).$$

We use this function to construct an ω-sequence$^{1\text{-}1}$ in S. Let $n^\star$ $(n < \omega)$ be the cardinality of $\mathrm{seq}^{1\text{-}1}(n)$.

Then $0^\star = 1$, $1^\star = 2$, $2^\star = 5, \ldots, 16^\star = 56\,874\,039\,553\,217, \ldots$ (see [Sl, no. 589]), and in general,

$$n^\star = \sum_{i=0}^{n} \frac{n!}{i!}.$$

We begin by choosing four distinct elements of S, $S_4 := \{s_0, s_1, s_2, s_3\}$ and then use these elements to construct a 4-sequence$^{1\text{-}1}\langle s_0, s_1, s_2, s_3\rangle_4$ in S. This sequence will give us an order on the set $\mathrm{seq}^{1\text{-}1}(S_4)$ (e.g., we order $\mathrm{seq}^{1\text{-}1}(S_4)$ by length and lexicographically).

If we have already constructed an n-sequence$^{1\text{-}1}\langle s_0, s_1, \ldots, s_{n-1}\rangle_n$ in S $(n \geq 4)$, put $S_n := \{s_i : i < n\}$. Then $B[\mathrm{seq}^{1\text{-}1}(S_n)] \subseteq \mathscr{P}(S)$ has cardinality $n^\star$.

We now define an equivalence relation on S by

$$x \sim y \quad \text{iff} \quad \forall q \in \mathrm{seq}^{1\text{-}1}(S_n)(x \in B(q) \Leftrightarrow y \in B(q)).$$

It is easy to see that for each $q \in \mathrm{seq}^{1\text{-}1}(S_n)$

(1) $B(q)$ is the *disjoint union* of *less* than $n^\star$ equivalence classes.

Take the above order on $\mathrm{seq}^{1\text{-}1}(S_n)$. This induces an order on the set of equivalence classes $\mathrm{eq} := \{x^\sim : x \in S\}$ and also an order on $\mathscr{P}(\mathrm{eq})$.

If there is a first $r \in \mathscr{P}(\mathrm{eq})$ such that $r \notin B[\mathrm{seq}^{1\text{-}1}(S_n)]$, then $q_r := B^{-1}(r)$ is a "new" sequence in S. This is $q_r \notin \mathrm{seq}^{1\text{-}1}(S_n)$, and we choose the first element s_n of q_r which is not in S_n. Hence, the sequence $\langle s_0, s_1, \ldots, s_n\rangle_{n+1}$ is now an $(n+1)$-sequence$^{1\text{-}1}$ in S.

If there is an $s_i \in S_n$ such that $\{s_i\} \notin B[\mathrm{seq}^{1\text{-}1}(S_n)]$, then use $B(\{s_i\})$ to construct an $(n+1)$-sequence$^{1\text{-}1}$ in S.

Otherwise, our construction stops at S_n and we write $\mathrm{stop}(S_n)$. Our construction only stops if

for each $s_i \in S_n$, $\{s_i\} \in \mathrm{eq}$

and

for each $r \in \mathscr{P}(\mathrm{eq})$, there is a $q_r \in \mathrm{seq}^{1\text{-}1}(S_n)$ such that $B(q_r) = r$.

If κ ($\kappa < \omega$) is the cardinality of eq, then 2^κ is the cardinality of $\mathscr{P}(\mathrm{eq})$, and because of (1), we have $\mathrm{stop}(S_n) \Rightarrow 2^\kappa = n^\star$.

It is known that $0^\star = 1 = 2^0$, $1^\star = 2 = 2^1$, $3^\star = 16 = 2^4$, and if $n^\star$ is a power of 2 for some $n > 3$, then n has to be bigger than 10^8.

If there are only finitely many k, $n < \omega$ such that $2^k = n^\star$, then there is a least n_0 such that $2^k = n_0^\star$ and $\forall n > n_0(\neg\mathrm{stop}(S_n))$.

Refining our construction removes the need for this strong arithmetic condition.

Assume $\mathrm{stop}(S_n)$. If $x \notin S_n$, then let $S^x_{n+1} := S_n \cup \{x\}$, and let $S^x_{n+k} := S^x_{n+1} \cup \{Y\}$ with Y of cardinality $k-1$. Because (n is even)$\Rightarrow$ ($n^\star$ is odd) and $\mathrm{stop}(S_n)$, we cannot have $\mathrm{stop}(S^x_{n+1})$ for any $x \notin S_n$.

Now we recommence our construction with the set S^x_{n+1} and construct an $(n+k)$-sequence$^{1\text{-}1}$ $\langle s_0, s_1, \ldots, s_{n+k-1}\rangle_{n+k}$ ($k \geq 2$) in S. If the construction also stops at the $(n+\mathrm{stop})$th stage at the set $S^x_{n+\mathrm{stop}}$ ($\mathrm{stop} \geq 2$), then we write S^x instead of $S^x_{n+\mathrm{stop}}$).

If there is an $x \in S$ such that S^x is infinite, then our construction does not stop when we recommence with S^x_{n+1}, and we can construct an ω- sequence$^{1\text{-}1}$ in S. But this contradicts our Lemma. Thus, there cannot be such an x, and each $x \in S$ is in exactly one *finite* set S^x. If for each $x \in S$, S^x is the union of some elements of eq, then S must be finite because eq is finite. But this contradicts our assumption that S is infinite.

A subset of S is called *good* if it cannot be written as the union of elements of eq.

Consider the set $T_{\min} := \{x : S^x$ is good and of least cardinality$\}$, and let m_T be the cardinality of S^x for some x in $T_{\min}$. Further for $x \in T_{\min}$ let $x_= := \{y : S^y = S^x\}$ (the elements of S^x that we cannot distinguish), and let $m_=$ denote the least cardinality of the sets $x_=$.

If $T_{\min}$ is good, use $B^{-1}(T_{\min})$ to construct an $(n+1)$-sequence$^{1\text{-}1}$ in S. Otherwise, take $x \in T_{\min}$. Because S^x is good we, have

$$B^{-1}(S^x) \notin \mathrm{seq}^{1\text{-}1}(S_n).$$

Thus, there is a first y in $B^{-1}(S^x)$ which is not in S_n. It is easy to see that $S^y \subseteq S^x$, and if $S^y \neq S^x$ then S^y is not good (because $x \in T_{\min}$). But then $B^{-1}(S^x \setminus S^y) \notin \mathrm{seq}^{1\text{-}1}(S^y)$, and we may proceed. So for each $x \in T_{\min}$ construct an m_T-sequence $^{1\text{-}1}$ SEQ^x in S such that

$$S^x = S^y \Rightarrow \mathrm{SEQ}^x = \mathrm{SEQ}^y.$$

For $i < m_T$ define

$$Q_i = \{s \in S\colon s \text{ is the } i\text{th element in } \mathrm{SEQ}^x \text{ for some } x \in S\}.$$

Assume there is some $j < m_T$ such that Q_j is good. Then $B^{-1}(Q_j) \notin \mathrm{seq}^{1\text{-}1}(S_n)$. But $B^{-1}(Q_j) \notin \mathrm{seq}^{1\text{-}1}(S)$ and we get an $(n+1)$-sequence$^{1\text{-}1}$ in S.

It remains to justify our assumption. Note that if for some $i \neq j$, $z \in Q_i \cap Q_j$, then S^z cannot be good. Furthermore, for each $x \in T_{\min}$ there is exactly one i_x such that $x \in Q_{i_x}$ and if $z, y \in x_=$, $z \neq y$, then $i_x \neq i_y$. If there are no good Q_i's, $m_=$ cannot exceed κ (the cardinality of eq). But by the following this is a contradiction.

> An easy calculation modulo 2^r $(r \leq 4)$ shows that for each n, if $2^r | n^\star$, then $2^r | (n+2^r)^\star$ and $2^r \nmid (n+t)^\star$ if $0 < t < 2^r$.

Assume there is a smallest k $(k \geq 4)$ such that $2^{k+1} | n^\star$ and $2^{k+1} | (n+t)^\star$ for some t with $0 < t < 2^{k+1}$. Then because $2^k | 2^{k+1}$, we have $2^k | n^\star$ and $2^k | (n+t)^\star$. Since k is by definition the smallest such number, we know that t must be 2^k.

$$\begin{aligned}
(n+2^k)^\star = \textstyle\sum_{i=0}^{n+2^k} \frac{(n+2^k)!}{i!} = 1 \cdot 2 \cdots 2^k \cdot (2^k+1) \cdots & \qquad (2^k+n) \quad (1)\\
+2 \cdots 2^k \cdots \qquad \cdots & \qquad (2^k+n) \quad (2)\\
\ddots & \qquad \vdots\\
+2^k \cdots \qquad \cdots & \qquad (2^k+n) \quad (2^k)\\
\ddots & \qquad \vdots\\
& \qquad +(2^k+n) \quad (2^k+n)\\
& \qquad +1 \quad (2^k+n+1)
\end{aligned}$$

It is easy to see that 2^{k+1} divides lines (1)–(2^k) since $k \geq 2$ and $n \geq 2$. If we calculate the products of lines (2^k+1)–(2^k+n+1), then we only have to consider sums which are not obviously divisible by 2^{k+1}. So for a suitable natural number ε we have

$$(n+2^k)^\star = 2^k \cdot \left(\sum_{j=0}^{n-1} \sum_{i>j}^{n} \frac{n!}{i \cdot j!} \right) + n^\star + 2^{k+1} \cdot \varepsilon. \tag{2}$$

We know that $2^{k+1} | n^\star$ with $n \geq 3$, $k \geq 4$. And because $n^\star$ is even, n has to be odd. If j is $n-1$, $n-2$, or $n-3$, then $\sum_{i>j}^{n} \frac{n!}{i \cdot j!}$ is odd. Moreover, if $0 \leq j \leq (n-4)$, then $\sum_{i>j}^{n} \frac{n!}{i \cdot j!}$ is even. So $\sum_{j=0}^{n-1} \sum_{i>j}^{n} \frac{n!}{i \cdot j!}$ is odd. Hence, $2^{k+1} \nmid (n+2^k)^\star$ (by (2) and $2^{k+1} | n^\star$). We return to the proof.

(**) We know that if $2^k = n^\star$ and $(n+t)^\star$ is a power of 2, then 2^k divides t.

Take $x \in T_{\min}$ such that $|x_=| = m_=$. If $y \in S^x$, then

(i) $|S^y| = n + t_y$ with 2^κ divides t_y,

(ii) either $y \in x_=$ or S^y is not good.

This is because $2^\kappa = n^\star$ and (**).

Hence (for a suitable natural number ε), $m_T = |S^x| = n + 2^\kappa \cdot \varepsilon + m_=$ (by (ii)), and 2^κ divides $m_=$ (by (i)). But this implies that $m_=$ must be larger than κ, which justifies our assumption. □

The statement obtained when $\mathrm{seq}^{1\text{-}1}$ is replaced by seq is much easier to prove.

THEOREM 5. *$ZF \vdash \mathrm{seq}(\mathscr{C}) \neq \mathscr{P}(\mathscr{C})$ for all cardinals such that $\phi \neq \mathscr{C}$.*

PROOF. Take $S \in \mathscr{C}$. First, note the fact that if $\aleph_0 \leq \mathscr{C}$, then $\mathrm{seq}(\mathscr{C}) \not\geq \mathscr{P}(\mathscr{C})$. (The proof is the same as the proof of the Lemma except that we can skip the first lines of the proof of the Lemma.)

Assume there is a bijection B from $\mathrm{seq}(S)$ onto $\mathscr{P}(S)$. Choose an $s_0 \in S$, and define a 1-1 function f_{s_0} from ω into $\mathscr{P}(S)$ by $i \mapsto \xi_i := B(\langle s_0, s_0, \ldots, s_0\rangle)$ (i-times). Use the ξ_i's to construct pairwise disjoint subsets $c_i \subseteq S$ $(i < \omega)$.

Given an n-sequence$^{1\text{-}1}$ $\langle s_0, s_1, \ldots, s_{n-1}\rangle_n$ in S, let $S_n := \{s_i : i < n\}$ and the natural order on S_n induce a well-ordering on the set $\mathrm{seq}(S_n)$ with order type ω. Then there is a bijection $h : \omega \to \mathrm{seq}(S_n)$. Now the function $\Gamma := B \circ h$ is a 1-1 function from ω into $\mathscr{P}(S)$ with $t := \bigcup\{c_i : c_i \subseteq \Gamma(i)\} \notin \{\Gamma(k) : k \in \omega\}$. Hence, $B^{-1}(t)$ is a sequence in S which does not belong to S_n. Choose $s_n \in S$ to be the first element of $B^{-1}(t)$ not in S_n. Then $\langle s_0, s_1, \ldots, s_n\rangle_{n+1}$ is an $(n+1)$-sequence$^{1\text{-}1}$ in the set S.

We thus construct an ω-sequence$^{1\text{-}1}$ in S, contradicting the previous fact. □

REFERENCES

[Ba] H. BACHMANN, ***Transfinite Zahlen***, Springer-Verlag, Berlin, 1967.

[Je1] TH. JECH, ***Set theory***, Academic Press, New York, 1978.

[Je2] ———, ***The axiom of choice***, North-Holland, Amsterdam, 1973.

[La] H. LÄUCHLI, *Auswahlaxiom in der Algebra*, ***Commentarii Mathematici Helvetiei***, vol. 37 (1962), pp. 1–18.

[Sl] N. J. A. SLOANE, ***A handbook of integer sequence***, Academic Press, New York, 1973.

[Sp1] E. SPECKER, *Verallgemeinerte Kontinuumshypothese und Auswahlaxiom*, ***Archiv der Mathematik***, vol. 5 (1954), pp. 332–337.

[Sp2] ———, *Zur Axiomatik der Mengenlehre*, ***Zeitschrift für Mathematische Logik und Grundlagen der Mathematik***, vol. 3 (1957), pp. 173–210.

DEPARTMENT OF MATHEMATICS
ELDGEN. TECHNISCHE HOCHSCHULE
ZÜRICH. SWITZERLAND

E-mail: halbeisen@math.ethz.ch

INSTITUTE OF MATHEMATICS
HEBREW UNIVERSITY JERUSALEM
JERUSALEM. ISRAEL

E-mail: shelah@math.huji.ac.il