On the Cardinality of Infinite Symmetric Groups in ZF

Guozhen Shen

University of Chinese Academy of Sciences

April 6, 2018
Fudan Logic Seminar
Fudan University

Preliminaries

Convention

Let $\varphi(p_1, \ldots, p_m, x_0, \ldots, x_n)$ and $\psi(p_1, \ldots, p_m, x_0, \ldots, x_n, y)$ be formulas in the language of set theory with no free variables other than indicated. When we say that *from* $x_0, \ldots, x_n$ *such that* $\varphi(p_1, \ldots, p_m, x_0, \ldots, x_n)$, *one can explicitly define a* y *such that* $\psi(p_1, \ldots, p_m, x_0, \ldots, x_n, y)$, we mean the following:

> *There exists a class function* G *without free variables such that if* $\varphi(p_1, \ldots, p_m, x_0, \ldots, x_n)$, *then* $(x_0, \ldots, x_n)$ *is in the domain of* G *and* $\psi(p_1, \ldots, p_m, x_0, \ldots, x_n, G(x_0, \ldots, x_n))$.

Preliminaries

Examples

- From a surjection $f\colon y \twoheadrightarrow x$ and a well-ordering r of y, one can explicitly define a well-ordering s of x.

  > *There exists a class function G without free variables such that if f is a surjection from y onto x and r well-orders y, then $G(f, r)$ is defined and is a well-ordering of x.*

- (Cantor-Bernstein) From an injection $f\colon x \rightarrowtail y$ and an injection $g : y \rightarrowtail x$, one can explicitly define a bijection $h : x \twoheadrightarrow y$.

  > *There exists a class function G without free variables such that if f is an injection from x into y and g is an injection from y into x, then $G(f, g)$ is defined and is a bijection from x onto y.*

Preliminaries

Project

Restate all theorems of ZFC in this form!

Preliminaries

Project

Restate all theorems of ZFC in this form!

Further examples

- (Zermelo 1904) From a choice function on $\wp(x)$, one can explicitly define a well-ordering on x.
- (Aronszajn 1934) From a ladder system $\langle C_\alpha \mid \alpha < \omega_1 \rangle$, one can explicitly define a Aronszajn tree.
- (Jensen 1968) From a $\diamondsuit$-sequence $\langle S_\alpha \mid \alpha < \omega_1 \rangle$ and a ladder system $\langle C_\alpha \mid \alpha < \omega_1 \rangle$, one can explicitly define a Souslin tree.

Preliminaries

Definition of cardinality in ZF

$$|x| = \begin{cases} \min\{\alpha \mid \alpha \approx x\}, & \text{if } x \text{ is well-orderable;} \\ \{y \mid y \approx x \wedge \forall z \approx x(\mathrm{rank}(y) \leqslant \mathrm{rank}(z))\}, & \text{otherwise.} \end{cases}$$

We shall use lower case German letters $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$ for cardinals.

Preliminaries

Definition

- $|x| + |y| = |x \times \{0\} \cup y \times \{1\}|$
- $|x| \cdot |y| = |x \times y|$
- $|y|^{|x|} = |\{f \mid f\colon x \to y\}|$

Preliminaries

Definition

- $x \preccurlyeq y$ means that there is an injection from x into y.
- $x \preccurlyeq^* y$ means that there is a surjection from a subset of y onto x.
- $\mathfrak{a} \leqslant \mathfrak{b}$ means that there are sets x, y such that $|x| = \mathfrak{a}$, $|y| = \mathfrak{b}$, and $x \preccurlyeq y$.
- $\mathfrak{a} \leqslant^* \mathfrak{b}$ means that there are sets x, y such that $|x| = \mathfrak{a}$, $|y| = \mathfrak{b}$, and $x \preccurlyeq^* y$.

Fact

$\mathfrak{a} \leqslant \mathfrak{b} \to \mathfrak{a} \leqslant^* \mathfrak{b} \to 2^{\mathfrak{a}} \leqslant 2^{\mathfrak{b}}$.

Preliminaries

Definition

- x is Dedekind infinite if $\omega \preccurlyeq x$; otherwise x is Dedekind finite.
- x is power Dedekind infinite if $\omega \preccurlyeq \wp(x)$; otherwise x is power Dedekind finite.
- $\mathfrak{a}$ is Dedekind infinite if $\aleph_0 \leqslant \mathfrak{a}$; otherwise $\mathfrak{a}$ is Dedekind finite.
- $\mathfrak{a}$ is power Dedekind infinite if $\aleph_0 \leqslant 2^{\mathfrak{a}}$; otherwise $\mathfrak{a}$ is power Dedekind finite.

Preliminaries

Fact

- $\mathfrak{a}$ is Dedekind infinite $\rightarrow$ $\mathfrak{a}$ is power Dedekind infinite $\rightarrow$ $\mathfrak{a}$ is infinite
- ZF $\nvdash$ $\mathfrak{a}$ is infinite $\rightarrow$ $\mathfrak{a}$ is power Dedekind infinite
- ZF $\nvdash$ $\mathfrak{a}$ is power Dedekind infinite $\rightarrow$ $\mathfrak{a}$ is Dedekind infinite
- (Dedekind 1888) $\mathfrak{a}$ is Dedekind infinite $\leftrightarrow$ $\mathfrak{a} + 1 = \mathfrak{a}$
- The class of all Dedekind finite sets is closed under disjoint unions.
- $\mathfrak{a}$ is infinite $\rightarrow$ $2^{\mathfrak{a}}$ is power Dedekind infinite

Preliminaries

Theorem (Kuratowski 1920s)

$\mathfrak{a}$ *is power Dedekind infinite* $\leftrightarrow \aleph_0 \leqslant^* \mathfrak{a} \leftrightarrow 2^{\aleph_0} \leqslant 2^{\mathfrak{a}}$

Preliminaries

Theorem (Kuratowski 1920s)

$\mathfrak{a}$ *is power Dedekind infinite* $\leftrightarrow \aleph_0 \leqslant^* \mathfrak{a} \leftrightarrow 2^{\aleph_0} \leqslant 2^{\mathfrak{a}}$

Proof.

- From an infinite subset x of $\wp(\omega)$, one can explicitly define an infinite proper subset y of x.
- From an infinite subset x of $\wp(\omega)$, one can explicitly define a surjection $f\colon x \twoheadrightarrow \omega$.
- From an injection $f\colon \omega \to \wp(x)$, one can explicitly define a surjection $f\colon x \twoheadrightarrow \omega$.

□

Preliminaries

Theorem (Kuratowski 1920s)

$\mathfrak{a}$ *is power Dedekind infinite* $\leftrightarrow \aleph_0 \leqslant^* \mathfrak{a} \leftrightarrow 2^{\aleph_0} \leqslant 2^{\mathfrak{a}}$

Corollary

The class of all power Dedekind finite sets is closed under unions.

Factorials of Cardinals

Definition

- $\mathcal{S}(x) = \{f \mid f \text{ is a permutation on } x\}$
- $\mathfrak{a}! = |\mathcal{S}(x)| \quad \text{where } |x| = \mathfrak{a}$
- $[x]^n = \{y \subseteq x \mid |y| = n\}$
- $[\mathfrak{a}]^n = |[x]^n| \quad \text{where } |x| = \mathfrak{a}$

Factorials of Cardinals

Definition

- $\mathcal{S}(x) = \{f \mid f \text{ is a permutation on } x\}$
- $\mathfrak{a}! = |\mathcal{S}(x)| \quad \text{where } |x| = \mathfrak{a}$
- $[x]^n = \{y \subseteq x \mid |y| = n\}$
- $[\mathfrak{a}]^n = |[x]^n| \quad \text{where } |x| = \mathfrak{a}$

Fact

- $\mathfrak{a}$ is power Dedekind finite $\to$ $\mathfrak{a}!$ is Dedekind finite
- (Bernstein 1905, Schönflies 1913) $\mathfrak{a} = 2\mathfrak{b} \to 2^{\mathfrak{b}} \leqslant \mathfrak{a}!$
- $[\mathfrak{a}]^2 \leqslant \mathfrak{a}!$

Factorials of Cardinals

Fact

- $\mathfrak{a}$ is power Dedekind finite $\to$ $\mathfrak{a}!$ is Dedekind finite
- (Bernstein 1905, Schönflies 1913) $\mathfrak{a} = 2\mathfrak{b} \to 2^{\mathfrak{b}} \leqslant \mathfrak{a}!$
- $[\mathfrak{a}]^2 \leqslant \mathfrak{a}!$

Theorem (Dawson and Howard 1976)

$\mathfrak{a} \geqslant 3 \to \mathfrak{a} < \mathfrak{a}!$

Factorials of Cardinals

Fact

- $\mathfrak{a}$ is power Dedekind finite $\to$ $\mathfrak{a}!$ is Dedekind finite
- (Bernstein 1905, Schönflies 1913) $\mathfrak{a} = 2\mathfrak{b} \to 2^{\mathfrak{b}} \leqslant \mathfrak{a}!$
- $[\mathfrak{a}]^2 \leqslant \mathfrak{a}!$

Theorem (Dawson and Howard 1976)

$\mathfrak{a} \geqslant 3 \to \mathfrak{a} < \mathfrak{a}!$

Proof.

- If $\mathfrak{a} < [\mathfrak{a}]^2$, then $\mathfrak{a} < [\mathfrak{a}]^2 \leqslant \mathfrak{a}!$
- Let $\mathfrak{a} = [\mathfrak{a}]^2$. The case $\mathfrak{a} = 3$ is trivial. Otherwise $\mathfrak{a}$ is infinite. Since $\mathfrak{a} \leqslant 2\mathfrak{a} \leqslant [\mathfrak{a}]^2$, we have $\mathfrak{a} = 2\mathfrak{a}$, and hence $\mathfrak{a} < 2^{\mathfrak{a}} \leqslant \mathfrak{a}!$

□

Factorials of Cardinals

Theorem (Dawson and Howard 1976)

$\mathfrak{a} \geqslant 3 \to \mathfrak{a} < \mathfrak{a}!$

Question

$\mathsf{ZF} \vdash [\mathfrak{a}]^2 < \mathfrak{a}!$?

Factorials of Cardinals

Theorem (Dawson and Howard 1976)

$\mathfrak{a} \geqslant 3 \to \mathfrak{a} < \mathfrak{a}!$

Question

$\mathsf{ZF} \vdash [\mathfrak{a}]^2 < \mathfrak{a}!$?

Theorem

$[\mathfrak{a}]^2 < \mathfrak{a}!$

Factorials of Cardinals

Theorem

$[\mathfrak{a}]^2 < \mathfrak{a}!$

Proof.

- (Specker 1954) From an infinite ordinal α, one can explicitly define an injection $f\colon \alpha \times \alpha \to \alpha$.
- From an injection $f\colon \alpha \to [x]^2$, where α is an infinite ordinal, one can explicitly define a 2-to-1 surjection g from a subset of x onto α.
- From a 2-to-1 function f from a subset of x into $\mathcal{S}(x)$, one can explicitly define a $u \in \mathcal{S}(x) - \mathrm{ran}(f)$.
- From an injection f from a subset of $\mathcal{S}(x)$ into $[x]^2$ and an injection $g : \omega \to \mathcal{S}(x)$, one can explicitly define a $u \in \mathcal{S}(x) - \mathrm{dom}(f)$.

□

Factorials of Cardinals

Theorem

$[\mathfrak{a}]^2 < \mathfrak{a}!$

Question

- $\mathsf{ZF} \vdash \mathfrak{a}$ is infinite $\rightarrow \mathfrak{a}! \not\leq [\mathfrak{a}]^3$?
- $\mathsf{ZF} \vdash \mathfrak{a}$ is infinite $\rightarrow \mathfrak{a}! \not\leq^* \mathfrak{a}$?

Factorials of Cardinals

Theorem

$[\mathfrak{a}]^2 < \mathfrak{a}!$

Question

- ZF $\vdash \mathfrak{a}$ is infinite $\rightarrow \mathfrak{a}! \not\leqslant [\mathfrak{a}]^3$?
- ZF $\vdash \mathfrak{a}$ is infinite $\rightarrow \mathfrak{a}! \not\leqslant^* \mathfrak{a}$?

Theorem

The following statement is consistent with ZF*:*
There exists an infinite cardinal $\mathfrak{a}$ *such that* $\mathfrak{a}! < [\mathfrak{a}]^3$ *and such that* $\mathfrak{a}! \leqslant^* \mathfrak{a}$.

Permutation Models

ZFU: Zermelo-Fraenkel set theory with **Urelements**

- The language of ZFU consists of the relation symbol "$\in$" and the constant symbol "$\mathtt{U}$"
- Axiom of Empty Set for ZFU:

$$\exists x(x \notin \mathtt{U} \wedge \forall z(z \notin x))$$

- Axiom of Extensionality for ZFU:

$$\forall x \forall y(x \notin \mathtt{U} \wedge y \notin \mathtt{U} \wedge \forall z(z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

- Axiom of Urelements:

$$\forall x(x \in \mathtt{U} \leftrightarrow x \neq \varnothing \wedge \forall z(z \notin x))$$

Permutation Models

- Let U be the set of urelements. We define V^U as follows:

$$
\begin{aligned}
\mathrm{V}_0^U &= U \\
\mathrm{V}_{\alpha+1}^U &= \wp(\mathrm{V}_\alpha^U) \\
\mathrm{V}_\alpha^U &= \bigcup_{\beta<\alpha} \mathrm{V}_\beta^U \quad \text{for limit } \alpha \\
\mathrm{V}^U &= \bigcup_{\alpha\in\mathrm{On}} \mathrm{V}_\alpha^U
\end{aligned}
$$

- $\mathrm{V} = \mathrm{V}^\varnothing \subseteq \mathrm{V}^U$

Permutation Models

Let $\mathcal{G}$ be a subgroup of $\mathcal{S}(U)$. We say that a set $\mathfrak{F}$ of subgroups of $\mathcal{G}$ is a **normal filter** on $\mathcal{G}$ if for all subgroups H, K of $\mathcal{G}$ we have:

- $\mathcal{G} \in \mathfrak{F}$
- If $H \in \mathfrak{F}$ and $H \subseteq K$ then $K \in \mathfrak{F}$
- If $H \in \mathfrak{F}$ and $K \in \mathfrak{F}$ then $H \cap K \in \mathfrak{F}$
- If $\pi \in \mathcal{G}$ and $H \in \mathfrak{F}$ then $\pi H \pi^{-1} \in \mathfrak{F}$
- For all $u \in U$, $\{\pi \in \mathcal{G} \mid \pi u = u\} \in \mathfrak{F}$

Permutation Models

- For all $\pi \in \mathcal{G}$ and all $x \in \mathrm{V}^U$, we define πx by recursion as follows:

$$\pi x = \begin{cases} \pi x & \text{if } x \in U \\ \{\pi y \mid y \in x\} & \text{otherwise.} \end{cases}$$

- For all $\pi \in \mathcal{G}$, π is an $\in$-automorphism of V^U
- For all $x \in \mathrm{V}^U$, we define $\mathrm{sym}_{\mathcal{G}}(x) = \{\pi \in \mathcal{G} \mid \pi x = x\}$
- $x \in \mathrm{V}^U$ is said to be $\mathfrak{F}$-**symmetric** if $\mathrm{sym}_{\mathcal{G}}(x) \in \mathfrak{F}$
- $x \in \mathrm{V}^U$ is said to be $\mathfrak{F}$-**hereditarily symmetric** if x as well as each element of its transitive closure is $\mathfrak{F}$-symmetric.
- For all $\pi \in \mathcal{G}$ and all $x \in \mathrm{V}^U$, x is $\mathfrak{F}$-hereditarily symmetric iff πx is $\mathfrak{F}$-hereditarily symmetric.
- For all $u \in U$, u is $\mathfrak{F}$-hereditarily symmetric.

Permutation Models

Theorem

Let $\mathcal{V}_{\mathfrak{F}} = \{x \in \mathrm{V}^{U} \mid x \text{ is } \mathfrak{F}\text{-hereditarily symmetric}\}$.
Then $\mathcal{V}_{\mathfrak{F}}$ *is a transitive model of* ZFU *such that* $\mathrm{V} \subseteq \mathcal{V}_{\mathfrak{F}} \subseteq \mathrm{V}^{U}$.
We call $\mathcal{V}_{\mathfrak{F}}$ *a* ***permutation model***.

Permutation Models

Let $\mathcal{G}$ be a subgroup of $\mathcal{S}(U)$. A family $\mathcal{I}$ of subsets of U, for example $\mathcal{I} = \mathrm{fin}(U)$, is a **normal ideal** if for all subsets E, F of U we have:

- $\varnothing \in \mathcal{I}$
- If $E \in \mathcal{I}$ and $F \subseteq E$ then $F \in \mathcal{I}$
- If $E \in \mathcal{I}$ and $F \in \mathcal{I}$ then $E \cup F \in \mathcal{I}$
- If $\pi \in \mathcal{G}$ and $E \in \mathcal{I}$ then $\pi E \in \mathcal{I}$
- For all $u \in U$, $\{u\} \in \mathcal{I}$

Permutation Models

- For all $T \subseteq U$, we define $\mathrm{fix}_{\mathcal{G}}(T) = \{\pi \in \mathcal{G} \mid \forall u \in T(\pi u = u)\}$
- If $\mathcal{I}$ is a normal ideal of subsets of U, then the filter $\mathfrak{F}_{\mathcal{I}}$ on $\mathcal{G}$ generated by the subgroups $\{\mathrm{fix}_{\mathcal{G}}(E) \mid E \in \mathcal{I}\}$ is a normal filter on $\mathcal{G}$.
- $x \in \mathrm{V}^U$ is $\mathfrak{F}_{\mathcal{I}}$-symmetric iff $\exists E \in \mathcal{I}(\mathrm{fix}_{\mathcal{G}}(E) \subseteq \mathrm{sym}_{\mathcal{G}}(x))$. We call such an E a **support** of x.

The Basic Fraenkel Model

- The set of urelements U is a countable infinite set.
- $\mathcal{G} = \mathcal{S}(U)$
- $\mathcal{I} = \mathrm{fin}(U)$
- Let $\mathcal{V}_{\mathrm{F}}$ (F for Fraenkel) be the corresponding permutation model, the so-called **basic Fraenkel model**.

The Basic Fraenkel Model

- The set of urelements U is a countable infinite set.
- $\mathcal{G} = \mathcal{S}(U)$
- $\mathcal{I} = \text{fin}(U)$
- Let $\mathcal{V}_{\text{F}}$ (F for Fraenkel) be the corresponding permutation model, the so-called **basic Fraenkel model**.

Fact

- $\mathcal{V}_{\text{F}} \models U$ is amorphous, i.e., U is infinite but every subset of U is finite or co-finite.
- $\mathcal{V}_{\text{F}} \models$ there are no injections from $[U]^3$ into $\mathcal{S}(U)$

A Shelah-Type Permutation Model

- U_0 is an infinite set.
- $\mathcal{G}_0 = \mathcal{S}(U_0)$
- $U_{n+1} = U_n \cup \{\langle n, f, \varepsilon\rangle \mid f \in \mathcal{S}_{\mathrm{fin}}(U_n) \wedge \varepsilon \in \{0, 1, 2\}\}$
- $\mathcal{G}_{n+1} \subseteq \mathcal{S}(U_{n+1})$ is such that for all $h \in \mathcal{S}(U_{n+1})$, $h \in \mathcal{G}_{n+1}$ iff there exists a $g \in \mathcal{G}_n$ such that $h \restriction U_n = g$ and such that for all $f \in \mathcal{S}_{\mathrm{fin}}(U_n)$, there exists a permutation τ on $\{0, 1, 2\}$ such that for all $\varepsilon \in \{0, 1, 2\}$, $h(\langle n, f, \varepsilon\rangle) = \langle n, g \circ f \circ g^{-1}, \tau(\varepsilon)\rangle$
- $U = \bigcup_{n\in\omega} U_n$
- $\mathcal{G} = \{\pi \in \mathcal{S}(U) \mid \forall n \in \omega(\pi \restriction U_n \in \mathcal{G}_n)\}$
- $\mathcal{I} = \mathrm{fin}(U)$
- Let $\mathcal{V}_{\mathrm{S}}$ (S for Shelah) be the corresponding permutation model.

A Shelah-Type Permutation Model

Theorem

$\mathcal{V}_{\mathrm{S}} \models \mathfrak{a}$ *is infinite,* $\mathfrak{a}! < [\mathfrak{a}]^3$ *and* $\mathfrak{a}! \leqslant^* \mathfrak{a}$*, where* $\mathfrak{a} = |U|$.

Thank you