จำนวนเชิงการนับของเซตของการเรียงสับเปลี่ยนบนเซตที่มีจุดไม่ตรึง n จุด

นายจักรกฤษณ์ นันทศรี

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2565

THE CARDINALITY OF THE PERMUTATIONS ON A SET WITH n NON-FIXED POINTS

Mr. Jukkrid Nuntasri

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Mathematics
Department of Mathematics and Computer Science
Faculty of Science Chulalongkorn University
Academic Year 2022

Thesis Title	THE CARDINALITY OF THE PERMUTATIONS ON A SET WITH n NON-FIXED POINTS
By	Mr. Jukkrid Nuntasri
Field of Study	Mathematics
Thesis Professor	Professor Pimpen Vejjajiva, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirement for the Master's Degree.

.... Dean of the Faculty of Science

(Professor Polkit Sangvanich, Ph.D.)

THESIS COMMITTEE

.... Chairman

(Assistant Professor Athipat Thamrongthanyalak, Ph.D.)

.... Thesis Advisor

(Professor Pimpen Vejjajiva, Ph.D.)

.... Committee

(Nattapon Sonpanow, Ph.D.)

.... External Examiner

(Assistant Professor Zu Yao Teoh, Ph.D.)

จักรกฤษณ์ นันทศรี: จำนวนเชิงการนับของเซตของการเรียงสับเปลี่ยนบนเซตที่มีจุดไม่ตรึง n จุด. (THE CARDINALITY OF THE PERMUTATIONS ON A SET WITH n NON-FIXED POINTS) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ศาสตราจารย์ ดร.พิมพ์เพ็ญ เวชชาชีวะ, 38 หน้า.

ในวิทยานิพนธ์นี้เราศึกษาความสัมพันธ์ระหว่าง $|\mathcal{S}_n(A)|$ และ $|\mathrm{seq}_n^{1-1}(A)|$ รวมถึง $|\mathrm{seq}_n(A)|$ สำหรับเซตอนันต์ A โดยที่ $\mathcal{S}_n(A)$ เป็นเซตของการเรียงสับเปลี่ยนบนเซต A ทั้งหมดที่มีจุดไม่ตรึง n จุด $\mathrm{seq}_n(A)$ และ $\mathrm{seq}_n^{1-1}(A)$ เป็นเซตของลำดับและเซตของลำดับหนึ่งต่อหนึ่งของสมาชิกใน A ทั้งหมดที่มีความยาว n ตามลำดับ โดยที่ n เป็นจำนวนธรรมชาติที่มากกว่า 1 เมื่อมีสัจพจน์การเลือก เราได้ว่า ทั้ง $|\mathcal{S}_n(A)|$ $|\mathrm{seq}_n^{1-1}(A)|$ และ $|\mathrm{seq}_n(A)|$ เท่ากันสำหรับทุกเซตอนันต์ A เราแสดงในทฤษฎีเซตแซร์เมโล-แฟรงเคลว่า $|\mathcal{S}_n(A)| \leq |\mathrm{seq}_n^{1-1}(A)|$ สำหรับทุกเซตอนันต์ A ภายใต้สัจพจน์การเลือกแบบอ่อนบางสัจพจน์ และข้อสมมตินี้ไม่สามารถเอาออกได้ ในอีกทิศทาง เราได้แสดงว่า $|\mathrm{seq}_n^{1-1}(A)| \leq |\mathcal{S}_{n+1}(A)|$ สำหรับทุกเซตอนันต์ A และดัชนีล่าง $n+1$ ไม่สามารถลดเป็น n ได้ นอกจากนี้ เราได้แสดงว่า ข้อความ "$|\mathcal{S}_n(A)| \leq |\mathcal{S}_{n+1}(A)|$ สำหรับทุกเซตอนันต์ A" ไม่สามารถพิสูจน์ได้ในทฤษฎีเซตแซร์เมโล-แฟรงเคล

ภาควิชา . . คณิตศาสตร์และวิทยาการคอมพิวเตอร์ . . ลายมือชื่อนิสิต . . . .
สาขาวิชา . . คณิตศาสตร์ . . ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก . . . .
ปีการศึกษา . . . . . 2565 . . . . .

##6370170523 : MAJOR MATHEMATICS.
KEYWORDS: AXIOM OF CHOICE / CARDINAL / PERMUTATION
JUKKRID NUNTASRI: THE CARDINALITY OF THE PERMUTATIONS ON A SET WITH n NON-FIXED POINTS
ADVISOR: PROFESSOR PIMPEN VEJJAJIVA, Ph.D., 38 pp.

In this thesis, we study relationships between $|\mathcal{S}_n(A)|$ and $|\mathrm{seq}^{1-1}_n(A)|$ as well as $|\mathrm{seq}_n(A)|$ for infinite sets A, where $\mathcal{S}_n(A)$ is the set of permutations of A with n non-fixed points and $\mathrm{seq}_n(A)$ and $\mathrm{seq}^{1-1}_n(A)$ are the set of sequences and the set of one-to-one sequences of elements of A with length n, respectively, where n is a natural number greater than 1. With the Axiom of Choice (AC), $|\mathcal{S}_n(A)|$, $|\mathrm{seq}^{1-1}_n(A)|$, and $|\mathrm{seq}_n(A)|$ are equal for all infinite sets A. Among our results, we show, in the Zermelo-Fraenkel set theory (ZF), that $|\mathcal{S}_n(A)| \le |\mathrm{seq}^{1-1}_n(A)|$ for any infinite set A under some weak form of AC and the assumption cannot be removed. In the other direction, we show that $|\mathrm{seq}^{1-1}_n(A)| \le |\mathcal{S}_{n+1}(A)|$ for any infinite set A and the subscript $n+1$ cannot be reduced to n. Moreover, we also show that "$|\mathcal{S}_n(A)| \le |\mathcal{S}_{n+1}(A)|$ for any infinite set A" is not provable in ZF.

Department	Mathematics and Computer Science	Student's Signature	....
Field of Study	Mathematics	Advisor's Signature	....
Academic Year	2022		

Acknowledgements

I would like to thank my advisor, Professor Pimpen Vejjajiva, for guiding my thesis, giving some background knowledges and suggestions. Also I would like to thank Assistant Professor Athipat Thamrongthanyalak and Dr. Nattapon Sonpanow for being members of the thesis committee. In addition, I would like to thank Assistant Professor Zu Yao Teoh for being the external examiner of this thesis. All of them have made useful suggestions.

Finally, I would like to thank my family very much for supporting me. This thesis is funded by the His Royal Highness Crown Prince Maha Vajiralongkorn Scholarship from the Graduate School, Chulalongkorn University to commemorate the 72nd anniversary of his Majesty King Bhumibala Aduladeja.

Jukkrid Nuntasri

Contents

CHAPTER I
Introduction

The factorial $|A|!$ is the cardinality of the set of permutations of a set A. Dawson and Howard showed in [2] that, in the Zermelo-Fraenkel set theory (ZF) with the Axiom of Choice (AC), $|A|! = 2^{|A|}$ for any infinite set A, where $2^{|A|}$ is the cardinality of the power set of A. They also showed that, without AC, each of "$|A|! < 2^{|A|}$", "$2^{|A|} < |A|!$", and "$|A|!$ and $2^{|A|}$ are not comparable" for some infinite set A is consistent with ZF.

Relations between the cardinality of the set of finite sequences of elements of a set A, written $\operatorname{seq}(A)$, and $2^{|A|}$ have been studied in [5] and [6]. Halbeisen and Shelah showed that "$|\operatorname{seq}(A)| \neq 2^{|A|}$ for any infinite set A" is the best possible result in ZF while $|\operatorname{seq}(A)| < 2^{|A|}$ for any infinite set A when AC is assumed. The same results also hold when $\operatorname{seq}(A)$ is replaced by the set of one-to-one finite sequences of elements of A, written $\operatorname{seq}^{1-1}(A)$. Although, without AC, we cannot conclude any relationship between $|A|!$ and $2^{|A|}$ for an arbitrary infinite set A, it has been shown in [11] that, in ZF, relations between $|\operatorname{seq}(A)|$ and $|A|!$ (also $|\operatorname{seq}^{1-1}(A)|$ and $|A|!$) are exactly the same as those of $|\operatorname{seq}(A)|$ and $2^{|A|}$ for infinite sets A. In contrast, the main theorem in [10] showed, in ZF, that $|\operatorname{seq}_n(A)| < |A|!$ for any infinite set A and any natural number n, where $\operatorname{seq}_n(A)$ is the set of sequences of elements of A with length n, although Specker showed in [12] that "$|\operatorname{seq}_2(A)| \leq 2^{|A|}$ for any infinite set A" is not provable in ZF.

In this thesis, we investigate relationships between $|\mathcal{S}_n(A)|$ and $|\operatorname{seq}_n^{1-1}(A)|$ as well as $|\operatorname{seq}_n(A)|$ for infinite sets A, where $\mathcal{S}_n(A)$ is the set of permutations of A with n non-fixed points and $\operatorname{seq}_n^{1-1}(A)$ is the set of one-to-one sequences of elements of A with length n where n is a natural number greater than 1. With AC, $|\mathcal{S}_n(A)|$,

$|\mathrm{seq}_n^{1-1}(A)|$, and $|\mathrm{seq}_n(A)|$ are equal for all infinite sets A. Among our results, we show, in ZF, that $|\mathcal{S}_n(A)| \leq |\mathrm{seq}_n^{1-1}(A)|$ for any infinite set A under some weak form of AC and this assumption cannot be removed. In the other direction, we show that $|\mathrm{seq}_n^{1-1}(A)| \leq |\mathcal{S}_{n+1}(A)|$ for any infinite set A and the subscript $n+1$ cannot be reduced to n. Moreover, we also show that "$|\mathcal{S}_n(A)| \leq |\mathcal{S}_{n+1}(A)|$ for any infinite set A" is not provable in ZF.

The thesis is arranged as follows. First, we give some background on set theory in Chapter II, and permutation models in Chapter III. Results in ZF are in Chapter IV and consistency results are in Chapter V. We conclude our thesis in Chapter VI.

CHAPTER II
Preliminaries

Firstly, G. Cantor used sets as collections of objects but this leads to paradoxes. To avoid this problem, we can use an axiomatic method and leave set be undefined. This is called axiomatic set theory. Nowadays, Zermelo-Frankel set theory (ZF) with the Axiom of Choice (AC), denoted by ZFC, is the most well-known axiomatic set theory. In this thesis, we shall work in ZF.

In this section, we give some prerequisite knowledge on set theory. Proofs of all theorems will be omitted but it can be found in [3].

2.1 Cardinal Numbers

A *cardinal (number)* is a number used to measure the size of a set, i.e. the number of all elements of a set. Denote the *cardinal number* of a set X by $|X|$. Cardinals are defined so that for any sets X and Y, $|X| = |Y|$ if and only if there is a bijection from X onto Y, written $X \approx Y$.

Definition. *Natural numbers* are constructed as follows:

$$0 = \emptyset, 1 = \{0\}, 2 = \{0, 1\}, 3 = \{0, 1, 2\}, \ldots.$$

Let ω be the set of all natural numbers.

Definition. Let X be a set. If $X \approx n$ for some $n \in \omega$, X is said to be *finite* and define $|X| = n$; otherwise, X is said to be *infinite*. We call $|X|$ a *finite cardinal* if X is finite; otherwise, $|X|$ is an *infinite cardinal*.

Note. *Every finite cardinal is a natural number and vice-versa.*

Definition. Let $\aleph_0 = |\omega|$.

Definition. Let X and Y be sets with $\kappa = |X|$ and $\lambda = |Y|$. Define

1. $\kappa + \lambda = |X \cup Y|$ where $X \cap Y = \emptyset$,

2. $\kappa \cdot \lambda = |X \times Y|$,

3. $\kappa^\lambda = |\{f \mid f : Y \to X\}|$.

Some basic properties of cardinal arithmetic are listed in the following theorem.

Theorem 2.1.1. *Let κ, λ and μ be cardinals. Then*

1. $\kappa + \lambda = \lambda + \kappa$,

2. $(\kappa + \lambda) + \mu = \kappa + (\lambda + \mu)$,

3. $\kappa \cdot \lambda = \lambda \cdot \kappa$,

4. $(\kappa \cdot \lambda) \cdot \mu = \kappa \cdot (\lambda \cdot \mu)$,

5. $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$,

6. $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$,

7. $(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$,

8. $(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$.

Definition. Let X and Y be sets with $\kappa = |X|$ and $\lambda = |Y|$.
Then we say that

1. $\kappa \leq \lambda$ if there is an injection from X into Y, written $X \preceq Y$,

2. $\kappa < \lambda$ if $\kappa \leq \lambda$ and $\kappa \neq \lambda$.

Theorem 2.1.2 (Cantor-Bernstein Theorem)**.** *For any cardinal numbers κ and λ, if $\kappa \leq \lambda$ and $\lambda \leq \kappa$, then $\kappa = \lambda$.*

Note that $\leq$ partially orders the cardinal numbers. Moreover, the following theorem shows that $\leq$ also preserves cardinal arithmetic.

Theorem 2.1.3. *Let κ, λ and μ be cardinals such that $\kappa \leq \lambda$. Then*

1. $\kappa + \mu \leq \lambda + \mu$,
2. $\kappa \cdot \mu \leq \lambda \cdot \mu$,
3. $\kappa^\mu \leq \lambda^\mu$,
4. $\mu^\kappa \leq \mu^\lambda$, *if* $\mu \neq 0$ *or* $\kappa \neq 0$.

Note that in the above theorem, if we assume $\kappa < \lambda$, we cannot replace $\leq$ in each statement in the list by $<$. For example, $\aleph_0 + 1 = \aleph_0 = \aleph_0 + 2$.

2.2 Ordinals

Definition. We say that a set A is a *transitive set* if and only if

$$a \subseteq A \text{ for all } a \in A.$$

Definition. We say that α is an *ordinal (number)* if and only if α is a transitive set and $\in$ well orders α.

For example, every natural numbers and ω are ordinals.

Theorem 2.2.1. *Every well-ordered set is isomorphic to a unique ordinal.*

Definition. Let $\mathbf{ON} = \{\alpha \mid \alpha \text{ is an ordinal}\}$.

Definition. Let α, β be ordinals. We define $\alpha < \beta$ if and only if $\alpha \in \beta$ and define $\alpha \leq \beta$ if $\alpha < \beta$ or $\alpha = \beta$.

Theorem 2.2.2. *Let α, β, γ be ordinals. Then*

1. $\alpha \nless \alpha$,
2. *if* $\alpha < \beta$ *and* $\beta < \gamma$, *then* $\alpha < \gamma$,
3. *exactly one of the statements "$\alpha < \beta$", "$\alpha = \beta$", "$\beta < \alpha$" is true,*
4. *any nonempty set of ordinals has a least element.*

In conclusion, the above theorem tell us that $<$ well orders **ON**.

Definition. For a set A, let $A^+ = A \cup \{A\}$.

Theorem 2.2.3. *If α is an ordinal, α^+ is the least ordinal greater than α.*

Theorem 2.2.4. *If A is a set of ordinals, then $\bigcup A = \sup A$.*

Definition. Let $\alpha \neq 0$ be an ordinal. We say that α is a *successor ordinal* if $\alpha = \beta^+$ for some ordinal β, otherwise α is said to be a *limit ordinal.*

Furthermore, ordinal numbers also have arithmetic structure. In this thesis, we only use the addition of ordinals.

Definition. Define the ordinal addition recursively as follows:

1. $\alpha + 0 = \alpha$,
2. $\alpha + \beta^+ = (\alpha + \beta)^+$,
3. $\alpha + \lambda = \bigcup\{\alpha + \xi | \xi < \lambda\}$ if λ is a limit ordinal.

Addition on ordinals is not commutative. For example,

$$1 + \omega = \bigcup\{1 + n | n < \omega\} = \omega \neq \omega + 1.$$

However, left addition preserves order.

Theorem 2.2.5. *If α and β are ordinals such that $\alpha < \beta$, then $\gamma + \alpha < \gamma + \beta$ for any ordinal γ.*

2.3 Axiom of Choice

Definition. A *choice function* f for a set X is a function $f : X \setminus \{\emptyset\} \to \bigcup X$ such that for any $x \in X \setminus \{\emptyset\}, f(x) \in x$.

The following statements are some equivalent forms of the Axiom of Choice (AC).

1. Well-Ordering Theorem: Every set can be well-ordered.

2. Cardinal Comparability: For any cardinal numbers κ and λ, $\kappa \leq \lambda$ or $\lambda \leq \kappa$.

3. Every set has a choice function.

4. For every infinite cardinal $\kappa, \kappa^2 = \kappa$.

Since the Axiom of Choice is equivalent to the Well-Ordering Theorem, if we assume AC, then cardinal numbers can be defined as follows:

Definition. The *cardinal number* of a set A is the least ordinal α such that $A \approx \alpha$.

For example, $|\omega^+| = \omega$ since $\omega^+ \approx \omega$ and every ordinal which is less than ω is finite.

The following are consequences of AC.

Theorem 2.3.1 (Absorption law of arithmetic)**.** *For any cardinals κ and λ of which at least one is infinite,*

1. $\kappa + \lambda = \max\{\kappa, \lambda\}$,

2. $\kappa \cdot \lambda = \max\{\kappa, \lambda\}$ *if* $\min\{\kappa, \lambda\} \neq 0$.

More details about AC can be found in [8].

2.4 Cardinal numbers without AC

Since the Axiom of Choice is equivalent to the Well-Ordering Theorem, without AC, we cannot guarantee that every set can be well-ordered. As a result, in general, we cannot define the cardinal number of a set to be an ordinal. To solve this problem, we can use Foundation Axiom and the rank function to define a cardinal number of a set. However, the definition is not needed here. We use only the fact that cardinal numbers are defined so that for any sets A and B,

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

Since the Cardinal Comparability is equivalent to AC, without AC, we cannot guarantee whether two infinite cardinals are comparable or not. In particular, infinite cardinals may not be compared with $\aleph_0$.

Definition. A set X is *Dedekind-infinite* if $\aleph_0 \leq |X|$; otherwise, X is a *Dedekind-finite.*

Note. *Every Dedekind-infinite set is infinite but the converse is not necessarily true without AC.*

Theorem 2.4.1. *A set X is Dedekind-infinite if and only if $X \approx Y$ for some $Y \subset X$.*

2.5 Weak forms of AC

Even though AC is equivalent to many important theorems, for example, Zorn's lemma, Tychonoff's theorem, and "every vector space has a basis", it also leads to some counterintuitive results such as Banach-Tarski paradox. Thus some mathematicians avoid using AC and sometimes use weaker forms of AC instead.

The following weak choice principles are relevant to our work. In the statements below, n is a natural number greater than 1.

- AC_n: Every family of n-element sets has a choice function. (This will be used in Theorem 4.4 and Corollary 4.5.)
- $\mathrm{AC}_{\leq n}$: Every family of nonempty sets with cardinalities less than or equal to n has a choice function. (This will be used in Theorems 4.3,4.6 and Corollary 4.7.)

CHAPTER III
Permutation Models

The Zermelo-Frankel set theory with atoms (ZFA) is a modified version of ZF, which admits objects other than sets, called *atoms*. Atoms are objects which do not have any elements.

For consistency results, we shall use permutation models, which are models of ZFA. Proofs of all theorems in this chapter will be omitted. More details can be found in [8, Chapter 4].

3.1 Permutation Models

Definition. Let S be a set. For each ordinal α, define $\mathcal{P}^\alpha(S)$ recursively as follows.

1. $\mathcal{P}^0(S) = S$,
2. $\mathcal{P}^\alpha(S) = \mathcal{P}^\beta(S) \cup \mathcal{P}(\mathcal{P}^\beta(S))$ if $\alpha = \beta + 1$,
3. $\mathcal{P}^\alpha(S) = \bigcup_{\xi<\alpha} \mathcal{P}^\xi(S)$ if α is a limit ordinal.

Define $\mathcal{P}^\infty(S) = \bigcup_{\alpha\in\mathbf{ON}} \mathcal{P}^\alpha(S)$.

We call $\mathcal{P}^\infty(\emptyset)$ the *kernel*.

Throughout this section, let A be a set of atoms.

Theorem 3.1.1. $\mathcal{P}^\infty(A)$ *is a model of* ZFA.

Let $\mathcal{M} = \mathcal{P}^\infty(A)$.

Definition. Let π be a permutation on A. We extend π by defining $\pi(x)$, which can also be written as πx, for every x in $\mathcal{M}$ recursively as follows.

$$\pi(\emptyset) = \emptyset \text{ and } \pi(x) = \{\pi(y) \mid y \in x\}.$$

Theorem 3.1.2. *Let π be a permutation on A and let $x, y \in \mathcal{M}$. Then*

1. *$x \in y$ if and only if $\pi x \in \pi y$.*
2. *$\pi\{x, y\} = \{\pi x, \pi y\}$ and $\pi(x, y) = (\pi x, \pi y)$.*
3. *If f is a function on a set X containing x, then πf is a function on πX and $(\pi f)(\pi x) = \pi(f(x))$,*
4. *$\pi x = x$ if x is in the kernel.*

Definition. Let $\mathcal{G}$ be a group of permutations of A. A set $\mathcal{F}$ of subgroups of $\mathcal{G}$ is a *normal filter* on $\mathcal{G}$ if for all subgroups H and K of $\mathcal{G}$,

1. $\mathcal{G} \in \mathcal{F}$,
2. if $H \in \mathcal{F}$ and $H \subseteq K$, then $K \in \mathcal{F}$,
3. if $H \in \mathcal{F}$ and $K \in \mathcal{F}$, then $H \cap K \in \mathcal{F}$,
4. if $\pi \in \mathcal{G}$ and $H \in \mathcal{F}$, then $\pi H \pi^{-1} \in \mathcal{F}$,
5. for each $a \in A$, $\{\pi \in \mathcal{G} \mid \pi(a) = a\} \in \mathcal{F}$.

In the following, let $\mathcal{G}$ be a group of permutations of A and $\mathcal{F}$ be a normal filter on $\mathcal{G}$.

Definition. Let $x \in \mathcal{M}$. Define

$$\operatorname{sym}_{\mathcal{G}}(x) = \{\pi \in \mathcal{G} \mid \pi x = x\}.$$

Note that $\operatorname{sym}_{\mathcal{G}}(x)$ is a subgroup of $\mathcal{G}$.

Definition. For $x \in \mathcal{M}$, x is called *symmetric* if $\operatorname{sym}_{\mathcal{G}}(x) \in \mathcal{F}$.

The class $\mathcal{V}$ consisting of all hereditarily symmetric objects is called a *permutation model.*

Theorem 3.1.3. *The class $\mathcal{V}$ is a transitive model of* ZFA *which contains all the elements of the kernel and $A \in \mathcal{V}$.*

Definition. A set $\mathcal{I}$ of subsets of A is a *normal ideal* if

1. $\emptyset \in \mathcal{I}$,
2. if $E \in \mathcal{I}$ and $F \subseteq E$, then $F \in \mathcal{I}$,
3. if $E \in \mathcal{I}$ and $F \in \mathcal{I}$, then $E \cup F \in \mathcal{I}$,
4. if $\pi \in \mathcal{G}$ and $E \in \mathcal{I}$, then $\pi(E) \in \mathcal{I}$,
5. for each $a \in A$, $\{a\} \in \mathcal{I}$.

Remark. *The set of all finite subsets of A, denoted by $\operatorname{fin}(A)$ is a normal ideal.*

Definition. For each $x \in \mathcal{M}$, define

$$\operatorname{fix}_{\mathcal{G}}(x) = \{\pi \in \mathcal{G} \mid \pi y = y \text{ for all } y \in x\}.$$

Theorem 3.1.4. *Let $\mathcal{I}$ be a normal ideal. Then*

$$\mathcal{F}_{\mathcal{I}} = \{H \mid H \textit{ is a subgroup of } \mathcal{G} \textit{ such that } \operatorname{fix}_{\mathcal{G}}(E) \subseteq H \textit{ for some } E \in \mathcal{I}\}$$

is a normal filter.

In the following, $\mathcal{I}$ is a normal ideal.

Note. *By Theorems 3.1.3 and 3.1.4, $\mathcal{I}$ has a corresponding normal filter $\mathcal{F}_{\mathcal{I}}$ and a corresponding permutation model $\mathcal{V}$. We call such permutation model, the permutation model determined by $\mathcal{G}$ and $\mathcal{I}$.*

Definition. For each $x \in \mathcal{M}$ and each $E \in \mathcal{I}$, we say

$$E \text{ is a } \textit{support} \text{ of } x \text{ if } \operatorname{fix}_{\mathcal{G}}(E) \subseteq \operatorname{sym}_{\mathcal{G}}(x).$$

Remark. *If $\mathcal{V}$ is a permutation model determined by $\mathcal{G}$ and $\mathcal{I}$, then*

1. $x \in \mathcal{V}$ if and only if x has a support and $x \subseteq \mathcal{V}$,
2. for each $x \in \mathcal{M}$ and each $E, F \in \mathcal{I}$, if E is a support of x and $E \subseteq F$, then F is also a support of x.

Definition. Let $\pi \in \mathcal{G}$ and $x \in \mathcal{M}$. We say

1. π fixes x setwise if $\pi x = x$, i.e. $\pi \in \operatorname{sym}_{\mathcal{G}}(x)$,
2. π fixes x pointwise if $\pi y = y$ for all $y \in x$, i.e. $\pi \in \operatorname{fix}_{\mathcal{G}}(x)$.

3.2 Well-known Models

These following permutation models are used in this thesis.

The basic Fraenkel model

Definition. Let A be a denumerable set of atoms. Let $\mathcal{G}$ be the group of all permutations on A. The *basic Fraenkel model*, $\mathcal{V}_{F_0}$, is the permutation model determined by $\mathcal{G}$ and the normal ideal $\text{fin}(A)$.

Theorem 3.2.1. *[7, page 177]* AC_n *fails in* $\mathcal{V}_{F_0}$.

The second Fraenkel model

Definition. Let the set of atoms A be the disjoint union of pairs $P_n = \{a_n, b_n\}$ where $n \in \omega$. Let $\mathcal{G}$ be the group of all permutations ψ on A such that $\psi[P_n] = P_n$ for all $n \in \omega$. The *second Fraenkel model*, $\mathcal{V}_{F_2}$, is the permutation model determined by $\mathcal{G}$ and the normal ideal $\text{fin}(A)$.

Note that AC_2 fails in this model since the set of atoms A is Dedekind-finite in the model (see [7, page 178])

3.3 Transferable statements

Let $\mathcal{V}$ be a permutation model. A formula $\phi(x)$ is *boundable* if $\mathcal{V} \models \phi(x) \leftrightarrow \phi^{\mathcal{P}^\gamma(x)}(x)$ for some ordinal γ. A statement is *boundable* if it is the existential closure of a boundable formula.

From the Jech-Sochor First Embedding Theorem (cf. [8, Theorem 6.1]), we have that if a boundable statement holds in a permutation model, then it is consistent with ZF.

From our consistency results in Chapter V, all statements that are shown to hold in some permutation models are boundable and thus they are consistent with ZF.

CHAPTER IV
Results in ZF

In this chapter, we shall investigate relations between the permutations with n non-fixed points and the sequences with length n of a set, where n is a natural number greater than 1.

To get started, we list the notations used in this chapter below.

Notation. For a set A and a natural number n, let

1. $[A]^n = \{X \subseteq A \mid |X| = n\}$,
2. $[A]^{\leq n} = \{X \subseteq A \mid |X| \leq n\}$,
3. $\operatorname{fin}(A) = \bigcup_{k\in\omega} [A]^k$,
4. $\operatorname{seq}_n(A) = \{f \mid f\colon n \to A\}$,
5. $\operatorname{seq}(A) = \bigcup_{k\in\omega} \operatorname{seq}_k(A)$,
6. $\operatorname{seq}_n^{1-1}(A) = \{f \in \operatorname{seq}_n(A) \mid f \text{ is injective}\}$,
7. $\operatorname{seq}^{1-1}(A) = \bigcup_{k\in\omega} \operatorname{seq}_k^{1-1}(A)$,
8. $\mathcal{S}(A) = \{f\colon A \to A \mid f \text{ is bijective}\}$,
9. $\mathcal{S}_n(A) = \{f \in \mathcal{S}(A) \mid |\{a \in A \mid f(a) \neq a\}| = n\}$,
10. $\mathcal{S}_{\text{fin}}(A) = \bigcup_{k\in\omega} \mathcal{S}_k(A)$,

and for $\pi \in \mathcal{S}(A)$, let $(\pi) = \{a \in A \mid \pi(a) \neq a\}$, in other words, (π) collects all elements in A that π permutes.

We write $(a_0; a_1; \ldots; a_n)$ for the cyclic permutation such that

$$a_0 \mapsto a_1 \mapsto \ldots \mapsto a_n \mapsto a_0.$$

Throughout, n is a natural number which is greater than 1, unless otherwise stated.

First, by using some combinatorial argument, we have the following relations for the case of finite sets.

Theorem 4.1. *For any finite set X with $|X| = m \geq n$,*

$$|\mathcal{S}_n(X)| \leq |\mathrm{seq}_n^{1-1}(X)|.$$

Proof. Let X be a finite set with $|X| = m \geq n$. For each $A \in [X]^n$, define

$$\mathcal{S}_n(X; A) = \{\pi \in \mathcal{S}_n(X) \mid (\pi) = A\} \text{ and}$$
$$\mathrm{seq}_n^{1-1}(X; A) = \{f \in \mathrm{seq}_n^{1-1}(X) \mid \mathrm{ran}(f) = A\}.$$

Then $\mathcal{S}_n(X) = \bigcup_{A \in [X]^n} \mathcal{S}_n(X; A)$, $\mathrm{seq}_n^{1-1}(X) = \bigcup_{A \in [X]^n} \mathrm{seq}_n^{1-1}(X; A)$ and for any distinct $A, A' \in [X]^n$, we have

$$\mathcal{S}_n(X; A) \cap \mathcal{S}_n(X, A') = \emptyset \text{ and } \mathrm{seq}_n^{1-1}(X; A) \cap \mathrm{seq}_n^{1-1}(X; A') = \emptyset.$$

Hence

$$|\mathcal{S}_n(X)| = \sum_{A \in [X]^n} |\mathcal{S}_n(X; A)| = \sum_{A \in [X]^n} |\mathcal{S}_n(A)| \text{ and}$$
$$|\mathrm{seq}_n^{1-1}(X)| = \sum_{A \in [X]^n} |\mathrm{seq}_n^{1-1}(X; A)|.$$

Since for any $A \in [X]^n$, we have $\mathcal{S}_n(A) \subseteq \mathcal{S}(A)$ and $|\mathcal{S}(A)| = n! = |\mathrm{seq}_n^{1-1}(X; A)|$, we conclude that

$$|\mathcal{S}_n(X)| = \sum_{A \in [X]^n} |\mathcal{S}_n(A)| \leq \binom{m}{n} n! = |\mathrm{seq}_n^{1-1}(X)|$$

as desired. □

Theorem 4.2. *For any set X with $|X| = n$,*

$$|\mathcal{S}_n(X)| = n! \left[\frac{1}{0!} - \frac{1}{1!} + \ldots + \frac{(-1)^n}{n!} \right].$$

Proof. Let $X = \{x_1, \ldots, x_n\}$ be a set. For each $i \le n$, define $X_i = \{\pi \in \mathcal{S}(X) \mid \pi(x_i) = x_i\}$ and $X_i^c = \mathcal{S}(X) \setminus X_i$. Then

$$|\mathcal{S}_n(X)| = |X_1^c \cap \ldots \cap X_n^c| = |\mathcal{S}(X)| - |X_1 \cup \ldots \cup X_n|$$

and for any $1 \le l \le n$ and $1 \le i_1 < \ldots < i_l \le n$, $|X_{i_1} \cap \ldots \cap X_{i_l}| = (n-l)!$.

By the inclusion-exclusion principle, we have

$$\begin{aligned} |X_1 \cup \ldots \cup X_n| &= \sum_{1 \le i_1 \le n} |X_{i_1}| - \sum_{1 \le i_1 < i_2 \le n} |X_{i_1} \cap X_{i_2}| + \ldots + (-1)^{n-1} |X_1 \cap \ldots \cap X_n| \\ &= \binom{n}{1}(n-1)! - \binom{n}{2}(n-2)! + \ldots + (-1)^{n-1}\binom{n}{n}0! \\ &= n!\left[\frac{1}{1!} + \ldots + \frac{(-1)^{n-1}}{n!}\right], \end{aligned}$$

and so $|\mathcal{S}_n(X)| = n!\left[\frac{1}{0!} - \frac{1}{1!} + \ldots + \frac{(-1)^n}{n!}\right]$ as desired. □

Next, we give a relation between $|\mathcal{S}_n(A)|$ and $|\mathrm{seq}_n^{1-1}(A)|$ for an infinite set A under the weak form $\mathrm{AC}_{\le n}$. Later, we shall show in the next chapter that this assumption cannot be removed.

Theorem 4.3. $\mathrm{AC}_{\le n}$ *implies that* $|\mathcal{S}_n(A)| \le |\mathrm{seq}_n^{1-1}(A)|$ *for every infinite set* A.

Proof. Let A be an infinite set. By $\mathrm{AC}_{\le n}$, $[A]^{\le n}$ has a choice function, say F. Hence every $B \in [A]^n$ has a linear order $<_B$ induced by the ordering on ω via the map $\phi_B : |B| \to B$ defined recursively by $\phi_B(k) = F(B \setminus \phi_B[k])$.

For each $\pi \in \mathcal{S}_n(A)$ where $(\pi) = \{b_1, \ldots, b_n\}$ and $b_1 <_{(\pi)} \cdots <_{(\pi)} b_n$, we define $f\colon \mathcal{S}_n(A) \to \mathrm{seq}_n^{1-1}(A)$ by

$$f(\pi) = (\pi(b_1), \ldots, \pi(b_n)).$$

We will show that f is an injection. Let $\pi, \psi \in \mathcal{S}_n(A)$ be distinct permutations. We distinguish into cases below.

<u>Case 1</u> $(\pi) \ne (\psi)$.

Since each entry of $f(\chi)$ is a member of (χ) and vice versa for any $\chi \in \mathcal{S}_n(A)$, $f(\pi) \ne f(\psi)$.

<u>Case 2</u> $(\pi) = (\psi)$.

Hence there exists an integer $1 \leq k \leq n$ such that $\pi(b_k) \neq \psi(b_k)$ where $(\pi) = \{b_1, \ldots, b_n\}$ and $b_1 <_{(\pi)} \ldots <_{(\pi)} b_n$. Since $\pi(b_k)$ and $\psi(b_k)$ are the k$^{\text{th}}$ entries of $f(\pi)$ and $f(\psi)$ respectively, $f(\pi) \neq f(\psi)$. □

From the above proof, the theorem below shows that if we restrict the domain of f to $\mathcal{C}_n(A) = \{\pi \in \mathcal{S}_n(A) \mid \pi \text{ is a cyclic permutation}\}$, then $\mathrm{AC}_{\leq n}$ in the above theorem can be weaken to AC_n.

Theorem 4.4. AC_n *implies that* $|\mathcal{C}_n(A)| \leq |\mathrm{seq}_n^{1-1}(A)|$ *for every infinite set* A.

Proof. Let A be an infinite set. By AC_n, there exists a choice function $F : [A]^n \to A$. Now, define $g : \mathcal{C}_n(A) \to \mathrm{seq}_n^{1-1}(A)$ by

$$g(\pi) = (\pi(b), \pi(\pi(b)), \ldots, \pi^n(b)),$$

where $b = F((\pi))$.

To show that g is an injection, suppose $\pi, \psi \in \mathcal{C}_n(A)$ are distinct permutations.

If $(\pi) \neq (\psi)$, then, for the same reason as Case 1 in the proof of the above theorem, we have $g(\pi) \neq g(\psi)$.

Suppose $(\pi) = (\psi)$. Since π and ψ are distinct cyclic permutations, $\pi^k(b) \neq \psi^k(b)$ for some $1 \leq k \leq n$, where $b = F((\pi))$. Since $\pi^k(b)$ and $\psi^k(b)$ are the k$^{\text{th}}$ entries of $g(\pi)$ and $g(\psi)$ respectively, $g(\pi) \neq g(\psi)$. □

Note that for $n \leq 3$, $\mathcal{S}_n(A) = \mathcal{C}_n(A)$ for any set A with $|A| \geq 3$. As a result, from the above theorem, we obtain the following corollary.

Corollary 4.5. *If* $n \leq 3$*, then* AC_n *implies* $|\mathcal{S}_n(A)| \leq |\mathrm{seq}_n^{1-1}(A)|$ *for every infinite set* A.

Relations between $|\mathrm{seq}(A)|$ and $|\mathrm{fin}(A)|$ for infinite sets A have been studied in [1]. The theorem below is a result which is related to our work.

Theorem 4.6. $\mathrm{AC}_{\leq n}$ *implies that* $|\mathrm{seq}_n(A)| \leq |\mathrm{fin}(A)|$ *for every infinite set* A.

Proof. Cf. [1, Corollary 2.2]. □

Thus the following corollary follows immediately from the above theorems.

Corollary 4.7. $\mathrm{AC}_{\leq n}$ *implies that* $|\mathcal{S}_n(A)| \leq |\mathrm{fin}(A)|$ *for every infinite set* A.

Next, we show relationships between $|\mathcal{S}_n(\alpha)|$ and other related cardinals when α is an infinite ordinal.

Theorem 4.8. *For any infinite ordinal* α, $\alpha \preceq \mathcal{S}_n(\alpha)$.

Proof. Let α be an infinite ordinal. We define $f\colon \alpha \to \mathcal{S}_n(\alpha)$ by

$$f(\beta) = \begin{cases} (\beta+1; \beta+2; \ldots; \beta+n) & \text{if } \beta+n < \alpha, \\ (k+2; k+4; \ldots; k+2n) & \text{if } \beta+k = \alpha \leq \beta+n. \end{cases}$$

To show that f is an injection, suppose $\beta < \gamma < \alpha$. We distinguish into cases as follows:

<u>Case 1</u> $\gamma + n < \alpha$.

Then $\beta + i < \gamma + n < \alpha$ for all $1 \leq i \leq n$ and so

$$f(\beta) = (\beta+1; \beta+2; \ldots; \beta+n) \neq (\gamma+1; \gamma+2; \ldots; \gamma+n) = f(\gamma).$$

<u>Case 2</u> $\alpha \leq \beta + n$.

Since $\beta < \alpha \leq \beta + n < \gamma + n$, $\alpha = \beta + k$ and $\alpha = \gamma + l$ for some $l < k \leq n$. Hence $f(\beta) = (k+2; k+4; \ldots; k+2n) \neq (l+2; l+4; \ldots; l+2n) = f(\gamma)$.

<u>Case 3</u> $\beta + n < \alpha \leq \gamma + n$.

Since $(f(\beta)) = \{\beta+1, \beta+2, ..., \beta+n\}$ and

$$(f(\gamma)) = \{k+2, k+4, ..., k+2n\} \text{ where } \gamma + k = \alpha,$$

$(f(\beta))$ is the set of n consecutive ordinals where $n \geq 2$, meanwhile $(f(\gamma))$ is not. Hence $f(\beta) \neq f(\gamma)$. $\square$

Fact 4.9. *For any infinite ordinal* α, $\alpha \approx \mathrm{seq}(\alpha)$.

Proof. Cf. [4, Theorem 5.19]. $\square$

Corollary 4.10. *For all infinite ordinals* α,

$$\alpha \approx \mathrm{seq}_n^{1-1}(\alpha) \approx \mathrm{seq}_n(\alpha) \approx \mathcal{S}_n(\alpha) \approx \mathcal{S}_{n+1}(\alpha).$$

Proof. Let α be an infinite ordinal. By Theorems 4.3 and 4.8 and Fact 4.9, we have

$$\operatorname{seq}(\alpha) \approx \alpha \preceq \mathcal{S}_n(\alpha) \preceq \operatorname{seq}_n^{1-1}(\alpha) \preceq \operatorname{seq}_n(\alpha) \preceq \operatorname{seq}(\alpha).$$

By the Cantor-Bernstein theorem, we have that $\alpha \approx \mathcal{S}_n(\alpha) \approx \operatorname{seq}_n^{1-1}(\alpha) \approx \operatorname{seq}_n(\alpha)$. Since n is arbitrary, we also have $\alpha \approx \mathcal{S}_{n+1}(\alpha)$. □

We have shown that if $\mathrm{AC}_{\leq n}$ is assumed, then $|\mathcal{S}_n(A)| \leq |\operatorname{seq}_n(A)|$ for all infinite sets A. Now we shift our focus to the other direction. It has been shown in [9, Lemma 3.27] that for any set A with $|A| \geq 2n(n+1)$, $|\operatorname{seq}_n(A)| \leq |\mathcal{S}_{\leq 2n+1}(A)|$, where $\mathcal{S}_{\leq 2n+1}(A)$ is the set of permutations of A which move at most $2n+1$ elements of A. Now, we shall show that $|\operatorname{seq}_n(A)| \leq |\mathcal{S}_{n+1}(A)|$ for any large enough finite set A and $|\operatorname{seq}_n^{1-1}(A)| \leq |\mathcal{S}_{n+1}(A)|$ for any infinite set A. First, we look at the finite case.

Theorem 4.11. *Let A be a finite set with $|A| \geq 3 \cdot 2^n + n$. Then $|\operatorname{seq}_n(A)| \leq |\mathcal{S}_{n+1}(A)|$.*

Proof. For convenience, let $|A| = a$. For any natural number $n \geq 1$, we have

$$\frac{1}{0!} - \frac{1}{1!} + \cdots + \frac{(-1)^{n+1}}{(n+1)!} \geq 1 - 1 + \frac{1}{2} - \frac{1}{6} = \frac{1}{3}.$$

Since $a \geq 3 \cdot 2^n + n > 2n$, $a < 2(a-n)$ and so

$$\begin{aligned}
|\operatorname{seq}_n(A)| = a^n &< (2(a-n))^n \\
&< a \cdot (a-1) \cdot \ldots \cdot (a-(n-1))2^n \\
&\leq a \cdot (a-1) \cdot \ldots \cdot (a-n+1) \left[\frac{a-n}{3}\right] \\
&\leq a \cdot (a-1) \cdot \ldots \cdot (a-n) \left[\frac{1}{0!} - \frac{1}{1!} + \ldots + \frac{(-1)^{n+1}}{(n+1)!}\right] \\
&= \binom{a}{n+1}(n+1)! \left[\frac{1}{0!} - \frac{1}{1!} + \cdots + \frac{(-1)^{n+1}}{(n+1)!}\right] \\
&= |\mathcal{S}_{n+1}(A)|
\end{aligned}$$

as desired. □

For the infinite case, we need some "large enough" finite set to construct an injection.

Lemma 4.12. *There exists a natural number $K_n \geq 2n+1$ such that for all natural numbers $k < n$,*

$$k!\binom{n}{k}\binom{K_n}{k} \leq (k+1)!\binom{K_n}{k+1}.$$

Proof. Note that for any natural number $x > n$,

$$k!\binom{n}{k}\binom{x}{k} = k!\binom{n}{k} \cdot \tfrac{x(x-1)\ldots(x-k+1)}{k!} \text{ and } (k+1)!\binom{x}{k+1} = (k+1)! \cdot \tfrac{x(x-1)\ldots(x-k)}{(k+1)!}.$$

Hence, for any natural number x such that $k < n < x$, the condition $k!\binom{n}{k}\binom{x}{k} \leq (k+1)!\binom{x}{k+1}$ is equivalent to $\binom{n}{k} \leq x - k$, that is, $x \geq \binom{n}{k} + k$.

Therefore, $x = K_n = \max\{2n+1, \binom{n}{0} + 0, \ldots, \binom{n}{n-1} + n - 1\}$ satisfies the inequalities. $\square$

We shall create an equivalence relation $\sim$ on $\mathrm{seq}^{1-1}_{n+1}(X)$ which tells us that two related sequences will generate the same cyclic permutation.

Definition 4.13. For any $(a_0, \ldots, a_n), (b_0, \ldots, b_n) \in \mathrm{seq}^{1-1}_{n+1}(X)$,

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \text{ iff there exists } k \in \omega \text{ such that } a_l = b_{l+k} \text{ for all } l \in \omega,$$

where the indices of a_i and b_i are considered in modulo $n+1$.

The lemma below shows that this definition gives the desired property.

Lemma 4.14. *For any $(a_0, \ldots, a_n), (b_0, \ldots, b_n) \in \mathrm{seq}^{1-1}_{n+1}(X)$, we have*

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \text{ iff } (a_0; \ldots; a_n) = (b_0; \ldots; b_n).$$

Proof. Let $a = (a_0, \ldots, a_n) \in \mathrm{seq}^{1-1}_{n+1}(X)$ and $b = (b_0, \ldots, b_n) \in \mathrm{seq}^{1-1}_{n+1}(X)$. In this proof, we consider the indices of a_i's and b_i's in modulo $n+1$.

$(\rightarrow)$: Suppose that $a \sim b$. Then there exists $k \in \omega$ such that for all $l \in \omega$, we have $a_l = b_{l+k}$ and so

$$(a_0; \ldots; a_n)(a_l) = a_{l+1} = b_{l+k+1} = (b_0; \ldots; b_n)(b_{l+k}) = (b_0; \ldots; b_n)(a_l).$$

Thus these two permutations are equal.

$(\leftarrow)$: Suppose that $(a_0; \ldots; a_n) = (b_0; \ldots; b_n)$. Then we have

$$(b_0; \ldots; b_n)(a_0) = (a_0; \ldots; a_n)(a_0) = a_1 \neq a_0.$$

Since $(b_0; \dots; b_n)$ moves only elements in the set $\{b_0, \dots, b_n\}$, we conclude that $a_0 = b_k$ for some $k \in \omega$. Hence for any $s \in \omega$, we have

$$a_s = (a_0; \dots; a_n)^s(a_0) = (b_0; \dots; b_n)^s(b_k) = b_{s+k}$$

as desired. □

Next, we shall construct a cyclic permutation from two injective sequences of two disjoint sets.

Definition 4.15. Let X and Y be two disjoint sets and p and q be natural numbers such that $p, q \geq 1$. For each $a = (a_1, \dots, a_p) \in \mathrm{seq}_p^{1-1}(X)$ and $b = (b_1, \dots, b_q) \in \mathrm{seq}_q^{1-1}(Y)$. We define $a^\frown b = (a_1; \dots; a_p; b_1; \dots; b_q)$.

Note that $a^\frown b \in \mathcal{S}_{p+q}(X \cup Y)$.

We shall show that two concatenations give the same permutation if and only if each corresponding "components" are equal.

Lemma 4.16. *Let X and Y be two disjoint sets, $p, q \geq 1$ be natural numbers, $a, a' \in \mathrm{seq}_p^{1-1}(X)$ and $b, b' \in \mathrm{seq}_q^{1-1}(Y)$ be such that $a^\frown b = a'^\frown b'$. Then we have $a = a'$ and $b = b'$.*

Proof. Let $c = a^\frown b = a'^\frown b'$ and $c_X = (c) \cap X$ and $c_Y = (c) \cap Y$. Let $a = (a_1, \dots, a_p), b = (b_1, \dots, b_q), a' = (a'_1, \dots, a'_p)$, and $b' = (b'_1, \dots, b'_q)$. From the construction of $c = a^\frown b = a'^\frown b'$, there exists a unique pair $(c^*, c_*) \in c_X \times c_Y$ such that $(c(c^*), c(c_*)) \in c_Y \times c_X$. Since

$$c(a_p) = b_1, c(a'_p) = b'_1, c(b_q) = a_1, \text{ and } c(b'_q) = a'_1,$$

where $a_p, a'_p, a_1, a'_1 \in c_X$ and $b_1, b'_1, b_q, b'_q \in c_Y$, $a_p = c^* = a'_p$ and $b_q = c_* = b'_q$

Since $c(a_i) = a_{i+1}$ and $c(a'_i) = a'_{i+1}$ for all $1 \leq i < p$ where c is injective, by backward induction on i, we have $a'_i = a_i$ for all $1 \leq i \leq p$. Similarly, we have $b'_j = b_j$ for all $1 \leq j \leq q$. We conclude that $a = a'$ and $b = b'$ as desired. □

Now we are ready for the main theorem.

Theorem 4.17. *For all infinite sets A, $|\mathrm{seq}_n^{1-1}(A)| \leq |\mathcal{S}_{n+1}(A)|$.*

Proof. Let A be an infinite set. By Lemma 4.12, there exists a natural number $K_n \geq 2n+1$ such that for all natural numbers $k < n$,

$$k!\binom{n}{k}\binom{K_n}{k} \leq (k+1)!\binom{K_n}{k+1}.$$

Since $K_n \geq 2n+1$, we also have that $\binom{K_n}{n} \leq \binom{K_n}{n+1}$.

Let $X = \{x_1, x_2, \ldots, x_{K_n}\} \subseteq A$ and for each natural number $k \leq n$, we define

$$A_k = \{(a_1, \ldots, a_n) \in \mathrm{seq}_n^{1-1}(A) \mid |\{a_1, \ldots, a_n\} \cap X| = k\}.$$

It suffices to show that for each natural number $k \leq n$, there exists an injection $f_k \colon A_k \to \mathcal{S}_{n+1}(A)$ where $f_0, \ldots, f_n$ have disjoint images.

First we deal with the case $k = n$. From Lemma 4.14, we have that the map $[(a_0, \ldots, a_n)]_\sim \mapsto (a_0; \ldots; a_n)$ is a well-defined injection and thus $\mathrm{seq}_{n+1}^{1-1}(X)/{\sim} \preceq \mathcal{S}_{n+1}(A)$. Since

$$\begin{aligned}|A_n| = n!\binom{K_n}{n} &\leq n!\binom{K_n}{n+1} \\ &= \frac{1}{n+1}|\mathrm{seq}_{n+1}^{1-1}(X)| = |\mathrm{seq}_{n+1}^{1-1}(X)/{\sim}|,\end{aligned}$$

there exists an injection $f_n \colon A_n \to \mathcal{S}_{n+1}(A)$ as desired.

Now, let $k < n$ be a natural number. We may assume that $0, 1 \notin A$. We start by defining functions i_X, Q_X, and Q'_X from the same domain $\mathrm{seq}_n^{1-1}(A)$ as follows:

$$\begin{aligned} i_X(a_1, \ldots, a_n) &= (\epsilon_1, \ldots, \epsilon_n), \text{ where } \epsilon_j = 1 \text{ if } a_j \in X \text{ and} \\ &\qquad \epsilon_j = 0 \text{ otherwise, for each } 1 \leq j \leq n, \\ Q_X(a_1, \ldots, a_n) &= (a_{i_1}, ..., a_{i_m}) \text{ if } \{a_1, \ldots, a_n\} \cap X = \{a_{i_1}, \ldots, a_{i_m}\}, \\ Q'_X(a_1, \ldots, a_n) &= (a_{j_1}, ..., a_{j_l}) \text{ if } \{a_1, \ldots, a_n\} \setminus X = \{a_{j_1}, \ldots, a_{j_l}\}, \end{aligned}$$

where the indices $i_1, \ldots, i_m$ and $j_1, \ldots, j_l$ are increasing.

Define $B_k = \{i_X(a) \mid a \in A_k\}$. We have that

$$|B_k \times \mathrm{seq}_k^{1-1}(X)| = \binom{n}{k}k!\binom{K_n}{k} \leq (k+1)!\binom{K_n}{k+1} = |\mathrm{seq}_{k+1}^{1-1}(X)|.$$

Hence there exists an injection $h_k \colon B_k \times \mathrm{seq}_k^{1-1}(X) \to \mathrm{seq}_{k+1}^{1-1}(X)$.

Now, we define $f_k \colon A_k \to \mathcal{S}_{n+1}(A)$ by

$$f_k(a) = h_k(i_X(a), Q_X(a))^\frown Q'_X(a).$$

Note that f_k moves exactly $k+1$ elements in X.

To show that f_k is injective, let $a, b \in A_k$ be such that $f_k(a) = f_k(b)$. Then, by Lemma 4.16, $h_k(i_X(a), Q_X(a)) = h_k(i_X(b), Q_X(b))$ and $Q'_X(a) = Q'_X(b)$. Since h_k is injective, $i_X(a) = i_X(b)$ and $Q_X(a) = Q_X(b)$. Therefore we can retrieve the sequence a from the information $Q_X(a), Q'_X(a)$, and $i_X(a)$ as follows:

Change the p^{th} occurrence of 1 in the sequence $i_X(a)$ to $Q_X(a)(p-1)$ for each $1 \leq p \leq k$ and change the q^{th} occurrence of 0 in the sequence $i_X(a)$ to $Q'_X(a)(q-1)$ for each $1 \leq q \leq n-k$. We can see that the resulting sequence is a. Since the values of i_X, Q_X, and Q'_X at a and b are equal, we can conclude that $a = b$. Therefore f_k is injective.

Finally, since for each natural number $m \leq n$ and each $a \in A_m$, $f_m(a)$ moves exactly $m+1$ elements in X, $f_0, \ldots, f_n$ have disjoint images. Thus $\bigcup_{i=0}^{n} f_i \colon \mathrm{seq}_n^{1-1}(A) \to \mathcal{S}_{n+1}(A)$ is an injection. $\square$

Note that the above proof requires the choice of elements $x_1, x_2, \ldots, x_{K_n}$ from A. Thus, in the absence of AC, we cannot make such choices for infinitely many n. Therefore, from the above theorem, we cannot conclude that $|\mathrm{seq}^{1-1}(A)| \leq |A|!$ for any infinite set A. It has been shown in [11, Theorem 3.1] that this statement is not provable in ZF as well.

It is still questionable whether we can obtain a stronger result by replacing $\mathrm{seq}_n^{1-1}(A)$ in Theorem 4.17 by $\mathrm{seq}_n(A)$. Shen and Yuan showed in [9, Corollary 2.23] that for any set A, $|\mathrm{seq}(A)| = |\mathrm{seq}^{1-1}(A)|$ if and only if $A = \emptyset$ or A is Dedekind infinite. For the set of sequences with length n, we also have the following result.

Theorem 4.18. *For any Dedekind infinite set A,*

$$|\mathrm{seq}_n(A)| = |\mathrm{seq}_n^{1-1}(A)|.$$

Proof. Let A be a Dedekind infinite set. Without loss of generality, suppose that $A \cap (n \times n) = \emptyset$. Since there is a canonical bijection from $A \cup (n \times n)$ onto A, it is enough to construct an injection from $\mathrm{seq}_n(A)$ into $\mathrm{seq}_n^{1-1}(A \cup (n \times n))$.

For each $a = (a_0, \ldots, a_{n-1}) \in \mathrm{seq}_n(A)$ and $k < n$, let $B_{a,k} = \{l < k \mid a_l = a_k\}$

and define $f : \mathrm{seq}_n(A) \to \mathrm{seq}_n^{1-1}(A \cup (n \times n))$ by

$$f(a)(k) = \begin{cases} a_k & \text{if } B_{a,k} = \emptyset, \\ (\min B_{a,k}, |B_{a,k}|) & \text{otherwise.} \end{cases}$$

To show that f is injective, let $s, t \in \mathrm{seq}_n(A)$ be distinct sequences. Therefore there exists a least $l < n$ such that $s(l) \neq t(l)$. It is clear that $f(s) \neq f(t)$ if one of $f(s)(l), f(t)(l)$ is in $n \times n$ while the other is not. We are left to deal with two following cases:

Case 1 $f(s)(l), f(t)(l) \in A$.

We have $f(s)(l) = s(l) \neq t(l) = f(t)(l)$. Hence $f(s) \neq f(t)$.

Case 2 $f(s)(l), f(t)(l) \in n \times n$.

The minimality of l implies that $s(k) = t(k)$ for all $k < l$. However, since $s(l) \neq t(l)$, $B_{s,l} \cap B_{t,l} = \emptyset$ and both sets are not empty because $f(s)(l), f(t)(l) \in n \times n$. Therefore $\min B_{s,l}$ and $\min B_{t,l}$, which are the first coordinates of $f(s)(l)$ and $f(t)(l)$ respectively, are not equal.

We conclude that $f(s) \neq f(t)$. Then f is injective, so

$$|\mathrm{seq}_n(A)| \leq |\mathrm{seq}_n^{1-1}(A \cup (n \times n))| = |\mathrm{seq}_n^{1-1}(A)|.$$

However, since $\mathrm{seq}_n^{1-1}(A) \subseteq \mathrm{seq}_n(A)$, we must have that $|\mathrm{seq}_n^{1-1}(A)| = |\mathrm{seq}_n(A)|$ as desired. $\square$

Thus the following corollary follows immediately from Theorems 4.17 and 4.18.

Corollary 4.19. *For all Dedekind infinite sets A, $|\mathrm{seq}_n(A)| \leq |\mathcal{S}_{n+1}(A)|$.*

CHAPTER V
Consistency Results

For relative consistency results, we shall work in permutation models.

First, we use the basic Fraenkel model $\mathcal{V}_{F_0}$. We have shown in Theorem 4.17 that "$|\mathrm{seq}_n^{1-1}(X)| \leq |\mathcal{S}_{n+1}(X)|$ for any infinite set X" is provable in ZF. Now, we show that the subscript $n+1$ cannot be reduced to n. Let A be the set of atoms of $\mathcal{V}_{F_0}$.

Theorem 5.1. $\mathcal{V}_{F_0} \models |\mathrm{seq}_n^{1-1}(A)| \nleq |\mathcal{S}_n(A)|$.

Proof. Assume there is an injection $f\colon \mathrm{seq}_n^{1-1}(A) \to \mathcal{S}_n(A)$ with a support E. Let $M \subseteq A \backslash E$ be such that $|M| = n$ and let $u \in \mathrm{seq}_n^{1-1}(M)$. So $\mathrm{ran}(u) = M$.

Suppose that there is $v \in M \setminus (f(u))$. We select $w \in A \backslash (E \cup (f(u)))$ which is distinct from v and let $\tau = (v; w)$. Since $\tau \in \mathrm{fix}_{\mathcal{G}}(E \cup (f(u)))$,

$$f(u) = \tau f(u) = (\tau f)(\tau u) = f(\tau u)$$

but, since $v \in \mathrm{ran}(u)$, $\tau u \neq u$ whereas f is injective, a contradiction.

Thus $M \subseteq (f(u))$. Since $|M| = n = |(f(u))|$, $M = (f(u))$. Thus $f(s) \restriction M \in \mathcal{S}_n(M)$ for all $s \in \mathrm{seq}_n^{1-1}(M)$. Since f is an injection, $|\mathrm{seq}_n^{1-1}(M)| \leq |\mathcal{S}_n(M)|$ but $|\mathrm{seq}_n^{1-1}(M)| = n! > |\mathcal{S}_n(M)|$, a contradiction. $\square$

Intuitively, among the sets of permutations of a set with finitely many non-fixed points, it seems the size of the set with smaller number of non-fixed points is less than or equal to those with greater numbers. However, in this model, we show that such relation does not generally hold.

Theorem 5.2. $\mathcal{V}_{F_0} \models |\mathcal{S}_n(A)| \nleq |\mathcal{S}_{n+1}(A)|$.

Proof. Suppose there is an injection $f\colon \mathcal{S}_n(A) \to \mathcal{S}_{n+1}(A)$ with a support E such that $|E| \geq n+1$. Let $L = |\mathcal{S}_{n+1}(E)| + 1$, $M_1, \ldots, M_L$ be distinct subsets of $A \backslash E$ with cardinality n, and $\pi_1, \ldots, \pi_L$ be permutations of A such that $(\pi_i) = M_i$ for all $1 \leq i \leq L$.

Let $1 \leq t \leq L$. To show that $(f(\pi_t)) \subseteq E \cup M_t$, suppose to the contrary that there is $y \in (f(\pi_t))$ such that $y \notin E \cup M_t$. Then $y = f(\pi_t)(x)$ for some $x \in A$ such that $x \neq y$.

<u>Case 1</u> $x \in M_t$.

Let $z \in A \backslash (E \cup M_t \cup \{y\})$ and $\sigma = (y; z)$. Then σ fixes $E \cup M_t$ pointwise and so

$$z = \sigma(y) = \sigma(f(\pi_t)(x)) = (\sigma f(\sigma \pi_t))(\sigma x) = f(\pi_t)(x) = y$$

but $y \neq z$.

<u>Case 2</u> $x \in A \setminus M_t$.

Since $|M_t| = n$, $|(f(\pi_t))| = n+1$, and $x, y \in (f(\pi_t)) \setminus M_t$, there exists $r \in M_t$ such that $f(\pi_t)$ fixes r. Let $s \in A \backslash (E \cup M_t \cup (f(\pi_t)))$ and $\tau = (r; s)$. Then τ fixes E and $f(\pi_t)$ fixes $\{r, s\}$ pointwise. Hence

$$f(\pi_t) = \tau f(\pi_t) = (\tau f)(\tau \pi_t) = f(\tau \pi_t)$$

but $\tau \pi_t \neq \pi_t$ whereas f is an injection.

Therefore, $(f(\pi_t)) \subseteq E \cup M_t$. Since $|\{f(\pi_i) \mid i \in \{1, \ldots, L\}\}| = L > |\mathcal{S}_{n+1}(E)|$, there exists $s \in \{1, \ldots, L\}$ such that $f(\pi_s) \restriction_E \notin \mathcal{S}_{n+1}(E)$. Hence, since $|M_s| = n < n+1 = |(f(\pi_s))|$, there exists $w \in M_s$ such that $f(\pi_s)(w) \in E$. Since π_s fixes E pointwise and $\pi\pi = \pi$ for all $\pi \in \mathrm{fix}_{\mathcal{G}}(E)$, we have

$$f(\pi_s)(w) = \pi_s(f(\pi_s)(w)) = (\pi_s f)(\pi_s \pi_s)(\pi_s w) = f(\pi_s)(\pi_s w)$$

but $\pi_s(w) \neq w$ whereas $f(\pi_s)$ is injective, a contradiction. $\square$

It follows from Theorems 4.3 and 4.17 that $\mathrm{AC}_{\leq n}$ implies $|\mathcal{S}_n(X)| \leq |\mathcal{S}_{n+1}(X)|$ for any infinite set X. The above theorem tells us that, in the absence of $\mathrm{AC}_{\leq n}$, "$|\mathcal{S}_n(X)| \leq |\mathcal{S}_{n+1}(X)|$ for any infinite set X" may fail. Since this statement is not provable in ZF, this condition in Theorem 4.3 cannot be removed as well. However, we shall give a model in which $|\mathcal{S}_n(X)| \nleq |\mathrm{seq}_n(X)|$ for some infinite set X by modifying the second Fraenkel model as follows:

Let the set of atoms $A = \bigcup\{P_m | m \in \omega\}$ where $|P_m| = n$ for all $m \in \omega$ and all P_m's are mutually disjoint. Let $\mathcal{G}$ be the group of all permutation of A which fix each P_m setwise, i.e, $\pi[P_m] = P_m$ for all $m \in \omega$. Let $\mathcal{V}_{F_n}$ be the permutation model induced by the normal ideal $\mathrm{fin}(A)$.

Theorem 5.3. $\mathcal{V}_{F_n} \models |\mathcal{S}_n(A)| \nleq |\mathrm{seq}_n(A)|$.

Proof. Assume there is an injection $f\colon \mathcal{S}_n(A) \to \mathrm{seq}_n(A)$ with a support $E = \bigcup\{P_m \mid m \leq k\}$. Let ψ be a permutation of A such that $(\psi) = P_l$ for some $l > k$. Suppose $f(\psi)(i) \notin E$ for some $i < n$. Then $f(\psi)(i) \in P_t$ for some $t > k$. Let π_t be a permutation of A such that $(\pi_t) = P_t$ and if $t = l$, let $\pi_t = \psi$. Then $\pi_t\psi = \psi$ and $\pi_t \in \mathrm{fix}_{\mathcal{G}}(E)$. Hence

$$\pi_t(f(\psi)(i)) = (\pi_t f)(\pi_t\psi)(i) = f(\psi)(i)$$

but π_t moves all elements of P_t, a contradiction.

Therefore each entry of $f(\psi)$ must be in E. This leads to a contradiction since $\mathrm{seq}_n(E)$ is finite but $\{f(\chi) \mid \chi \in \mathcal{S}_n(A)$ and $(\chi) = P_r$ for some $r > k\}$ is infinite whereas f is injective. □

Actually, the statement in the above theorem also hold in $\mathcal{V}_{F_0}$ as shown below.

Theorem 5.4. $\mathcal{V}_{F_0} \models |\mathcal{S}_n(A)| \nleq |\mathrm{seq}_n(A)|$.

Proof. Assume there is an injection $f\colon \mathcal{S}_n(A) \to \mathrm{seq}_n(A)$ with a support E. Let $\pi \in \mathcal{S}_n(A \backslash E)$. Suppose to the contrary that there is $x \in (\pi) \setminus \mathrm{ran}(f(\pi))$. We select $y \in A\backslash(E \cup (\pi) \cup \mathrm{ran}(f(\pi)))$ which is distinct from x and let $\tau = (x; y)$. Since $\tau \in \mathrm{fix}_{\mathcal{G}}(E \cup \mathrm{ran}(f(\pi)))$, $f(\pi) = \tau f(\pi) = (\tau f)(\tau\pi) = f(\tau\pi)$ but $\tau\pi \neq \pi$ whereas f is injective, a contradiction. Thus $(\pi) \subseteq \mathrm{ran}(f(\pi))$. Since $|(\pi)| = n \geq |\mathrm{ran}(f(\pi))|$, $(\pi) = \mathrm{ran}(f(\pi))$. Thus $f(\pi) \in \mathrm{seq}_n^{1-1}((\pi))$. Since $\pi \in \mathrm{fix}_{\mathcal{G}}(E)$ and $\pi\pi = \pi$ for all $\pi \in \mathrm{fix}_{\mathcal{G}}(E)$, $\pi(f(\pi)) = (\pi f)(\pi\pi) = f(\pi)$ but $\pi(f(\pi)) \neq f(\pi)$ because the first entry of $f(\pi)$ must be moved by π, a contradiction. □

The result from all theorems in this section can be transferred to ZF by using the Jech-Sochor First Embedding Theorem (cf. [8, Theorem 6.1]). For example, from Theorem 5.3, we have that "$\exists X(|\mathcal{S}_n(X)| \nleq |\text{seq}_n(X)|)$" holds in $\mathcal{V}_{F_n}$. Let $\phi(X)$ be a formula which represent "$|\mathcal{S}_n(X)| \nleq |\text{seq}_n(X)|$", i.e. "$\forall f(f : \mathcal{S}_n(X) \to \text{seq}_n(X)$ is not injective)". We can see that $\mathcal{V} \models \phi(X) \leftrightarrow \phi^{\mathcal{P}^{n+5}(X)}(X)$. Hence $\phi(X)$ is boundable, and so is the statement "$\exists X(|\mathcal{S}_n(X)| \nleq |\text{seq}_n(X)|)$". Therefore this statement is consistent with ZF. The results from Theorem 5.1 and 5.2 can be transferred to ZF in a similar way.

It is known that AC_n fails in $\mathcal{V}_{F_0}$ (cf. [7, page 177]). Obviously, AC_n fails in $\mathcal{V}_{F_n}$ as well since the set of atoms of this models is Dedekind finite in the model. Since $\text{AC}_{\leq n}$ implies AC_n, $\text{AC}_{\leq n}$ fails in these models too. This fact also follows from Theorem 4.3 and 5.3.

CHAPTER VI
Conclusion

In conclusion, our main results in ZF together with related consistency results are listed below.

1. $\mathrm{AC}_{\leq n}$ implies that $|\mathcal{S}_n(A)| \leq |\mathrm{seq}_n^{1-1}(A)|$ for every infinite set A and the assumption can be weakened to AC_n for $n \leq 3$ but $\mathcal{V}_{F_0} \models \exists A(|\mathcal{S}_n(A)| \nleq |\mathrm{seq}_n(A)|)$ (Theorems 4.3 and 5.4 and Corollary 4.4).

2. For all infinite ordinals α, $\mathcal{S}_n(\alpha) \approx \mathcal{S}_{n+1}(\alpha)$ but $\mathcal{V}_{F_0} \models \exists A(|\mathcal{S}_n(A)| \nleq |\mathcal{S}_{n+1}(A)|)$ (Theorems 4.10 and 5.2).

3. For all infinite sets A, $|\mathrm{seq}_n^{1-1}(A)| \leq |\mathcal{S}_{n+1}(A)|$ but $\mathcal{V}_{F_0} \models \exists A(|\mathrm{seq}_n^{1-1}(A)| \nleq |\mathcal{S}_n(A)|)$ (Theorems 4.17 and 5.1).

However, there are some problems left unsolved. For example,

1. Can $\mathrm{AC}_{\leq n}$ in the statement of Theorem 4.3 be replaced by some other weak forms of AC, in particular, some weaker one?

2. Can the condition "A is Dedekind-infinite" in Theorem 4.19 be weaken?

3. Can Theorem 5.2 be generalized to "$\mathcal{V}_{F_0} \models \forall m > n(|\mathcal{S}_n(A)| \nleq |\mathcal{S}_m(A)|)$"?

These problems are left open for further research.

BIBLIOGRAPHY

[1] N. Aksornthong and P. Vejjajiva, Relations between cardinalities of the finite sequences and the finite subsets of a set, *Math. Logic Quart.*, **64** (2018), 529–534.

[2] J. Dawson, Jr. and P. Howard, Factorials of infinite cardinals, *Fund. Math.*, **93** (1976), 185–195.

[3] H.B. Enderton, *Elements of Set Theory*, 1st edn, Academic Press, 1977.

[4] L. Halbeisen, *Combinatorial Set Theory: With a Gentle Introduction to Forcing*, 2nd edn, Springer Monographs in Mathematics, Springer, Cham, 2017.

[5] L. Halbeisen and S. Shelah, Consequences of arithmetic for set theory, *J. Symb. Log.*, **59** (1994), 30–40.

[6] ————, Relations between some cardinals in the absence of the axiom of choice, *Bull. Symb. Log.*, **7** (2001), 237–261.

[7] P. Howard and J.E. Rubin, *Consequences of the Axiom of Choice*, Mathematical Surveys and Monographs 59, Americam Mathematical Society, Providence, RI, 1998.

[8] T. Jech, *The Axiom of Choice*, Studies in Logic and the Foundations of Mathematics, vol. 75, North-Holland, Amsterdam, 1973.

[9] G. Shen and J. Yuan, Factorials of infinite cardinals in ZF Part I: ZF results, *J. Symb. Log.*, **85** (2020), 224–243.

[10] N. Sonpanow and P. Vejjajiva, Some properties of infinite factorials, *Math. Logic Quart.*, **64** (2018), 201–206.

[11] ————, Factorials and the finite sequences of sets, *Math. Logic Quart.*, **65** (2019), 116–120.

[12] E. Specker, Zur Axiomatik der Mengenlehre (Fundierungs- und Auswahlaxiom), *Z. Math. Log. Grundlagen Math.*, **3** (1957), 173–210.

VITA

Name	Mr. Jukkrid Nuntasri
Date of Birth	April 21, 1998
Place of Birth	Phang-Nga, Thailand
Education	B.Sc. (Mathematics) 1st class honour, Chulalongkorn University, 2020
Awards	Bronze medal from the 8$^{\text{th}}$ Thailand Mathematical Olympiad
	Gold medal from the 9$^{\text{th}}$ Thailand Mathematical Olympiad (1$^{\text{st}}$ prize)