文章编号:1007-5321(2019)05-0001-07 DOI:10.13190/j.jbupt.2019-001

选择公理与 Tukey 引理等价性的机器证明

孙天宇, 郁文生
(北京邮电大学 天地互联与融合北京市重点实验室, 北京 100876)

摘要: 基于计算机证明辅助工具 Coq,提出一种选择公理与 Tukey 引理等价性的形式化证明. 在公理化集合论形式化系统基础上,给出选择公理与 Tukey 引理的形式化描述,这是 Tukey 引理的首次形式化. 完成了选择公理与 Tukey 引理等价性的证明代码,并在 Coq 中通过验证. 体现了基于 Coq 的数学定理机器证明具有可读性和交互性的特点,其证明过程规范、严谨、可靠,在集合论、拓扑学和代数学的形式化构建中具有重要应用.

关 键 词: 机器证明; 形式化数学; 选择公理; Tukey 引理
中图分类号: TN929.53 **文献标志码**: A

A Mechanized Proof of Equivalence Between the Axiom of Choice and Tukey's Lemma

SUN Tian-yu, YU Wen-sheng
(Beijing Key Laboratory of Space-Ground Interconnection and Convergence, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: On the basis of the computer proof assistant Coq, a formal proof of the equivalence between the axiom of choice and Tukey's lemma is presented. The formal description of axiom of choice and Tukey lemma was given based on the "axiomatic set theory" formal system, which was the first formalization of Tukey's lemma. A complete proof code of the equivalence between the axiom of choice and Tukey's lemma was completed. All the proofs were formally checked in Coq. The formal proof demonstrated that the Coq-based mechanized proof of mathematics theorem had the characteristics of readability and interactivity. The proof process was standardized, rigorous and reliable. This formal work has important applications in many fields of formal mathematics, especially in set theory, topology and algebra.

Key words: mechanized proof; formal mathematics; axiom of choice; Tukey's lemma

人工智能研究是国家当前重大科技发展战略之一,夯实人工智能基础理论尤为重要,数学定理机器证明是人工智能基础理论的深刻体现.

选择公理是集合论里有关映射存在性的一条公理,最早于 1904 年由 Zermelo 提出,并用于对良序原则的证明[1-2]. 选择公理在现代数学中有很重要的作用,与许多深刻的数学结论有着十分密切的联系. 没有选择公理,甚至无法确定 2 个集合能否比较元素的多少、非空集的积是否非空、线性空间是否一定有一组基、环是否一定有极大理想等. 选择公理有多个等价定理,Tukey 引理是其常见和重要的一种. 通过 Tukey 引理容易证明 Hausdorff 极大原则、极大元则、Zermelo 假定、Zorn 引理、良序定理等与选择公理等价的著名定理. 拓扑学中重要的 Ty-

收稿日期: 2019-01-19
基金项目: 国家自然科学基金项目(61571064, 61936008)
作者简介: 孙天宇(1993—), 男, 博士生, E-mail: stycyj@bupt.edu.cn; 郁文生(1967—), 男, 教授, 博士生导师.

chonoff 乘积定理同样依赖于 Tukey 引理,这是选择公理较为深刻的一个应用.

近年来数学定理形式化证明的研究,随着计算机科学的迅猛发展,特别是交互式定理证明辅助工具 Coq[3]、Isabelle、HOL Light 等的出现,取得了长足的进展. 国际计算机专家 Gonthier[4] 成功基于 Coq 给出了著名的"四色定理"的计算机证明,进而,Gonthier 等又经过6年努力,于2012年完成对有限单群分类定理的机器验证(该证明过程约有4 200个定义和1.5万条定理,约17万行的 Coq 代码)[5],使得证明辅助工具 Coq 在学术界的影响日益增强. Wiedijk 指出全球各相关研究团队已经或计划完成包括 Gödel 不完全性定理、Jordan 曲线定理、素数定理以及 Fermat 大定理等在内的100个著名数学定理的计算机形式化证明,目前已经完成其中93个定理的形式化证明[6].

笔者在"公理化集合论"形式化系统基础上,通过调用该系统中的一些基本公理、定义和定理,给出选择公理与 Tukey 引理等价性的机器证明. 创新研究在于利用交互式定理证明工具 Coq,给出纯计算机形式化证明,体现了基于 Coq 的数学定理机器证明所具有的可读性、交互性和智能性等特点,机器证明的过程规范、严谨、可靠.

1 "公理化集合论"形式化系统

19世纪末和20世纪初,朴素集论中一些悖论的发现,使集合论之公理化研究成为必要. 公理化集合论的出发点就是给出一组集合应该满足的公理,在此基础上研究集合的性质. 集合论里普遍采用的公理体系是 ZFC 体系,它由策梅洛-弗兰克尔(ZF, Zermelo-Fraenkel)集合论公理化体系加上选择公理(AC, axiom of choice)构成. 其他著名的公理化集合理论有冯·诺伊曼-博内斯-哥德尔(NBG, von Neumann-Bernays-Gödel)集合论和摩斯-凯利(MK, Morse-Kelley)集合论[2].

"公理化集合论"形式化系统是基于 MK 集合论公理化体系搭建的. MK 集合论公理化体系最早在1949年由王浩提出[7],1955年在 Kelley 的《一般拓扑学》中正式发表[8],此后在1965年由 Morse 完善. 该公理系统构造了序数和基数,定义了非负整数,并把 Peano 公设当做定理给予了证明,在此基础上实数也可以由"整数类是一个集"和"利用归纳法在整数上定义一个函数是可能的"这两点事实以及 Peano 公设和无限性公理来构造. 该公理化系统可用来迅速而又自然地给出一个数学基础,摆脱了集合论中较明显的悖论. 由此,有限的公理体系被遗弃,而把整个理论建筑在8个公理和1个公理图示之上. 该公理体系相当于承认存在比集合更广之类,与 ZF 公理化系统无矛盾.

"公理化集合论"形式化系统已经完成对 MK 集合论公理化体系的 Coq 形式化,包括8个公理和1个公理图示的形式化描述以及全部181条定义或定理的形式化描述或证明. 完整的代码可见文献[9]. Tukey 引理是"公理化集合论"形式化系统的一个重要应用. 在该系统的基础上,现代数学主体的拓扑学和近世代数等理论可以快速地形式化构建.

下面介绍一些"公理化集合论"系统中的基本概念. 首先,定义一个在系统中描述集合和元素的概念"类". 在 Coq 形式化中选择一般类型"Type"表示,其形式化定义如下:

```
Parameter Class: Type.
```

本系统除了"="和基本逻辑概念之外,定义2个基本的常项. 第1个是"∈",它读作"属于". 因为在本系统中不区分集合与元素的类型,统一用 Class 来表示. 因此"∈"的形式化定义如下:

```
Parameter In: Class → Class → Prop.
```

第2个常项是分类"{…:…}",读作"{所有…的集使得…}",其形式化定义如下:

```
Parameter Classifier:(Class→Prop)→Class.
```

通过"Notation"命令可以在 Coq 中添加数学符号,增强代码可读性.

```
Notation"\{ P \}" := (Classifier P) (at level 0).
```

在集合描述性定义基础上,引入分类公理图示,可避免明显的悖论,Coq 形式化如下:

集 x 为一集当且仅当对于某一 y,x 属于 y.

```
Definition Ensemble x: = exists y, In x y.
```

公理1(分类公理图式) 对于每一个 β,$\beta\in\{\alpha: P(\alpha)\}$ 的充分必要条件是"β 是集"和 $P(\beta)$,这里 $P(\cdot)$ 是适定的公式.

```
Axiom AxiomS:forall b (P: Class → Prop),
In b\{P\} ↔ Ensemble b /\ (P b).
```

"公理化集合论"系统中共有8条公理,下面以外延公理为例展示如何在该系统中形式化描述公理.

公理2(外延公理) 对于每个 x 与 y,$x=y$ 成

立之充要条件就是对每一个 z 当且仅当 $z \in x$ 时，$z \in y$.

```
Axiom Axiom_Extent : forall x y,
    x = y ↔ (forall z, In z x ↔ In z y)
```

表 1 列出了该系统中一些重要概念的 Coq 定义、数学定义和数学符号.

表 1　“公理化集合论”系统重要概念

Coq 定义	数学定义	数学符号
Union x y	x 与 y 的并	$x \cup y$
Intersection x y	x 与 y 的交	$x \cap y$
$x \sim y$	x 与 y 的差	$x \sim y$
Empty	空类	$\varnothing$
Full	全域	μ
\cup x	x 元的并	$\cup x$
\cap x	x 元的交	$\cap x$
Subclass x y	y 包含 x	$x \subset y$
PSubclass x y	y 真包含 x	$x \subsetneq y$
pow(x)	x 的幂集	2^x
[x]	x 的单点集	$\{x\}$
[x|y]	无序偶	$\{x\ y\}$
[x,y]	有序偶	(x,y)
Function f	f 是一个函数	f
dom(f)	f 的定义域	domain(f)
ran(f)	f 的值域	range(f)
f[x]	f 在 x 处的值	$f(x)$
$x * y$	笛卡儿积	$x \times y$

为了形式化的完整性和独立性，笔者使用的集合论是“公理化集合论”系统的简化和修改版，其包含了系统中的 8 条公理、40 个定义和 50 个定理.

2　基本定义

首先给出选择函数的定义，在其基础上可以完成选择公理的形式化.

定义 1（选择函数）　设 X 是一个集合，记 $\widetilde{X}$ 为由 X 的所有非空子集构成的集族. 称函数 $f:\widetilde{X} \to X$（f 的定义域为 $\widetilde{X}$，f 的值域为 X 的子集）为 X 的一个选择函数，如果它满足条件：对于任意 $A \in \widetilde{X}$，有 $f(A) \in A$.

```
Definition Choice_Function X f: Prop: =
    Function f /\ dom(f) = pow(X) ~ [Empty]
    /\Subclass ran(f) X /\(forall A, In A dom(f)
    → In f[A] A).
```

下面给出极大成员、套、有限特征集的定义，这些定义将在 Tukey 引理的描述和证明中使用.

定义 2（极大成员）　设 $\mathscr{F}$ 是一个集族，F 是 $\mathscr{F}$ 的一个成员. 如果 $\mathscr{F}$ 中没有任何成员以 F 为真子集，则称 F 为 $\mathscr{F}$ 的一个极大成员.

```
Definition MaxMember F f : Prop : =
    f < > Empty → In F f /\ (forall E: Class,
    In E f → ~ (PSubclass F E)).
```

定义 3（套）　设 $\mathscr{F}$ 是一个集族，如果对于任意 $A, B \in \mathscr{F}$ 有 $A \subset B$ 或者 $B \subset A$，则称 $\mathscr{F}$ 为一个套.

```
Definition Nest f: Prop : =
    forall A B: Class, In A f /\ In B f →
    Subclass A B \/ Subclass B A.
```

定义 4（有限特征集）　设 $\mathscr{F}$ 是一个集族. 如果 F 是 $\mathscr{F}$ 的一个成员当且仅当 F 的每一个有限子集都是 $\mathscr{F}$ 的成员，则称 $\mathscr{F}$ 是一个具有有限特征的集族.

```
Definition FiniteSet f : Prop : =
    Ensemble f /\ (forall F, In F f →
    (forall z, Subclass z F /\ Finite z →
    In z f)) /\ (forall F, Ensemble F /\
    (forall z, Subclass z F /\ Finite z →
    In z f) → In F f).
```

3　Tukey 引理形式化证明

3.1　选择公理及相关公式

选择公理可以通过选择函数定义，其具体概念及形式化描述如下.

选择公理　任何一个集合都有一个选择函数.

```
Axiom Choice_Axiom : forall (X: Class),
    Ensemble X →exists ε: Class,
    Choice_Function ε X.
```

Tukey 引理是与选择公理相关的重要定理. Tukey 引理的描述和形式化表达如下.

Tukey 引理　非空的具有有限特征的集族中必有极大成员.

```
Theorem Tukey : forall (f: Class),
    FiniteSet f /\ f < > Empty → exists x,
    MaxMember x f.
```

假设 $\mathscr{F}$ 为一个非空的具有有限特征的集族，因此 $X = \cup\mathscr{F}$ 是一个集合. 根据选择公理，X 有选择函数 $\varepsilon:\widetilde{X} \to X$ 使得对于任意 $A \in \widetilde{X}$，$\varepsilon(A) \in A$. 其中 $\widetilde{X}$ 为 X 的所有非空子集构成的集族. 对每一个 $F \in \mathscr{F}$，

构造一个更大的集合 $\hat{F}$ 为

$$\hat{F}=\{x:x\in X\wedge F\cup\{x\}\in\mathscr{F}\} \tag{1}$$

对集合 $\hat{F}$ 的形式化定义记作 Ex_F,以该公式为例,本文中的公式都已在 Coq 中形式化定义,具体如下:

```
Definition Ex_F (F f: Class) : Class : =
  \{fun x = > In x (\cup f) /\ In (Union
  F[x]) f \}.
```

这里简单介绍一下之前定义的 Classifier 的使用方法. Classifier 的输入项为 Class→Prop 类型. 第1个参数 Class 代表分类中的变量,第2个参数 Prop 表示该变量满足的公式. λ 演算的性质刚好能满足上述要求,在 Coq 中使用 fun 函数来实现.

根据集合 $\hat{F}$ 的定义可知,$F\subset\hat{F}$ 或者 $F=\hat{F}$. 因此根据 $\hat{F}$ 定义一个函数 $\chi:\mathscr{F}\to\mathscr{F}$,该函数的具体描述为

$$\chi(F)=\begin{cases}F\cup\{\varepsilon(\hat{F}-F)\}, & \hat{F}-F\neq\varnothing\\ F, & \hat{F}-F=\varnothing\end{cases} \tag{2}$$

对此函数的 Coq 形式化分为3部分完成:

1) 首先定义一个判定函数 eq_dec,该函数对任意类型为 Type 的变量都满足. 定义中会使用 Coq 库中的 sumbool 函数,

```
Inductive sumbool (P1 P2: Prop) : Set : =
  |left: P1 → {P1} + {P2}
  |right: P2 → {P1} + {P2}
```

通过构造子 left 和 right 可以直接得到 P1 和 P2. 函数 eq_dec 的形式化定义如下:

```
Definition eq_dec (A: Type): Prop : =
  forall x y: A, {x = y} + {x 〈〉 y}.
```

2) 将特定类型 Class 作为函数 eq_dec 中变元的类型,从而得到新的函数 beq:

```
Parameter beq:eq_dec Class.
```

3) 在函数 beq 的基础上定义函数 Fun_X. 在 Coq 中通过模式匹配定义,具体实现如下:

```
Definition Fun_X F f ε: Class : =
  match beq ((En_F' F f) ~ F) Empty with
  | left _ = > F
  | right _ = > Union F [ε[(En_F' F f) ~F]]
  end.
```

通过该函数的定义,将 Tukey 引理的证明目标转化为是否存在一个 $\mathscr{F}$ 中的元 F,使得 $\chi(F)=F$. 下面在函数 χ 的基础上定义 t-子集.

定义 5(t-子集) f 是 $\mathscr{F}$ 的 t-子集,当且仅当 f 是 $\mathscr{F}$ 的子集并且满足条件:

1) $\varnothing\in f$;

2) 若 $F\in f$,则 $\chi(F)\in f$;

3) 若 φ 为 f 中的套,则 $\cup\varphi\in f$.

在 Coq 中对 t-子集的形式化定义如下:

```
Definition tSubclass g f ε : Prop: =
  Subclass g f /\ In Empty g /\ (forall F,
  In F g →In (Fun_X F f ε) g)/\(forall L,
  Subclass L g /\ Nest L → In (\cup L) g).
```

下面通过上述 t-子集的定义构造一些特殊集合,令 f_0 为 $\mathscr{F}$ 中所有 t-子集的交,

$$f_0=\cap\{f:\mathrm{tSubclass}\ f\ \mathscr{F}\varepsilon\} \tag{3}$$

若证明了 f_0 是一个套,即可证明 Tukey 引理. 对于每一个 $C\in f_0$,都可以构建一个套,并且使得 C 为该套中的元素:

$$u(C)=\{A:A\in f_0\wedge(A\subset C\vee C\subset A)\} \tag{4}$$

通过式(3)和式(4)可以构建 f_0 中的套 f_1:

$$f_1=\{C:C\in f_0\wedge(u(C)=f_0)\} \tag{5}$$

为了验证 f_1 满足 t-子集定义中的条件(2),对于每一个 $D\in f_1$,如下构造集合 $v(D)$. 只要证明 $v(D)$ 是一个 t-子集,即可完成全部证明.

$$v(D)=\{A:A\in f_0\wedge(A\subset D\vee\chi(D)\subset A)\} \tag{6}$$

上述公式的 Coq 形式化如下:

```
Definition En_f0 (f ε : Class) : Class : =
  \cap \{ fun g = > tSubclass g f ε \}.
Definition En_u C (f ε : Class) : Class : =
  \{ fun A = > In A (En_f0 f ε) /\
  (Subclass A C \/ Subclass C A) \}.
Definition En_f1 (f ε : Class) : Class : =
  \{ fun C = > In C (En_f0 f ε) /\
  (En_u C f ε) = (En_f0 f ε) \}.
Definition En_v D (f ε : Class) : Class : =
  \{ fun A = > In A (En_f'0 f ε) /\
  (Subclass A D\/Subclass(Fun_X D f ε)A)\}.
```

另外,容易证明关于 f_0 和函数 χ 的2个性质,二者均已在证明工具 Coq 中完成形式化验证,它们将在后面的定理证明中反复使用. 性质的具体描述和 Coq 形式化定义如下.

性质 1 有限特征集合 $\mathscr{F}$ 中的任意元素 F 都包含于 $\chi(F)$.

```
Lemma Property_x : forall (ε F f: Class),
  Choice_Function ε (\cup f)→ In F f →
  Subclass F (Fun_X F f ε).
```

性质 2 f_0 是 $\mathscr{F}$ 最小的一个 t-子集,亦即若 f 为

一个 t-子集，则 $f_0 \subset f$.

```
Lemma Property_f0 : forall (f ε : Class),
  FiniteSet f /\ f <> Empty →
  Choice_Function ε (\cup f) →
  tSubclass (En_f0 f c) f c /\ (forall g,
  Subclass g f /\ tSubclass g f ε →
  Subclass (En_f0 f ε) g).
```

下面将分 5 步完成 Tukey 引理的证明. 前 3 步证明了 f_0 是一个套. 第 4 步证明了当 $F = \cup f_0$ 时，$\chi(F) = F$. 最后，根据前 4 步证明的引理在第 5 步中证明 Tukey 引理.

3.2　预备引理证明

首先介绍证明中前四步证明的引理. 第 1 步通过之前的定义和性质证明引理 1.

引理 1　如果 D 是集合 f_1 中的一个元素，则 $v(D)$ 是非空有限特征集 $\mathscr{F}$ 的一个 t-子集.

在形式化过程中，当调用 t-子集的形式化定义时，必须声明参数 ε. 因此在引理的条件中加入 ε 是 $\cup\mathscr{F}$ 的选择函数. 具体描述如下：

```
Lemma LemmaT1 : forall (f ε : Class),
  FiniteSet f /\ f <> Empty →
  Choice_Function ε (\cup f) → (forall D,
  In D (En_f1 f ε) → tSubclass (En_v D f
  ε) f ε).
```

证明　首先根据式(6)中 $v(D)$ 的定义以及性质 2 可以得到 $v(D) \subset \mathscr{F}$. 因此对于任意 $A \in v(D)$ 有 $A \in \mathscr{F}$. 此结论将在后面的证明中反复使用. 通过性质 2 可以证明 f_0 是 $\mathscr{F}$ 的一个 t-子集. 下面逐步验证 $v(D)$ 满足 t-子集的 3 个条件.

1) 显然，根据式(6)可知 $\varnothing \in v(D)$.

2) 第 2 步验证：若 $A \in v(D)$，则 $\chi(A) \in v(D)$. 分为 3 种情形讨论：

① $A \subset D$，$A \neq D$ 证明这是必有 $\chi(A) \subset D$. 这里采用反证法证明，首先假设 $\chi(A) \subset D$ 是错的. 由于 $D \in f_1$，那么可以证明 D 是 $\chi(A)$ 的真子集. 因此 $\chi(A)$ 比 A 多两点，矛盾. 于是 $\chi(A) \subset \chi(D)$，从而可以证明 $\chi(A) \in v(D)$.

② $A = D$. 此时可以证明 $\chi(A) = \chi(D)$. 因为 $\chi(D) \in v(D)$ 是显然的，所以 $\chi(A) \in v(D)$.

③ $\chi(D) \subset A$. 由于在性质 1 的基础上可证明 $A \subset \chi(A)$，所以 $\chi(D) \subset \chi(A)$，从而 $\chi(A) \in v(D)$.

3) 若 φ 是 $v(D)$ 中的一个套. 由式(6)中 $v(D)$ 的定义可知要讨论 2 种情况. 首先，如果 φ 的每一个成员都包含于 D，则 $\cup\varphi \subset D$；如果 φ 中有一个成员包含 $\chi(D)$，则 $\chi(D) \subset \cup\varphi$. 又因为 f_0 是 t-子集，$\cup\varphi \in f_0$. 于是按 $v(D)$ 的定义，有 $\cup\varphi \in v(D)$. 至此引理 1 证明完毕.

引理 1 证明了 $v(D)$ 是 $\mathscr{F}$ 的一个 t-子集. 第 2 步将通过引理 1 证明 f_1 满足 t-子集定义中的条件 2). 具体描述如下.

引理 2　如果 D 是集合 f_1 中的一个元，则 $\chi(D)$ 同样是 f_1 中的一个元.

```
Lemma LemmaT2 : forall (f ε : Class),
  FiniteSet f /\ f <> Empty →
  Choice_Function ε (\cup f) → (forall D,
  In D (En_f1 f ε)→ In (Fun_X D f ε)
  (En_f1 f ε)).
```

证明　根据式(4)和式(6)，显然可以得到 $v(D) \subset u(\chi(D))$. 由引理 1 可知 $v(D)$ 是 $\mathscr{F}$ 的一个 t-子集，又根据性质 2 可知 f_0 是最小的 t-子集. 因此对于每一个 $D \in f_1$，$u(\chi(D)) = f_0$，即 $\chi(D) \in f_1$. 这也就是说 f_1 满足 t-子集条件 2).

接下来第 3 步通过引理 2 证明 f_0 是一个套，即引理 3. 该引理的具体描述和 Coq 形式化描述如下.

引理 3　如果 $\mathscr{F}$ 为一个非空的具有有限特征的集族，ε 是 $\cup\mathscr{F}$ 的选择函数，则 f_0 是一个套.

```
Lemma LemmaT3 : forall (f ε : Class),
  FiniteSet f /\ f <> Empty →
  Choice_Function ε (\cup f) →
  Nest (En_f0 f ε).
```

证明　根据式(5)中 f_1 的定义，显然 f_1 是 f_0 中的一个套. 由于 f_0 是最小的 t-子集，假如证明了 f_1 是一个 t-子集，那么便有 $f_0 = f_1$. 于是 f_0 便是一个套，也就完成了引理 3 的证明. 下面根据定义 5 证明 f_1 是一个 t-子集. 空类属于 f_1 是显然的. 又引理 2 证明了 f_1 满足条件 2)，下面验证 f_1 满足条件 3)：设 φ 为 f_1 中的一个套，任意 $A \in f_0$，如果所有 φ 中成员都包含于 A，则 $\cup\varphi \subset A$；如果 φ 中有一个成员包含 A，则 $A \cup \subset \varphi$. 因此可以证明 $u(\cup\varphi) = f_0$，这也就是 $\cup\varphi \in f_1$. 综上，当 $\mathscr{F}$ 为一个非空有限特征集族且 ε 是 $\cup\mathscr{F}$ 的选择函数时，f_0 是一个套.

在证明了 f_0 是一个套之后，第 4 步证明存在某一元 $F \in \mathscr{F}$ 使得 $\chi(F) = F$，具体引理描述及 Coq 形式化描述如下所示：

引理 4　$\cup f_0$ 是 $\mathscr{F}$ 中的一个元并且 $\chi(\cup f_0) = \cup f_0$.

```
Lemma LemmaT4: forall (f ε : Class),
  FiniteSet f /\ f <> Empty →
  Choice_Function ε (\cup f) →
  In (\cup (En_f0 f ε)) f /\
  (Fun_x (\cup (En_f0 f ε)) f ε) =
  \cup (En_f0 f ε).
```

证明 令 $F=\cup f_0$,根据之前证明的性质1可得 $F\subset\chi(F)$. 由性质2可知 f_0 是一个t-子集,显然 $f_0\subset f_0$. 又根据引理3,f_0 是一个套. 因此 F 是 $\mathscr{T}$ 中的一个元. 下面证明 $\chi(F)=F$,根据t-子集定义中的条件2)和3)可得 $F\in f_0$ 和 $F\in\chi(F)$. 于是 $\chi(F)\subset F$,从而 $\chi(F)=F$,引理得证.

3.3 Tukey引理证明

最后证明的第5步通过引理4证明Tukey引理,也就是证明非空的具有有限特征的集族必有极大成员. 具体证明过程如下.

证明 根据之前的假设定义,$\mathscr{T}$ 为一个非空的具有有限特征的集族. 根据选择公理,$X=\cup\mathscr{T}$ 有选择函数 $\varepsilon:\widetilde{X}\to X$ 使得对于任意 $A\in\widetilde{X}$,$\varepsilon(A)\in A$. 由引理4可证明存在一个元 $F=\cup f_0$ 使得 $\chi(F)=F$. 因此根据式(2)中函数的定义,可证明 $F=\hat{F}$,从而 F 是集合 $\mathscr{T}$ 的极大值,定理得证. 至此,Tukey引理全部证明完毕.

4 选择公理形式化证明

第3节中将选择公理看作一条公理证明了Tukey引理. 本节将选择公理作为一条定理,并通过Tukey引理证明,从而证明了选择公理与Tukey引理间的等价性. 具体定理的形式化描述如下:

```
Theorem Tukey_Choice : forall X,
Ensemble X→exists ε, Choice_Function ε X.
```

在证明之前,首先构造一个特殊的集合 $\mathscr{T}$. 假设类 μ 为非空集合所成的集族,令 $m=\cup\mu$,定义一个函数 $f:\mu\to m$,使得对任意 $(E,e)\in f\subset\mu\times m$,都有 $e\in E$. 该函数的形式化定义如下:

```
Definition Function_C f X : Prop : =
  Ensemble X /\ Function f /\ dom(f) = X /\
  ran(f) ⊂ (\cup X) /\ (forall E: Class,
  In E dom(f) → In f[E] E).
```

设 X 为非空集合,$\widetilde{X}=2^X\sim\{\varnothing\}$,令

$$\mathscr{T}=\{f:f\text{是}\widetilde{X}\text{的子集上的选择函数}\}\tag{7}$$

对集合 $\mathscr{T}$ 的形式化定义如下:

```
Definition En_f X : Class: =
  \{ λ f, exists A, Subclass A (pow(X) ~[∅])
  /\ Function_C f A \}.
```

证明 首先证明 $\mathscr{T}$ 是非空的具有有限特征的集族. 因为 $\varnothing\in\mathscr{T}$,所以 $\mathscr{T}$ 非空. 根据有限特征集的定义,证明分为2个方面:

1) 若 $f\in\mathscr{T}$ 且 $g\subset f$,则易证明 $g\in\mathscr{T}$;

2) 若集 f 的每一个有限子集都为 $\mathscr{T}$ 的成员,则有

a) $f\subset\cup\mathscr{T}\subset\widetilde{X}\times X$;

b) 对每一个 $(E,e)\in f$,$e\in E$;

c) 若 $(E,e),(E,e')\in f$,则 $f_0=\{(E,e),(E,e')\}\in\mathscr{T}$,从而由函数的定义可得 $e'=e$.

综上,$\mathscr{T}$ 是一个非空的具有有限特征的集族,对其应用Tukey引理可得 $\mathscr{T}$ 有极大元. 设 f_1 是 $\mathscr{T}$ 的一个极大元,设 f_1 的定义域为 D. 若 $D\subsetneq\widetilde{X}$,则有 $\widetilde{X}\sim D\neq\varnothing$. 因此设 $E_2\in\widetilde{X}\sim D$,取 $e_2\in E_2$. 令集合 $f_2=f(\{(E_2,e_2)\})$,则可以证明 $f_2\in\mathscr{T}$ 并且 f_1 是 f_2 的真子集,这与 f_1 是 $\mathscr{T}$ 极大元矛盾. 故 f_1 的定义域 $D=\widetilde{X}$,即对于集合 X,f_1 是 X 的选择函数,定理得证.

5 其他集合论形式化工作

公理化集合论的形式化工作方面,Werner的工作研究了公理化集合论与类型论间的关系,提出了一种ZFC集合论与Coq归纳构造演算(CIC)理论一致性的证明[10]. 基于Werner的工作,Barras在Coq上形式化了CIC的元理论[11]. Simpson完成了ZFC集合论中大部分概念的形式化,Kirst和Smolka通过Coq形式化了二阶ZF集合理论[12].

选择公理的形式化工作方面,Schepler通过选择公理证明了Zorn引理和良序定理,但其是在Coq标准库中的朴素集合论的基础上实现的. 此外,Paulson基于Isabelle证明了选择公理的相容性[13].

笔者[14]完成了选择公理与Hausdorff极大原则、Zermelo假定等定理的形式化证明,其中使用了Tukey引理未给出完整证明. 应该指出,选择公理与Tukey引理等价性的传统数学证明散见于众多数学文献[1,2,15].

6 形式化证明总览

选择公理是公理化集合论中的一个重要公理,其在现代数学中有着重要应用. 笔者在“公理化集

合论”形式化系统的基础上，完成了选择公理与 Tukey 引理的形式化，并对二者间的等价性进行了完整的形式化证明. 文中的所有证明都已在证明辅助工具 Coq 中验证. 完整的 Coq 证明代码可见参考文献[16].

整个形式化工作大约 3 800 行代码，其中包括 30 个定义、20 个引理和 10 个定理. 全部代码都已在 Coq 8.8.0 中测试编译通过. 表格 2 展示了具体每个脚本文件的形式化工作量，为了方便理解还标注了文件的对应章节.

表 2　选择公理与 Tukey 引理的形式化

文件	章节	概念	证明
Logic_Property. v	第 2 节	20	10
Axiomatic_Set_Theory. v	第 2 节	800	1 200
Basic_Definition. v	第 3 节	160	70
Tukey_Lemma. v	第 4 节	90	340
Proof_AC. v	第 5 节	10	80

7　结束语

选择公理和 Tukey 引理的形式化在数学领域中具有深远的意义，未来可以进一步研究选择公理与更多定理的等价性证明. 在 Tukey 引理的基础上可以证明拓扑学中重要的 Tychonoff 定理. 此外，在本文“公理化集合论”形式化系统基础上，可以快速构建近世代数理论和拓扑学理论. 这对开发布尔巴基学派提出的现代数学三大母结构—序结构、代数结构、拓扑结构—的形式化具有重大意义.

参考文献：

[1] Jech T. The axiom of choice[M]. Amsterdam: North Holland Publishing Company, 1973: 1-56.

[2] Bernays P, Fraenkel A A. Axiomatic set theory[M]. Amsterdam: North Holland Publishing Company, 1958: 1-73.

[3] Bertot Y, Castéran P. Interactive theorem proving and program development, Coq'art: the calculus of inductive constructions[M]. Heidelberg: Springer, 2004: 1-11.

[4] Gonthier G. Formal proof-the four color theorem[J]. Notices of the American Mathematical Society, 2008, 55(11): 1382-1393.

[5] Gonthier G, Asperti A, Avigad J, et al. Machine-checked proof of the odd order theorem[C]//ITP 2013. Heidelberg: Springer, 2013: 163-179.

[6] Wiedijk F. Formal proof-getting started[J]. Notices of the American Mathematical Society, 2008, 55(11): 1408-1414.

[7] Wang Hao. On Zermelo's and Von Neumann's axioms for set theory[J]. Proc Natl Acad Sci USA, 1949, 35(3): 150-155.

[8] Kelley J L. General topology[M]. New York: Springer-Verlag, 1955: 250-281.

[9] Sun Tianyu. Axiomatic set theory[EB/OL]. (2018-10-20)[2018-12-10]. https://github.com/styzystyzy/Axiomatic_Set_Theory/.

[10] Werner B. Sets in types, types in sets[C]//Proceedings of TACS' 97. Heidelberg: Springer, 1997: 530-546.

[11] Barras B. Sets in Coq, Coq in sets[J]. Journal of Formalized Reasoning, 2010, 3(1): 29-48.

[12] Kirst D, Smolka G. Categoricity results for second-order ZF in dependent type theory[C]//ITP 2017. Heidelberg: Springer, 2017: 304-318.

[13] Paulson L C. The relative consistency of the axiom of choice mechanized using Isabelle/ZF[J]. LMS Journal of Computation and Mathematics, 2003(6): 98-248.

[14] Sun Tianyu, Yu Wensheng. Machine proving system for mathematical theorems based on Coq-machine proving of Hausdorff maximal principle and Zermelo postulate[C]//Proceedings of the 36th Chinese Control Conference. New York: IEEE, 2017: 9871-9878.

[15] 熊金城. 点集拓扑讲义[M]. 北京：高等教育出版社, 2011: 36-40.

[16] Sun Tianyu. Tukey's lemma and AC[EB/OL]. (2018-11-30)[2018-12-10]. https://github.com/BKLSIC/Tukey_AC/.