Forms of Choice in Ring Theory

Lorenz Halbeisen*, Norbert Hungerbühler*, Nir Lazarovich+,
Waltraud Lederle*, Marc Lischka*, Salome Schumacher*[1]

* Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland

+ Department of Mathematics, Technion – Israel Institute of Technology, Haifa 32000, Israel

key-words: square root functions in rings, root functions in integral domains, axiom of choice, finite choice, cycle choice, bounded multiple choice, consistency results

2010 Mathematics Subject Classification: **03E25** 13A99

Abstract

We investigate the relationship between various choice principles and nth-root functions in rings. For example, we show that the Axiom of Choice is equivalent to the statement that every ring has a square-root function. Furthermore, we introduce a choice principle which implies that every integral domain has an nth-root function (for odd integers n), and introduce another choice principle which is equivalent to the Prime Ideal Theorem restricted to certain ideals. Finally, we investigate the dependencies between the two new choice principles and a choice principle for families of n-element sets.

0 Introduction

Some Forms of Choice Related to Algebra

The investigation of consequences of the Axiom of Choice in algebra has a long tradition. Below we list a few choice principles in the context of rings and vector spaces. For more choice principles specifically related to rings we refer the reader to Howard and Rubin [5, pp. 71–75].

- Krull's Theorem (FORM 1 CD in [5]): Every proper ideal in a commutative ring can be extended to a maximal ideal.

  Krull proved in [7] that every non-zero ring has a maximal ideal. Since he used explicitly the Well-Ordering Principle (FORM 1 CD in [5]) in his proof (see [7, p. 735 f]), one may ask how much of the Axiom of Choice we get back from Krull's Theorem. This problem was solved by Hodges [4], who showed that Krull's Theorem is in fact equivalent to the Well-Ordering Principle, which is in turn equivalent to the Axiom of Choice.

- Prime Ideal Theorem (FORM 14 C in [5]): Every commutative ring with a unit has a prime ideal.

  This choice principle is weaker than the Axiom of Choice and is for example equivalent to the following statement: *For every graph G, if every finite subgraph of G is 3-colorable, then G is n-colorable, $n \geq 3$* (see Läuchli [8]).

[1]Partially supported by SNF grant 200021_178851.

- Downward Basis Principle (FORM 1 A in [5]): Every vector space V has the property that each set of vectors which generates V contains an algebraic basis.

  This choice principle is equivalent to the Axiom of Choice. The proof is due to Halpern [3] (and simplified by H. Läuchli).

- Vector-Space-Basis Principle (FORM 66 in [5]): Every vector space has an algebraic basis.

  Blass proved in [1] that this principle implies Multiple Choice (MC), which is FORM 67 in [5] and states that *for every family $\mathscr{F}$ of non-empty sets, there exists a function $f : \mathscr{F} \to \mathscr{P}(\bigcup \mathscr{F})$ such that for each $X \in \mathscr{F}$, $f(X)$ is a non-empty finite subset of X*. Since in Zermelo-Fraenkel Set Theory ZF, MC is equivalent to AC, we get that in ZF, the Vector-Space-Basis Principle is equivalent to the Axiom of Choice. On the other hand, it is not known whether the statement *every vector space over $\mathbb{Q}$ has an algebraic basis* is equivalent to AC (see FORM 110 in [5]).

Forms of Choice Related to Rings

In this section, we define some choice principles which are related to rings. For this, we have to give first some definitions.

In our convention, all rings will be commutative. Let R be a ring and for positive integers n let

$$R^{(n)} := \{y \in R : \exists x(x^n = y)\}$$

(*i.e.*, $R^{(n)}$ is the set of nth powers of R). Notice that for every positive integer n holds $0 \in R^{(n)}$, which shows that $R^{(n)}$ is non-empty.

Definition. *A function $f\colon R^{(n)} \to R$ is called an nth-root function if for every $y \in R^{(n)}$, $f(y)^n = y$ (i.e., if $y \in R^{(n)}$, then $f(y)$ is one of the nth-roots of y).*

Let us consider the case when $n = 2$: The set $R^{(2)}$ may be small, like in zero square rings (see [10]) where $x^2 = 0$ for all $x \in R$, or large like in the case $\mathbb{C} = \mathbb{C}^{(2)}$. Let now R denote an integral domain and consider $a^2 \in R^{(2)}$. Since $x^2 - a^2 = (x-a)(x+a)$, the equation $x^2 = a^2$ has at most two solutions, and only one solution if $1 = -1$. If R is a finite field with odd characteristic, exactly half of the non-zero elements are squares; the product of two squares and the product of two non-squares are squares. The product of a square and a non-square is a non-square. If the characteristic is even, it is equal to 2 and then all elements of a finite field are squares. If R is an integral domain and $-1 = 1$, then $x \mapsto x^2$ is injective, and therefore a square root function exists. If R is an ordered field, *e.g.*, $\mathbb{R}$, one may always choose the larger of two possible solutions of $x^2 = a^2$ as square root of a^2. In the case $F = \mathbb{C}$ one can use its structure of a Riemann surface to define a root by identifying an analytical principal branch of the root function. However, in general we need some form of the Axiom of Choice to define a square root function, and therefore it is not surprising that the existence of root functions in rings is related to some forms of choice.

In the present work we investigate the relationship between the following choice principles:

Classical Choice principles

- Axiom of Choice AC: Every family of non-empty sets has a choice function.
- Prime Ideal Theorem: Every ideal in a Boolean algebra can be extended to a prime ideal.
- Axiom of Choice for Families of n-element Sets C_n: Every family of n-element sets has a choice function.

New choice principles for rings

- nRR: Every ring has an nth-root function.
- nRID: Every integral domain has an nth-root function.
- nRF: Every field has an nth-root function.

Choice principles for families of n-element sets

- Bounded Multiple Choice for Families of n-element Sets kC_n (see Zuckerman [11]): If $\mathscr{F} = \{Y_\lambda : \lambda \in \Lambda\}$ is a family of n-element sets and k is a positive integer, then from each $Y_\lambda \in \mathscr{F}$ we can choose a non-empty set with at most k elements.
- Cycle Choice for Families of n-element Sets cC_n (new): If $\mathscr{F} = \{Y_\lambda : \lambda \in \Lambda\}$ is a family of n-element sets, then on each set $Y_\lambda \in \mathscr{F}$ we can choose a cyclic order.

In particular, we show the following relations:

1. For all $n > 1$, $n\mathsf{RR} \Leftrightarrow \mathsf{AC}$ (Theorem 2.1)
2. $\mathsf{C}_n \Rightarrow n\mathsf{RF}$ (Proposition 3.1) and $n\mathsf{RF} \Leftrightarrow n\mathsf{RID}$ (Proposition 3.2)
3. $2\mathsf{RID} \Leftrightarrow \mathsf{C}_2 \Leftrightarrow 2\mathsf{RF}$ (Proposition 3.3)
4. $3\mathsf{RID} \Leftrightarrow \mathsf{C}_3 \Leftrightarrow 3\mathsf{RF}$ (Proposition 3.4)
5. For every odd number $m \geq 3$: $2\mathsf{C}_m \Rightarrow m\mathsf{RID}$ (Proposition 3.5)
6. $\mathsf{cC}_n \wedge n\mathsf{RID} \Rightarrow \mathsf{C}_n$ (Proposition 3.7)
7. The Prime Ideal Theorem restricted to certain ideals is equivalent to cC_p for odd primes p. (Proposition 5.1)

8. $\mathsf{cC}_{n+1} \Leftrightarrow \bigwedge_{k=1}^{n} \mathsf{C}_k$ (Theorem 4.1)

9. $\mathsf{cC}_n \Leftrightarrow \bigwedge_{k=1}^{n} \mathsf{C}_k$ for composite numbers n (Corollary 4.2)

10. For two different primes p and q, $\mathsf{qC}_{p+q} \not\Rightarrow \mathsf{cC}_{p+q} \vee \mathsf{C}_{p+q}$ (Theorem 6.7). In particular, for two different primes p and q, qC_{p+q} implies neither cC_{p+q} nor C_{p+q} (Corollary 6.8).

In Section 1, we first give a construction of polynomial rings in arbitrarily many variables which does not use any non-trivial form of the Axiom of Choice. Then we give the definition of three choice principles for families of n-element sets, which are related to nth-root function in rings. In Section 2, we show that the Axiom of Choice is equivalent to the existence of square-root functions in rings. In Section 3 we investigate the relationship between nth-root functions in integral domains and some choice principles for families of n-element sets, and in Section 5 we show that one of these choice principles is equivalent to a weak form of the Prime Ideal Theorem. In Section 4 we investigate the relationship between two choice principles for families of n-element sets, and in Section 6 we prove an independence result.

Sections 1–5 are self-contained, whereas Section 6 requires some basic knowledge in the construction of Fraenkel–Mostowski type permutation models of set theory with atoms.

1 Basic definitions

1.1 Polynomial Rings

For the sake of completeness, we show that we do not need any non-trivial form of the Axiom of Choice in order to construct polynomial rings in arbitrarily many variables.

Let R be a ring and Λ a set. In the literature, polynomial rings in arbitrarily many variables $\{X_\lambda : \lambda \in \Lambda\}$ are usually defined very explicitly by first defining the set of monomials $\mathcal{M}$ as finitely supported functions $\Lambda \to \mathbb{N}$ and then the set of polynomials as finitely supported functions $\mathcal{M} \to R$. In this work we choose a different approach. We assume the polynomial ring in one variable as given and define arbitrary polynomial rings as direct limits.

1.2 Direct limit of rings

We first need to establish the notions of a directed set and a direct system.

Definition. *A* directed set *is a set I together with a binary relation $\preceq$ satisfying the three conditions*

1. *reflexivity:* $\forall i \in I : i \preceq i$

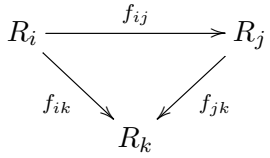
2. *transitivity:* $\forall i, j, k \in I \colon (i \preceq j) \wedge (j \preceq k) \Rightarrow (i \preceq k)$

3. *existence of an upper bound:* $\forall i, j \in I \, \exists k \in I \colon i, j \preceq k$.

DEFINITION. *A* direct system of rings *over a directed set* $(I, \preceq)$ *consists of a set of rings* $\{R_i : i \in I\}$ *and for all* $i, j \in I$ *with* $i \preceq j$ *a ring homomorphism* $f_{ij} \colon R_i \to R_j$ *satisfying the two conditions*

1. $\forall i \in I \colon f_{ii} = id_{R_i}$,

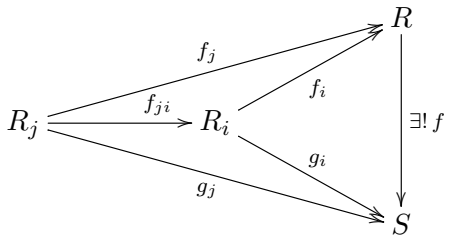
2. $\forall i, j, k \in I,\, i \preceq j \preceq k \colon f_{ik} = f_{jk} \circ f_{ij}$.



We will first define the direct limit of a direct system via its universal property and then give the explicit construction.

DEFINITION. *Let* $\{R_i : i \in I\}$ *be a direct system of rings over a directed set* $(I, \preceq)$. *A* direct limit, *denoted* $\operatorname{colim}_{i \in I} R_i$, *of the direct system is a ring* R *together with, for every* $i \in I$, *a ring homomorphism* $f_i \colon R_i \to R$ *with the following properties.*

For all $j \in I$ *with* $j \preceq i$ *holds* $f_i \circ f_{ji} = f_j$. *Moreover,* R *together with* $\{f_i : i \in I\}$ *is universal with respect to this property. This means that for every ring* S *and for all ring homomorphisms* $g_i \colon R_i \to S$ *such that for all* $j \in I$ *with* $j \preceq i$ *holds* $g_i \circ f_{ji} = g_j$ *there exists a unique ring homomorphism* $f \colon R \to S$ *such that for all* $i \in I$ *holds* $f \circ f_i = g_i$.



It is not difficult to check that the direct limit is unique up to unique isomorphism.

To construct a direct limit explicitly, define the following equivalence relation on the disjoint union $\bigsqcup_{i \in I} R_i$. Let $x \in R_i$ and $y \in R_j$. Then

$$x \sim y \quad :\Leftrightarrow \quad \exists k \in I \colon (i, j \preceq k) \wedge (f_{ik}(x) = f_{jk}(y)).$$

The underlying set of the direct limit is

$$\operatorname{colim}_{i \in I} R_i := \bigsqcup_{i \in I} R_i / \sim .$$

We now define the ring operations. For an element $x \in \bigsqcup_{i\in I} R_i$ we denote by $[x]$ its equivalence class. Let $x \in R_i$ and $y \in R_j$. Let $k \in I$ mit $i, j \preceq k$. Note that because of $f_{kk}(x) = x$ holds $[x] = [f_{ik}(x)]$ and $[y] = [f_{jk}(y)]$, so we define

$$[x] + [y] := [f_{ik}(x) + f_{jk}(y)]$$
$$[x] \cdot [y] := [f_{ik}(x) \cdot f_{jk}(y)].$$

It is straight forward to show that this actually defines a ring structure on $\operatorname{colim}_{i\in I} R_i$. We omit the proof that this is indeed the direct limit of the direct system of rings.

1.3 Polynomial rings in arbitrarily many variables

Now we apply the direct limit of rings to define polynomial rings. Let R be a ring and Λ a set. Denote by $\mathscr{X} = \{X_\lambda : \lambda \in \Lambda\}$ the set of variables.

The directed set. Let $\operatorname{fin}(\mathscr{X})$ be the set of all *finite* subsets of $\mathscr{X}$. For every $S \in \operatorname{fin}(\mathscr{X})$ let $\operatorname{Enum}(S)$ be the set of all bijections $\{1, \dots, |S|\} \to S$. Let

$$I := \bigcup_{S\in\operatorname{fin}(\mathscr{X})} \{S\} \times \operatorname{Enum}(S)\,,$$

so the elements of I are ordered pairs $\langle S, f\rangle$ with $S \in \operatorname{fin}(\mathscr{X})$ and $f \in \operatorname{Enum}(S)$. It is not difficult to see that I, together with the relation

$$\langle S, f\rangle \preceq \langle S', f'\rangle \quad \Leftrightarrow \quad S \subseteq S',$$

is a directed set.

The direct system of rings. Recall that we assumed the polynomial ring $R[X]$ as known, and we can of course iterate and consider the polynomial ring $R[X][Y]$ of polynomials with coefficients in $R[X]$. We will also need the universal property of the polynomial ring.

Universal Property of the Polynomial Ring. Let A and B be rings and let $\varphi\colon A \to B$ be a ring homomorphism. Consider $A \subset A[X]$ in the usual way. Let $b \in B$ be arbitrary. Then, there exists a unique ring homomorphism $\bar\varphi\colon A[X] \to B$ such that $\bar\varphi|_A = \varphi$ and $\bar\varphi(X) = b$.

Let $\langle S, f\rangle \in I$ and denote $R_{S,f} := R[f(1)][f(2)]\dots[f(|S|)]$. Let $\langle S', f'\rangle \in I$ with $\langle S, f\rangle \preceq \langle S', f'\rangle$. Consider $R \subset R[f'(1)]\dots[f'(|S'|)]$ in the usual way. With the universal property of the polynomial ring we can extend this inclusion uniquely to a ring homomorphism $R[f(1)] \to R[f'(1)]\dots[f'(|S'|)]$ mapping $f(1)$ to $f(1)$, which is also an element of S' since $S \subseteq S'$. In particular the extension is independent of f'. Inductively, there exists a unique ring homomorphism

$$f_{\langle S,f\rangle,\langle S',f'\rangle}\colon R[f(1)]\dots[f(|S|)] \to R[f'(1)]\dots[f'(|S'|)]$$

mapping for all $n \in \{1, \dots, |S|\}$ the element $f(n)$ to $f(n)$. It is obvious that this defines a direct system.

DEFINITION. *The polynomial ring $R[\mathscr{X}]$ is defined as the direct limit of the above direct system.*

The polynomial ring satisfies the following universal property.

UNIVERSAL PROPERTY OF THE POLYNOMIAL RING IN ARBITRARILY MANY VARIABLES. Let S be a ring and let $\varphi\colon R \to S$ be a ring homomorphism. Then, for every map $\alpha\colon \Lambda \to S$ there exists a unique ring homomorphism $\bar{\varphi}\colon R[\mathscr{X}] \to S$ satisfying the two conditions

1. $\bar{\varphi}|_R = \varphi$,
2. $\forall \lambda \in \Lambda\colon \bar{\varphi}(X_\lambda) = \alpha(\lambda)$.

1.4 Choice principles for families of n-element sets

Let n be a positive integer. If $\mathscr{F} = \{Y_\lambda : \lambda \in \Lambda\}$ is such that for each $\lambda \in \Lambda$ we have $|Y_\lambda| = n$ (*i.e.*, Y is an n-element set), then $\mathscr{F}$ is called a *family of n-element sets*.

The Axiom of Choice for Families of n-element Sets, denoted C_n, states that every family $\mathscr{F} = \{Y_\lambda : \lambda \in \Lambda\}$ of n-element sets has a choice function, *i.e.*, there is a function

$$\begin{array}{rccc} f: & \mathscr{F} & \longrightarrow & \bigcup \mathscr{F} \\ & Y_\lambda & \longmapsto & f(Y_\lambda) \in Y_\lambda \end{array}$$

which chooses an element from each set $Y_\lambda \in \mathscr{F}$.

A weaker choice principle than C_n we obtain by requiring that $f(Y_\lambda) \subseteq Y_\lambda$ is a non-empty set with at most k elements.

DEFINITION. *For positive integers k, n with $k \leq n$, k-Bounded Multiple Choice for Families of n-element Sets, denoted kC_n, states that if $\mathscr{F} = \{Y_\lambda : \lambda \in \Lambda\}$ is a family of n-element sets, then there exists a function which chooses from each $Y_\lambda \in \mathscr{F}$ a non-empty set with at most k elements.*

Below, we shall only consider the case when $k = 2$, denoted $\mathsf{2C}_n$.

The fact summarizes two results which are used later. The first part is well-known in the case $k = 1$, but we see that the generalization to $k \geq 1$ is almost immediate.

FACT 1.1. (a) *If m and n are positive integers and m divides n, then for every $k \leq m$ holds $\mathsf{kC}_n \Rightarrow \mathsf{kC}_m$. In particular, $\mathsf{C}_n \Rightarrow \mathsf{C}_m$.*

(b) *If n is a positive composite integer and we have C_k for all $1 \leq k < n$, then we also have C_n.*

Proof. (a) Let $\mathscr{F}_m = \{Y_\lambda : \lambda \in \Lambda\}$ be a family of m-element sets, let $k := \frac{n}{m}$, and for every $Y_\lambda \in \mathscr{F}$ let

$$Y_\lambda^k := \{\langle x, i\rangle : x \in Y_\lambda \wedge i \in k\}\,.$$

Then Y^k_λ is an n-element set and the family $\mathscr{F}_n = \{Y^k_\lambda : \lambda \in \Lambda\}$ is a family of n-element sets. By C_n, $\mathscr{F}_n$ has a choice function choosing subsets of $\mathscr{F}$ of size at most k, say f. Let $g\colon \mathscr{F}_m \to \bigcup \mathscr{F}_m$ be defined by stipulating

$$x \in g(Y_\lambda) \iff \exists i \in k\big(\langle x, i\rangle \in f(Y^k_\lambda)\big)\,,$$

i.e. we "forget" the second coordinate of the elements chosen by f. Since f is a choice function for $\mathscr{F}_n$, g is a choice function for $\mathscr{F}_m$.

(b) This is a consequence of Jech [6, Theorem 7.15] (see also Halbeisen [2, Theorem 6.17]). ⊣

In order to define cycle choice for families of n-element sets, we recall first the notion of a cyclic order: The triples (x, y, z) occurring in the following definition can be read and thought of as "after x comes y and then z".

Definition. *Let S be any set. A* cyclic order *on S is a subset $C \subseteq S \times S \times S$ satisfying the following requirements:*

1. *cyclicity:* $(x, y, z) \in C \Rightarrow (y, z, x) \in C$
2. *asymmetry:* $(x, y, z) \in C \Rightarrow (z, y, x) \notin C$
3. *transitivity:* $(x, y, z) \in C \wedge (x, z, w) \in C \Rightarrow (x, y, w) \in C$
4. *totality: If x, y, z are pairwise distinct, then $(x, y, z) \in C \vee (z, y, x) \in C$.*

We will usually write $[x, y, z]$ instead of $(x, y, z) \in C$.

One source of cyclic orders is the following. Assume that $(S, <)$ is a totally ordered set. Then, we get a cyclic order by stipulating $[x, y, z]$ if $x < y < z$ and "closing" this relation under cyclicity.

There are two important concepts in the notion of cyclic orders, namely immediate successors and intervals.

Definition. *Let S be a cyclically ordered set and let $s \in S$. The* immediate successor *of s is the unique element s_+ not equal to s such that there does not exist any element t with $[x, t, x_+]$.*

Immediate successors might not always exist, but they do if S is a finite set. They also can be used to define cyclic orders, because a cyclic order is uniquely determined by the immediate successors of every element.

Definition. *Let S be a cyclically ordered set and $s, s' \in S$. Similar to the real line we define the intervals*

- $(s, s') := \{t \in S : [s, t, s']\}$
- $[s, s') := (s, s') \cup \{s\}$

- $(s, s'] := (s, s') \cup \{s'\}$
- $[s, s'] := (s, s') \cup \{s, s'\}$.

The following are simple consequences of the definition of a cyclic order.

FACT 1.2. *If $|S| \leq 2$, then the empty set is a cyclic order on S. Otherwise, a cyclic order is always non-empty.*

FACT 1.3. *If $[x, y, z]$, then x, y, z are pairwise distinct.*

Proof. Assume that $x = y$. Applying cyclicity twice yields $[z, x, x]$, which is a contradiction to asymmetry. ⊣

DEFINITION. *The choice principle* Cycle Choice for Families of n-element Sets*, denoted* cC_n*, states that if $\mathscr{F} = \{Y_\lambda : \lambda \in \Lambda\}$ is a family of n-element sets, then there exists a function which chooses on each set $Y_\lambda \in \mathscr{F}$ a cyclic order.*

2 Roots in rings and the Axiom of Choice

In this section we consider the most classical of all choice axioms: the Axiom of Choice itself. The strategy we use to relate it to root functions in rings is the following. When constructing a choice function for a family of sets, we will use these sets as well as their elements as indefinite variables in a polynomial ring over some convenient ring, and then we will divide out an appropriate ideal to set a set and its elements in relation as well as getting rid of algebraic difficulties.

THEOREM 2.1. *The following are equivalent:*

1. AC – *Axiom of Choice.*
2. nRR *holds for all $n > 1$ – every ring has an nth-root function.*
3. nRR *holds for some $n > 1$.*
4. AC' – *For every collection $\mathscr{F}$ of non-empty sets there is a function choosing a singleton or a proper non-empty finite subset of every set in $\mathscr{F}$. Formally, there exists $g\colon \mathscr{F} \to \bigcup_{Y \in \mathscr{F}} \mathscr{P}(Y) \setminus \{\emptyset\}$ such that for all $Y \in \mathscr{F}$ the set $g(Y) \subsetneq Y$ is a proper finite subset, unless $|Y| = 1$, in which case $g(Y) = Y$.*

Proof. (1 ⇒ 2) Let R be a ring, let $n \in \mathbb{N}$ and denote as in the introduction $R^{(n)} := \{x^n : x \in R\}$. For $x, \tilde{x} \in R$ define the equivalence relation $x \sim \tilde{x} \Leftrightarrow x^n = \tilde{x}^n$. Denote the equivalence class of x by $[x]$ and let

$$\mathscr{F} := R/\sim = \big\{[x] : x \in R\big\}$$

be the set of equivalence classes. Clearly $\mathscr{F}$ is a partition of R into pairwise disjoint non-empty sets. Hence, by AC there is a choice function f for $\mathscr{F}$. Define now the nth root function $\sqrt[n]{\cdot}\colon R^{(n)} \to R$ by stipulating

$$\sqrt[n]{y} := f\big([x]\big),$$

where $[x]$ is such that $[x] = \{\tilde{x} \in R : \tilde{x}^n = y\}$.

$(2 \Rightarrow 3)$ is trivial.

$(3 \Rightarrow 4)$ For some index-set Λ, let $\mathscr{F} = \{Y_\iota : \iota \in \Lambda\}$ be a family of pairwise disjoint non-empty sets. Denote by $\mathscr{A} = \bigcup \mathscr{F}$ the union over all sets in $\mathscr{F}$. Let $I \subseteq \mathbb{Z}[\mathscr{A} \cup \mathscr{F}]$ be the ideal generated by

$$\begin{aligned} t \cdot s \qquad & \text{for all } s, t \in \mathscr{A} \cup \mathscr{F} \text{ with } s \neq t, \text{ and} \\ x^n - Y \qquad & \text{for all } x \in \mathscr{A} \text{ and } Y \in \mathscr{F} \text{ with } x \in Y. \end{aligned}$$

Notice that, for example, $Y_\iota^2 = x^n \cdot Y = x^{n-1} \cdot (x \cdot Y) \equiv x^{n-1} \cdot 0 = 0 \mod I$. Finally, let

$$R := \mathbb{Z}[\mathscr{A} \cup \mathscr{F}] \,/\, I$$

be the polynomial ring over $\mathscr{A} \cup \mathscr{F}$ modulo the ideal I. For every $k \in \mathbb{N}$, let $\mathscr{A}^{(k)} := \{x^k : x \in \mathscr{A}\}$. It is easy to see that as a $\mathbb{Z}$-module R is freely spanned by $\{1\} \cup \mathscr{A}^{(1)} \cup \mathscr{A}^{(2)} \cup \ldots \cup \mathscr{A}^{(n-1)} \cup \mathscr{F}$, and thus, as a $\mathbb{Z}$-module,

$$R = \mathbb{Z}1 \oplus A^{(1)} \oplus A^{(2)} \ldots \oplus A^{(n-1)} \oplus F,$$

where $A^{(k)}$ and F are the free $\mathbb{Z}$-modules over $\mathscr{A}^{(k)}$ and $\mathscr{F}$, respectively. For $Y \in \mathscr{F}$ denote by $\pi_{\cup Y}$ the projection

$$\pi_{\cup Y}\colon R \to \bigoplus_{x \in Y} \mathbb{Z}x \subseteq A^{(1)},$$

and by π_1 the projection

$$\pi_1\colon R \to \mathbb{Z}1.$$

By $n\mathsf{RR}$, there is an nth-root function $\sqrt[n]{\cdot}\colon R^{(n)} \to R$. Let us identify the elements of $\mathscr{F}$ and $\bigcup \mathscr{F}$ with the corresponding elements in $F \subseteq R^{(n)}$ and $A^{(1)}$ respectively. To define the function $g\colon \mathscr{F} \to \bigcup_{Y \in \mathscr{F}} \mathscr{P}(Y)$, let $Y \in \mathscr{F}$, and let $r = \sqrt[n]{Y} \in R$.

First observe that since π_1 is a ring homomorphism (identifying $\mathbb{Z}1$ with $\mathbb{Z}$) and $\pi_1(Y) = 0$, $\pi_1(r)^n = \pi_1(r^n) = 0$, and since $\pi_1(r) \in \mathbb{Z}$, we obtain $\pi_1(r) = 0$. We can write $r = s + \bar{t}$, where $s = \pi_{\cup Y}(r)$ and $\bar{t} = r - s \in \ker(\pi_{\cup Y}) \cap \ker(\pi_1)$. In particular,

$$s \in \bigoplus_{x \in Y} \mathbb{Z}x \quad \text{and} \quad \bar{t} \in \bigoplus_{x \in \mathscr{A} \setminus Y} \mathbb{Z}x \;\oplus\; \bigoplus_{k=2}^{n-1} A^{(k)} \;\oplus\; F.$$

An easy computation shows that

$$Y = r^n = s^n,$$

as all terms of the form $s^k \bar{t}^{n-k}$ belong to the ideal I, except when $k = n$.

Writing s in coordinates $s = \sum_{i=1}^{m} \alpha_i x_i$, where $x_1, \ldots, x_m \in Y$ are distinct and $\alpha_1, \ldots, \alpha_m \in \mathbb{Z} \setminus \{0\}$, we compute

$$Y = s^n = \left(\sum_{i=1}^{m} \alpha_i x_i \right)^n = \sum_{i=1}^{m} \alpha_i^n Y.$$

Thus $\sum_{i=1}^{m} \alpha_i^n = 1$.

We consider two cases:

Case 1: n is even. $\sum_{i=1}^{m} \alpha_i^n = 1$ implies that $m = 1$ and $\alpha_1 = \pm 1$. In this case, set $g(Y) = \{x_1\}$.

Case 2: n is odd. Then either $m = 1$ and $\alpha_1 = 1$ or there exist some i, j such that $\alpha_i > 0$ and $\alpha_j < 0$. In this case, set $g(Y) = \{x_i : \alpha_i > 0\}$.

It is clear that in both cases $g(Y)$ satisfies the requirements of AC'.

$(4 \Rightarrow 1)$ Let $\mathscr{F}$ be a collection of non-empty sets. Consider the collection of all their subsets $\mathscr{F}' = \bigcup_{Y \in \mathscr{F}} \mathscr{P}(Y)$. By AC', there is a function $g \colon \mathscr{F}' \to \bigcup_{A \in \mathscr{F}'} \mathscr{P}(A) = \mathscr{F}'$ satisfying AC'.

Note that for every $Y \in \mathscr{F}$ the intersection $\bigcap_{n \in \mathbb{N}} g^n(Y)$ is a singleton since $g(Y)$ is finite and the sequence $\{g^n(Y)\}_{n \in \mathbb{N}}$ is strictly decreasing until it stabilizes to a singleton. It is clear that the function $f \colon \mathscr{F} \to \bigcup \mathscr{F}$, where $f(Y)$ is such that $\bigcap_{n \in \mathbb{N}} g^n(Y) = \{f(Y)\}$, is a choice function. ⊣

As we can see in the proof, we do not need root functions on all rings to get AC. It is enough to have root functions on all rings of characteristic 0. Note however that the ring R we constructed has an abundance of zero divisors. This is unavoidable, as we will see later: If we allow only integral domains for defining square root functions, we get much weaker choice principles than AC.

3 Root Functions in Integral Domains

3.1 Relationships Between n-Element Choice and Root Functions

PROPOSITION 3.1. *If every family of n-element sets has a choice function, then every integral domain has an nth-root function. In short,* $\mathsf{C}_n \Rightarrow n\mathsf{RF}$.

Proof. Let $\mathbb{F}$ be an arbitrary field and denote as before $\mathbb{F}^{(n)} := \{y \in \mathbb{F} : \exists x(x^n = y)\}$. Recall that for any y in $\mathbb{F}$, the polynomial $X^n - y$ has at most n zeros in $\mathbb{F}$. More precisely, for all $y \in \mathbb{F}^{(n)}$ with $y \neq 0$ the cardinality of the set $W_y := \{x \in \mathbb{F} : x^n = y\}$ equals the number of nth roots of unity in $\mathbb{F}$. Recall as well that if we write $n = p^r \cdot k$, where p is the characteristic of $\mathbb{F}$ and p^r the highest power of p dividing n, then the number of nth roots of unity in a splitting field of $\mathbb{F}$ is precisely k. In particular, it divides n. It is clear that the nth roots of unity of $\mathbb{F}$ form a subgroup of the nth

roots of unity in any splitting field. So, by LAGRANGE'S THEOREM, this number and therefore also the cardinality $|W_y|$ divides n.

However, by FACT 1.1.(a), for any $k \mid n$, $\mathsf{C}_n \Rightarrow \mathsf{C}_k$. Hence, define

$$\mathscr{F} := \{W_y \subseteq \mathbb{F} : y \in \mathbb{F}^{(n)} \wedge y \neq 0\}$$

and apply C_k to $\mathscr{F}$ to get an nth root function on $\mathbb{F}^{(n)} \setminus \{0\}$. By choosing 0 as nth root of 0, we get an nth root function on $\mathbb{F}^{(n)}$. ⊣

PROPOSITION 3.2. *Every field has an nth-root function if and only if every integral domain has an nth root function. In short $n\mathsf{RF} \Leftrightarrow n\mathsf{RID}$.*

In particular, $\mathsf{C}_n \Rightarrow n\mathsf{RID}$.

Proof. ($\Rightarrow$) Let R be an arbitrary integral domain. Consider $\mathbb{F} := \mathrm{Quot}(R)$, the quotient field of R. Let $y \neq 0$ be an element of $R^{(n)} = \{y \in R : \exists x \in R(x^n = y)\}$. Let $W_y := \{x \in \mathbb{F} : x^n = y\}$. Recall that $k := |W_y|$ divides n and is independent of y. Let ζ be a primitive kth root of unity in $\mathbb{F}$. Note that such a ζ exists, since for every $y \in \mathbb{F}^{(n)}$ the set $\{\frac{x}{x'} : x, x' \in W_y\}$ is a cyclic group of roots of unity of order k which is independent of y. Now we explain how ζ induces a cyclic order on W_y. If $n = 2$ then it is the empty cyclic order. Otherwise, for every $x \in W_y$ the element ζx is the immediate successor of x. This means that for every $x \in W_y$ we have $[x, x', x'']$ if and only if there exist integers $0 < \alpha < \beta < k$ with $x' = \zeta^\alpha \cdot x$ and $x'' = \zeta^\beta \cdot x$.

With PROPOSITION 3.1, we have an nth-root function $\sqrt[n]{\cdot}$ on $\mathbb{F}^{(n)}$. Now, we can define the nth root of y in $R^{(n)}$ as the first element after $\sqrt[n]{y}$ that is in R in the cyclic order on W_y, i.e. the unique element x in R such that there does not exist any $x' \in R$ with $[\sqrt[n]{y}, x', x]$.

($\Leftarrow$) This follows from the fact that every field is an integral domain.

The last statement is now a direct consequence of PROPOSITION 3.1. ⊣

3.2 Small values of n

In this section we'll see that for small values of n the converse of the implications above are true as well.

PROPOSITION 3.3. *The following choice principles are equivalent.*

(i) Every family of two-element sets has a choice function.

(ii) Every integral domain has a square root function.

(iii) Every field has a square root function.

In short $\mathsf{C}_2 \Leftrightarrow 2\mathsf{RID} \Leftrightarrow 2\mathsf{RF}$.

Proof. $((i) \Rightarrow (ii))$ This implication is clear from Proposition 3.2.

$((ii) \Rightarrow (iii))$ This implication is clear since every field is also an integral domain.

$((iii) \Rightarrow (i))$ Let $\mathscr{F}$ be a family of pairwise disjoint 2-element sets and denote the union by $\mathscr{X} := \bigcup \mathscr{F}$. Furthermore, let K be a field of characteristic not equal to 2 and let $\mathbb{F} := \mathrm{Quot}(K[\mathscr{X}])$ be the field of rational functions with variables in $\mathscr{X}$ and coefficients in K. As in the introduction denote $\mathbb{F}^{(2)} := \{y \in \mathbb{F} : \exists x \in \mathbb{F}(x^2 = y)\}$. Consider the set

$$S := \big\{x^2 - 2x\tilde{x} + \tilde{x}^2 : \{x, \tilde{x}\} \in \mathscr{F}\big\}.$$

Notice that $S \subseteq \mathbb{F}^{(2)}$. Also notice that the square roots of $x^2 - 2x\tilde{x} + \tilde{x}^2$ are precisely $x - \tilde{x}$ and $\tilde{x} - x$, and these two elements are different because the characteristic of $\mathbb{F}$ is not equal to 2. By assumption there exists a square root function $sq\colon \mathbb{F}^{(2)} \to \mathbb{F}$ for $\mathbb{F}$. Now, we define a choice function f for $\mathscr{F}$ by stipulating

$$f\big(\{x, \tilde{x}\}\big) = \begin{cases} x & \text{if } sq(x^2 - 2x\tilde{x} + \tilde{x}^2) = x - \tilde{x}, \\ \tilde{x} & \text{if } sq(x^2 - 2x\tilde{x} + \tilde{x}^2) = \tilde{x} - x. \end{cases}$$

⊣

Proposition 3.4. *The following choice principles are equivalent:*

(i) Every family of three-element sets has a choice function.

(ii) Every integral domain has a third-root function.

(iii) Every field has a third-root function.

In short $\mathsf{C}_3 \Leftrightarrow \mathsf{3RID} \Leftrightarrow \mathsf{3RF}$.

Proof. (i) ⇒ (iii): This is Proposition 3.1.
(ii) ⇔ (iii): This is Proposition 3.2.

(ii) ⇒ (i): Let $\mathscr{F} := \{Y_\iota \mid \iota \in \Lambda\}$ be a collection of 3-element sets and let $\mathbb{F}_4$ be a field with 4 elements. Denote $\mathscr{X} := \bigcup \mathscr{F}$ and let $R = \mathbb{F}_4[\mathscr{X}]$ be the ring of polynomials with variables in $\mathscr{X}$ and coefficients in $\mathbb{F}_4$. Recall that the multiplicative group $\mathbb{F}_4^*$ of $\mathbb{F}_4$ is cyclic, and a generator $\zeta \in \mathbb{F}_4^*$ is a primitive third root of unity.

For every $Y_\iota \in \mathscr{F}$ consider the set

$$S_\iota := \{x + \zeta y + \zeta^2 z : x, y, z \in Y_\iota \text{ pairwise different}\}.$$

The set S_ι has 6 elements and is closed under multiplication by ζ. Note that for every $p \in R$ holds $p^3 = (\zeta p)^3$. Consequently the set $\{p^3 : p \in S_\iota\}$ has only two elements. Denote them by p_ι and q_ι. With 3RID we can choose a third root $\sqrt[3]{p_\iota}$ of p_ι and a third root $\sqrt[3]{q_\iota}$ of q_ι. Note that $\sqrt[3]{p_\iota}$ and $\sqrt[3]{q_\iota}$ are elements of S_ι. Let $x, y \in Y_\iota$ be the variables of $\sqrt[3]{p_\iota}$ and $\sqrt[3]{q_\iota}$ which occur with coefficient 1. Now we get a choice function for $\mathscr{F}$ as follows. If $x = y$ we can choose $x \in Y_\iota$. Otherwise we choose the unique element in $Y_\iota \setminus \{x, y\}$. ⊣

3.3 Root functions in integral domains, bounded choice and cyclic choice

PROPOSITION 3.5. *Let $m \geq 3$ be an odd integer. If for every family of m-element sets there exists a choice function choosing subsets of size at most two, then every integral domain has an mth-root function. In short, for every odd $m \geq 3$, $\mathsf{2C}_m \Rightarrow m\mathsf{RID}$.*

Proof. We prove $\mathsf{2C}_m \Rightarrow m\mathsf{RF}$ and then use PROPOSITION 3.2.

Let $\mathbb{F}$ be an arbitrary field. Denote as always $\mathbb{F}^{(m)} := \{y \in \mathbb{F} : \exists x \in \mathbb{F}(x^m = y)\}$. For $y \in \mathbb{F}^{(m)}$ denote $W_y := \{x \in \mathbb{F} : x^m = y\}$, *i.e.*, the set of mth roots of y. Then there is $l \mid m$ such that for every non-zero element $y \in \mathbb{F}^{(m)}$ we have $|W_y| = l$. By FACT 1.1 the principle $\mathsf{2C}_l$ holds, and we get a function f from $\mathscr{F} := \{W_y \subseteq \mathbb{F} : y \in \mathbb{F}^{(m)} \wedge y \neq 0\}$ to the power set of $\bigcup \mathscr{F}$ with the following properties:

$$\forall W_y \in \mathscr{F}\colon\ f(W_y) \subseteq W_y \wedge |f(W_y)| \in \{1, 2\}.$$

If, for a given y in $\mathbb{F}^{(m)}$, the set $f(W_y)$ has only one element, choose that element as the mth root of y. If $f(W_y)$ has two elements x_1 and x_2, let $k := \frac{m-1}{2}$ and observe that

$$\frac{x_1^{k+1}}{x_2^k} = \frac{x_2^{k+1}}{x_1^k}.$$

Hence this element is invariant under permutation of x_1 and x_2. In addition

$$\left(\frac{x_1^{k+1}}{x_2^k}\right)^m = \frac{(x_1^m)^{k+1}}{(x_2^m)^k} = \frac{y^{k+1}}{y^k} = y,$$

so we can choose this element as a root of y. ⊣

PROPOSITION 3.6. *Let p be an odd prime number and let $m = p+2$. The statement that every integral domain has an mth root function does not imply that every family of m-element sets has a choice function or that every family of m-element sets can be simultaneously cyclically ordered. In short, if p is prime and $m = p + 2$ is odd, then $m\mathsf{RID} \not\Rightarrow \mathsf{cC}_m \vee \mathsf{C}_m$.*

Proof. This follows immediately from PROPOSITION 3.5 and COROLLARY 6.8. ⊣

PROPOSITION 3.7. *Let $n \geq 4$ be an integer. Assume that every family of n-element sets can be simultaneously cyclically ordered. Assume also that every integral domain has an nth root function. Then, every family of n-element sets has a choice function. In short, $\mathsf{cC}_n \wedge n\mathsf{RID} \Rightarrow \mathsf{C}_n$.*

Proof. The proof is similar to the case $n = 3$. Let $\mathscr{F} = \{Y_\iota \mid \iota \in \Lambda\}$ be a collection of n-element sets and choose a prime number p with $\gcd(n, p) = 1$. Let Y_ι be cyclically ordered. Define

$$m := p^{\varphi(n)},$$

where $\varphi : \mathbb{N} \to \mathbb{N}$ is Euler's totient function. Note that

$$|\mathbb{F}_m^*| = m - 1 = p^{\varphi(n)} - 1.$$

By Euler's Theorem we have that

$$n \mid p^{\varphi(n)} - 1$$

since $\gcd(n, p) = 1$. Therefore, there is a $k \in \mathbb{N}$ with $nk = m-1$. Choose a generator ζ of the multiplicative group of $\mathbb{F}_m$. Note that

$$\operatorname{ord}(\zeta^k) = n.$$

Consider the set

$$S_\iota := \left\{ \sum_{i=0}^{n-1} \zeta^{ki} x_i : x_i \in Y_\iota, x_{i+1} \text{ immediate successor of } x_i \right\}.$$

Note that S_ι has cardinality n and is closed under multiplication with ζ. Moreover for every element $p \in S_\iota$ holds $(\zeta p)^n = p^n$, so all elements of S_ι have the same nth power p. With $n\mathsf{RID}$ we can choose an nth-root $\sqrt[n]{p}$ of p. Our choice function chooses the unique element $x \in Y_\iota$ that in $\sqrt[n]{p}$ occurs with coefficient 1. ⊣

Fact 3.8. *Let $m \geq 3$ be an odd number. Let $\mathscr{F}$ be a family of m-element sets. If $\mathscr{F}$ can be simultaneously cyclically ordered and in addition has a choice function choosing subsets of cardinality at most 2, then it has a choice function. In short, for odd numbers $m \geq 3$: $\mathsf{cC}_m \wedge \mathsf{2C}_m \Rightarrow \mathsf{C}_m$.*

Proof. Let $\mathscr{F} = \{Y_\iota \mid \iota \in \Lambda\}$ be a family of m-element sets and assume that cC_m and $\mathsf{2C}_m$ hold. Let $\iota \in \Lambda$. With $\mathsf{2C}_m$ we now choose a subset $\{x, x'\} \subset Y_\iota$. If $x = x'$ our choice function chooses x. Otherwise, the half-open intervals $[x, x')$ and $[x', x)$ are both non-empty, cover all of Y_ι and do not have the same length because m is odd. Our choice function chooses the smallest element of the shorter interval. ⊣

4 Relations between cycle choice and the axiom of choice for families of n-element sets

In this section we leave rings aside and investigate the relation between two weak choice principles, Cycle Choice and the Axiom of Choice for Families of n-element sets.

Theorem 4.1. *Let n be a natural number. Then, every family of $(n+1)$-element sets can be simultaneously cyclically ordered if and only if for each $k \leq n$, every family of k-element sets has a choice function. In short, for every natural number n we have that $\mathsf{cC}_{n+1} \Leftrightarrow \bigwedge_{k=1}^{n} \mathsf{C}_k$*

Proof. ($\Rightarrow$) Let $n \in \mathbb{N}$ and assume that cC_{n+1} holds. Let $k \in \{1, 2, \ldots, n\}$ and let

$$\mathscr{F} = \{Y_\lambda : \lambda \in \Lambda\}$$

be a family of k-element sets. Let $A = \{a_0, a_1, \ldots, a_{n-k}\}$ be a $(n-k+1)$-element set with $A \cap Y_\lambda = \emptyset$ for all $\lambda \in \Lambda$. Since cC_{n+1} holds, for every $\lambda \in \Lambda$ we can choose a cyclic order on $Y_\lambda \cup A$. We define now a choice function by choosing the first element in the cyclic order on $Y_\lambda \cup A$ that comes after the element a_0, *i.e.*, the unique element $y \in Y_\lambda$ such that there does not exist any $y' \in Y_\lambda$ with $[a_0, y', y]$.

($\Leftarrow$) Let $n \in \mathbb{N}$ and assume that C_k holds for every $1 \leq k \leq n$. Let $\mathscr{F} = \{Y_\lambda : \lambda \in \Lambda\}$ be a family of $(n+1)$-element sets. For every $1 \leq k \leq n$ let

$$f_k \colon \left\{Y \subset \bigcup \mathscr{F} : |Y| = k\right\} \to \bigcup \mathscr{F}$$

be a choice function. Let $\lambda \in \Lambda$. We define a directed graph on Y_λ by putting a directed edge from $x \in Y_\lambda$ to $y \in Y_\lambda$ if and only if $f_n(Y_\lambda \setminus \{x\}) = y$. Note that every vertex has precisely one outgoing edge, and in total there are as many edges as vertices. Now there are three cases to investigate.

Case 0: The graph on Y_λ is a cycle graph.
In this case we are done, we simply define the cyclic order by stipulating that y is the immediate successor of x if there is a directed edge from x to y.

In the other two cases, we will see that we can actually define a choice function on $\mathscr{F}$. We will first do that and then treat the cases together.

Case 1: There is a vertex which is not the endpoint of any edge.

Since the set of such vertices A without incoming edge cannot be all of Y_λ, we can choose $x_{0,\lambda} := f_{|A|}(A)$.

Case 2: Every vertex has an incoming edge, but the graph is no cycle graph.

In this case the graph on Y_λ is a union of disjoint cycles $C_0, C_1, \ldots, C_l$ for an $l \geq 1$. Now because $|C_i| \leq k$ we can choose a vertex c_i from every cycle via $c_i := f_{|C_i|}(C_i)$, and then we can choose out of those

$$x_{0,\lambda} := f_{l+1}\left(\{c_i : i \in \{0, 1, \ldots, l\}\}\right).$$

In Cases 1 and 2 we can now recursively define a total order on Y_λ by declaring the immediate successor of $x_{i,\lambda}$ for $0 \leq i \leq n$ to be $f_{n-i}(Y_\lambda \setminus \{x_{0,\lambda}, x_{1,\lambda}, \ldots, x_{i,\lambda}\})$. Recall that every total order induces a cyclic order, and we are done. $\dashv$

Corollary 4.2. *Let $n \in \mathbb{N}$ be a composite number. Then, every family of n-element sets cay by simultaneously cyclically ordered if and only if for every $1 \leq k \leq n$, every family of k-element sets has a choice function. In short, if $n \in \mathbb{N}$ is a composite number then $\mathsf{cC}_n \Leftrightarrow \bigwedge_{k=1}^{n} \mathsf{C}_k$.*

Proof. Let $n \in \mathbb{N}$ be a composite number. By THEOREM 4.1 it suffices to prove $\bigwedge_{k=1}^{n-1} \mathsf{C}_k \Rightarrow \mathsf{C}_n$, but this implication is well-known (see FACT 1.1.(b)). ⊣

5 Cyclic Choice for Primes and a Weak Form of the Prime Ideal Theorem

COROLLARY 4.2 means that for composite numbers n, the axiom cC_n is much stronger than it seems on first sight. The following proposition stands a bit in contrast to that. For prime numbers p we show that cC_p is equivalent to being able to extend just certain ideals in certain rings to prime ideals, which looks like a very weak assertion.

PROPOSITION 5.1. *Let p be an odd prime number. The axiom cC_p, which states that every family of p-element sets can be simultaneously cyclically ordered, is equivalent to the following weak version of the* Prime Ideal Theorem*:*

Let K be a field with characteristic not equal to p. Let $\mathscr{F} = \{Y_\lambda : \lambda \in \Lambda\}$ be a family of pairwise disjoint sets with p elements. Then, the ideal $\langle Y - x^p : Y \in \mathscr{F}, x \in Y\rangle$ in the ring $K[\bigcup \mathscr{F} \cup \mathscr{F}]$ can be extended to a prime ideal $\mathfrak{p}$ such that for all $x, x' \in \bigcup \mathscr{F}$ with $x \neq x'$ the element $x - x'$ is not in $\mathfrak{p}$.

Proof. Assume first the weak version of the Prime Ideal Theorem. Let $K = \mathbb{C}$. Let $\mathscr{F} = \{Y_\lambda : \lambda \in \Lambda\}$ be a collection of sets each of which has precisely p elements. Let $\mathfrak{p}$ be a prime ideal in the ring $K[\bigcup \mathscr{F} \cup \mathscr{F}]$ such that

- $\mathfrak{p} \supseteq \langle Y - x^p : Y \in \mathscr{F}, x \in Y\rangle$
- $\forall x, x' \in \bigcup \mathscr{F} : x - x' \notin \mathfrak{p}$.

Let $R := K[\bigcup \mathscr{F} \cup \mathscr{F}]/\mathfrak{p}$ and denote by $\pi\colon K[\bigcup \mathscr{F} \cup \mathscr{F}] \to R$ the usual projection. Since $\mathfrak{p}$ is a prime ideal, the ring R is an integral domain. Let $Y \in \mathscr{F}$. The equation $T^p = \pi(Y)$ in R by construction has p pairwise distinct solutions, namely $\pi(x)$ for every $x \in Y$. Recall that the number of zeroes of a polynomial in an integral domain is at most its degree. Let $\zeta \in \mathbb{C}$ be a primitive pth root of unity. Observe that for every $x \in Y$ the polynomial $T^p = \pi(Y)$ also has the pairwise distinct solutions $\zeta^k \pi(x)$ with $k \in \{0, \ldots, p-1\}$. Therefore, for every $x, x' \in Y$ there exists a k such that $\pi(x) = \zeta^k \pi(x')$. Now we define a cyclic order on Y by saying that x' is the immediate successor of x if $\pi(x') = \zeta\pi(x)$.

For the other direction, let K be a field with characteristic not equal to p. Let $\mathscr{F} = \{Y_\lambda : \lambda \in \Lambda\}$ be a family of pairwise disjoint sets with p elements. Assume that each $Y \in \mathscr{F}$ is cyclically ordered. Let $I := \langle Y - x^p : Y \in \mathscr{F}, x \in Y\rangle$ be an ideal in the ring $K[\bigcup \mathscr{F} \cup \mathscr{F}]$.

Step 1: Let L be a splitting field of the polynomial $T^p - 1$ over K. It suffices to consider L instead of K.

There is an obvious injection $\iota\colon K[\bigcup\mathscr{F}\cup\mathscr{F}]\to L[\bigcup\mathscr{F}\cup\mathscr{F}]$, namely the inclusion. Let I_L be the ideal in $L[\bigcup\mathscr{F}\cup\mathscr{F}]$ generated by I. Assume that we can extend I_L to a prime ideal $\mathfrak{p}_L$ in $L[\bigcup\mathscr{F}\cup\mathscr{F}]$ such that for any $x,x'\in\bigcup\mathscr{F}$ with $x\neq x'$ holds $x-x'\notin\mathfrak{p}_L$. Then $\mathfrak{p}:=\iota^{-1}(\mathfrak{p}_L)$ will be a prime ideal in $K[\bigcup\mathscr{F}\cup\mathscr{F}]$, because under ring homomorphisms it is always true that the inverse image of a prime ideal is a prime ideal. In addition, observe that $\mathfrak{p}=\mathfrak{p}_L\cap K[\bigcup\mathscr{F}\cup\mathscr{F}]$. Therefore, no $x-x'$ with $x\neq x'$ lies in $\mathfrak{p}$.

Step 2: Assume $K=L$.

Let $\zeta\in L$ be a primitive pth root of unity. For $x\in\bigcup\mathscr{F}$ let x_+ be the immediate successor of x, *i.e.*, the unique element not equal to x such that there does not exist any element x' with $[x,x',x_+]$. We claim that

$$\mathfrak{p}:=\langle I\cup\{x-\zeta x_+ : x\in\bigcup\mathscr{F}\}\rangle$$

has the desired properties.

First we show that $\mathfrak{p}$ is a prime ideal. Let $a,b\in L[\bigcup\mathscr{F}\cup\mathscr{F}]$ be such that $ab\in\mathfrak{p}$. If we can show that either a or b is in $\mathfrak{p}$, then we are done by the definition of a prime ideal. The idea here is the following: The polynomial ring $L[\bigcup\mathscr{F}\cup\mathscr{F}]$ is the direct limit of its polynomial subrings with finitely many variables. Likewise, both a and b only involve finitely many variables. In this way we reduce the situation to finitely many variables. Let $\mathscr{F}'\subset\mathscr{F}$ be a finite subset as follows. First we require that $a,b\in L[\bigcup\mathscr{F}'\cup\mathscr{F}']$. Next, denote by $S:=\{Y-x^p : Y\in\mathscr{F},x\in Y\}\cup\{x-\zeta x_+ : x\in\bigcup\mathscr{F}\}$ the set of generators of $\mathfrak{p}$. Then there exist $\alpha_1,\dots,\alpha_n\in L[\bigcup\mathscr{F}\cup\mathscr{F}]$ and $c_1,\dots,c_l\in S$ such that $ab\in L[\alpha_1,\dots,\alpha_n][c_1,\dots,c_l]$, *i.e.*, we write ab as a polynomial with coefficients in $L[\alpha_1,\dots,\alpha_n]$. We also require that $\alpha_1,\dots,\alpha_n,c_1,\dots,c_l\in S\in L[\bigcup\mathscr{F}'\cup\mathscr{F}']$. Since $\mathscr{F}'$ is finite, for every $Y\in\mathscr{F}'$ we can choose an element $x_{Y,1}$. By considering it "minimal" the cyclic order yields a total order on Y. Write $Y=\{x_{Y,1},\dots,x_{Y,p}\}$ with $x_{Y,i}<x_{Y,i+1}$. By the universal property of the polynomial ring there exists a unique homomorphism $\varphi\colon L[\bigcup\mathscr{F}'\cup\mathscr{F}']\to L[\mathscr{F}']$ satisfying

- $\varphi|_L=id$
- $\forall Y\in\mathscr{F}'\quad\forall x_{Y,k}\in Y\colon\varphi(x_{Y,k})=\zeta^kY$
- $\forall Y\in\mathscr{F}'\colon\varphi(Y)=Y^p$.

Also by considering $L[\bigcup\mathscr{F}'\cup\mathscr{F}']=L[\mathscr{F}'][\bigcup\mathscr{F}']$ the map φ is just an evaluation homomorphism followed by the injection $Y\mapsto Y^p$. From this we see that

$$\ker(\varphi)=\langle\{Y-x^p : Y\in\mathscr{F}',x\in Y\}\cup\{x_{Y,k}-\zeta^kx_{Y,1} : Y\in\mathscr{F}',k=1,\dots,p\}\rangle.$$

Note that by construction $ab\in\ker(\varphi)$. Also note that φ surjects on an integral domain, hence its kernel is a prime ideal. Therefore, a or b is in $\ker(\varphi)$, which is a subset of $\mathfrak{p}$, and we are done.

It remains to prove that for all $x,x'\in\mathscr{F}$ with $x\neq x'$ the difference $x-x'$ is not in $\mathfrak{p}$. We argue by contradiction, *i.e.*, we assume that $x-x'\in\mathfrak{p}$. Let Y be such that $x\in Y$. Let $\psi\colon L[\bigcup\mathscr{F}\cup\mathscr{F}]\to L[x]$ be the evaluation homomorphism such that

- $\psi|_{L[x]} = id$
- $\forall \tilde{x} \in Y\colon \psi(\tilde{x}) = \zeta^k x$, where k is such that $\tilde{x} - \zeta^k x \in \mathfrak{p}$
- $\psi(Y) = x^p$
- $\psi|_{\mathscr{F}\setminus\{Y\}} = 0$
- $\forall \tilde{Y} \in \mathscr{F} \setminus \{Y\}\colon \psi|_{\tilde{Y}} = 0$.

Obviously $\mathfrak{p} \subset \ker(\psi)$, but still $x \notin \ker(\psi)$. If $x' \notin Y$ then we are already done since clearly $x' \in \ker(\psi)$. If $x' \in Y$, observe that since there exists a $k \in \{1, \dots, p-1\}$ with $x - \zeta^k x' \in \mathfrak{p}$ we also have that $x' - \zeta^k x' = (1 - \zeta^k)x' \in \mathfrak{p}$. This implies that $x' \in \mathfrak{p}$. But then x, x' lie in $\ker(\phi)$, which is a contradiction. ⊣

Now we want to say a word about the case $p = 2$. Recall that cC_2 is true since for 2-element sets, the empty order is a cyclic order. Let $Y \in \mathscr{F}$ and denote $Y = \{x, \tilde{x}\}$. Since $Y - x^2$ and $Y - \tilde{x}^2$ are in the ideal, so is $x^2 - \tilde{x}^2$, which is equal to $(x - \tilde{x})(x + \tilde{x})$. If these elements are supposed to lie in a prime ideal not containing $x - \tilde{x}$, then it must contain $x + \tilde{x}$. Now we can check that

$$K\Big[\bigcup \mathscr{F} \cup \mathscr{F}\Big]\big/\big\langle x + \tilde{x},\, Y^2 - x : Y \in \mathscr{F}, x, \tilde{x} \in Y\big\rangle \cong K[\mathscr{F}],$$

so $\langle Y - x^2 : Y \in \mathscr{F}, x \in Y\rangle$ can be extended to a prime ideal.

6 A consistency result

In this section, we show that for two different primes p and q, qC_{p+q} does neither imply cC_{p+q} nor C_{p+q}. We will do this by showing that the statement $\mathsf{qC}_{p+q} \wedge \neg\mathsf{cC}_{p+q} \wedge \neg\mathsf{C}_{p+q}$ is consistent with the axioms of Zermelo-Fraenkel Set Theory (denoted ZF). In fact, we will show that there exists a model of ZF in which qC_{p+q} holds, but both statements cC_{p+q} and C_{p+q} fail. To show this we construct a permutation model $\boldsymbol{\mathcal{V}_{p+q}}$ in which we have $\neg\mathsf{cC}_{p+q} \wedge \neg\mathsf{C}_{p+q} \wedge \mathsf{qC}_{p+q}$ for all primes $p \neq q$. Recall that in order to establish the corresponding independence result in ZF, by Pincus [9] it suffices to construct a permutation model of ZFA in which qC_{p+q} holds but cC_{p+q} and C_{p+q} fail — where ZFA is a model of Zermelo-Fraenkel set theory with atoms (see Halbeisen [2, Chapter 8]).

For the sake of completeness, we give a short introduction to permutation models, which are models ZF with a set of atoms $\mathcal{A}$, denoted ZFA. An atom is a set which does not contain any element, but which is distinct from the empty set $\emptyset$. The development of the theory ZFA is very much the same as that of ZF. Similar to the cumulative hierarchy of sets in ZF, we define by induction on the class of ordinals Ω

the sets

$$\begin{aligned} \mathrm{M}_0 &:= \mathcal{A}\,, \\ \mathrm{M}_{\alpha+1} &:= \mathscr{P}(\mathrm{M}_\alpha)\,, \\ \mathrm{M}_\alpha &:= \bigcup_{\beta\in\alpha} \mathrm{M}_\beta \quad \text{if } \alpha \text{ is a limit ordinal}\,, \end{aligned}$$

as well as the class

$$\boldsymbol{\mathcal{M}} := \bigcup_{\alpha\in\Omega} \mathrm{M}_\alpha\ .$$

By construction, the class $\boldsymbol{\mathcal{M}}$ is a transitive model of ZFA. Furthermore, the class

$$\mathbf{V} := \bigcup_{\alpha\in\Omega} \mathscr{P}^\alpha(\emptyset),$$

which is a subclass of $\boldsymbol{\mathcal{M}}$, is a model of ZF and is called the *kernel*. Moreover, if the construction of the class $\boldsymbol{\mathcal{M}}$ was carried out in a model of ZFC, then $\mathbf{V}$ is a model of ZFC.

Now, the underlying idea of permutation models, which are models of ZFA, is the fact that the axioms of ZFA do not distinguish between the atoms, and so a permutation of the set of atoms induces an automorphism of the universe.

Let $\mathcal{A}$ be a set of atoms and let $\boldsymbol{\mathcal{M}} = \bigcup_{\alpha\in\Omega} \mathrm{M}_\alpha$ be a model of ZFA. Furthermore, in $\boldsymbol{\mathcal{M}}$, let G be a group of permutations (or automorphisms) of $\mathcal{A}$. We say that a set $\mathcal{F}$ of subgroups of G is a *normal filter* on G if for all subgroups H, K of G we have:

(A) $G \in \mathcal{F}$,

(B) if $H \in \mathcal{F}$ and $H \subseteq K$, then $K \in \mathcal{F}$,

(C) if $H \in \mathcal{F}$ and $K \in \mathcal{F}$, then $H \cap K \in \mathcal{F}$,

(D) if $\phi \in G$ and $H \in \mathcal{F}$, then $\phi H \phi^{-1} \in \mathcal{F}$,

(E) for each $a \in \mathcal{A}$, $\{\phi \in G : \phi a = a\} \in \mathcal{F}$.

For every set $x \in \boldsymbol{\mathcal{M}}$ there is a least ordinal α (in fact a successor ordinal) such that $x \in \mathscr{P}^\alpha(\mathcal{A})$. So, by induction on the ordinals, for every $\phi \in G$ and for every set $x \in \boldsymbol{\mathcal{M}}$ we can define $\phi\, x$ by stipulating

$$\phi\, x = \begin{cases} \emptyset & \text{if } x = \emptyset, \\ \phi\, x & \text{if } x \in \mathcal{A}, \\ \{\phi\, y : y \in x\} & \text{otherwise.} \end{cases}$$

Notice that for all $x, y \in \boldsymbol{\mathcal{M}}$ and every $\phi \in G$ we have $\phi\, x = y \iff x = \phi^{-1} y$ and $x \in y \iff \phi\, x \in \phi\, y$.

For $x \in \boldsymbol{\mathcal{M}}$, the *symmetry group* of x, denoted $\mathrm{sym}_G(x)$, is the group of all permutations in G which map x to x, in other words

$$\mathrm{sym}_G(x) = \{\phi \in G : \phi\, x = x\}.$$

A set x is said to be *symmetric (with respect to $\mathcal{F}$)* if the symmetry group of x belongs to $\mathcal{F}$, *i.e.*, $\mathrm{sym}_G(x) \in \mathcal{F}$. By (E) we have that every atom $a \in \mathcal{A}$ is symmetric. A set x is called *hereditarily symmetric* if x as well as each element of its transitive closure (*i.e.*, the smallest transitive set which contains x) is symmetric. Notice that for all $x \in \boldsymbol{\mathcal{M}}$ and every $\phi \in G$, x is hereditarily symmetric if and only if $\phi\, x$ is hereditarily symmetric. This follows from (D).

Let $\boldsymbol{\mathcal{V}} \subseteq \boldsymbol{\mathcal{M}}$ be the class of all hereditarily symmetric sets. Then $\boldsymbol{\mathcal{V}}$ is a transitive model of ZFA and we call $\boldsymbol{\mathcal{V}}$ a *permutation model*. Because $\mathcal{A}$, as well as every $a \in \mathcal{A}$, is symmetric, we get that the set of atoms $\mathcal{A}$ belongs to $\boldsymbol{\mathcal{V}}$.

Because $\emptyset$ is hereditarily symmetric and for all ordinals α the set $\mathscr{P}^\alpha(\emptyset)$ is hereditarily symmetric too, the kernel $\mathbf{V}$ is a subclass of $\boldsymbol{\mathcal{V}}$. In particular, by induction on α one easily verifies the following

Fact 6.1. *For any set $x \in \mathbf{V}$ and any $\phi \in G$ we have $\phi\, x = x$.*

Since the atoms $a \in \mathcal{A}$ do not contain any elements, but are distinct from the empty set, the permutation models are not models of ZF. However, one can embed arbitrarily large fragments of a permutation model into a well-founded model of ZF.

For each set $S \subseteq \mathcal{A}$, let

$$\mathrm{fix}_G(S) = \{\phi \in G : \phi a = a \text{ for all } a \in S\}$$

and let $\mathcal{F}$ be the filter on G generated by the subgroups $\big\{\mathrm{fix}_G(E) : E \in \mathrm{fin}(\mathcal{A})\big\}$, where $\mathrm{fin}(\mathcal{A})$ is the family of all subsets of $\mathcal{A}$ which have finitely many elements. Then $\mathcal{F}$ is a normal filter. Furthermore, a set x is symmetric if and only if there exists a set of atoms $E_x \in \mathrm{fin}(\mathcal{A})$ such that

$$\mathrm{fix}_G(E_x) \subseteq \mathrm{sym}_G(x)$$

where E_x is called a *support* of x. Notice that if E_x is a support of x and $E_x \subseteq F_x \in \mathrm{fin}(\mathcal{A})$, then F_x is a support of x as well.

Now, fix an arbitrary prime p and an arbitrary prime $q \neq p$. We start with a ground model $\boldsymbol{\mathcal{M}}_{p+q}$ of $\mathsf{ZFA} + \mathsf{AC}$ with a set of atoms

$$\mathcal{A} = \bigcup \big\{P_i : i \in \mathbb{N}\big\} \cup \bigcup \big\{Q_j : j \in \mathbb{N}\big\},$$

where $\mathbb{N}$ is the set of natural numbers, and the sets P_i and Q_j are called *blocks*. Blocks are pairwise disjoint finite sets with $|P_i| = p$ and $|Q_j| = q$. So we have that

1. for all $i, j \in \mathbb{N}$,

$$P_i := \{a_{i,0}, \ldots, a_{i,p-1}\} \quad \text{and} \quad Q_j := \{b_{j,0}, \ldots, b_{j,q-1}\},$$

2. for all $i, i', j, j' \in \mathbb{N}$,

$$P_i \cap Q_j = \emptyset, \qquad i \neq i' \to P_i \cap P_{i'} = \emptyset, \quad \text{and} \quad j \neq j' \to Q_j \cap Q_{j'} = \emptyset\,.$$

The group G of permutations of $\mathcal{A}$ is defined as follows:

3. For every $i \in \mathbb{N}$, $\tilde{\sigma}_i$ is the cyclic permutation of P_i with $a_{i,0} \mapsto a_{i,1} \mapsto \cdots \mapsto a_{i,p-1} \mapsto a_{i,0}$. In other words, $\tilde{\sigma}_i$ is the permutation of P_i defined by stipulating

$$\tilde{\sigma}_i(a_{i,k}) := \begin{cases} a_{i,k+1} & \text{if } k+1 < p, \\ a_{i,0} & \text{if } k+1 = p. \end{cases}$$

If we replace the elements of P_i with the elements of $\mathbb{Z}/p\mathbb{Z}$, then $\tilde{\sigma}_i$ becomes addition with 1 (modulo p) and $\tilde{\sigma}_i^t$ becomes addition with t (modulo p).

Now, for each $i \in \mathbb{N}$ we extend the permutation $\tilde{\sigma}_i$ of P_i to a permutation σ_i of $\mathcal{A}$ by stipulating

$$\sigma_i(a) := \begin{cases} \tilde{\sigma}_i(a) & \text{if } a \in P_i, \\ a & \text{otherwise.} \end{cases}$$

Similarly, for every $j \in \mathbb{N}$, let $\tilde{\tau}_j$ be the permutation of Q_j defined by stipulating

$$\tilde{\tau}_j(b_{j,l}) := \begin{cases} b_{j,l+1} & \text{if } l+1 < q, \\ b_{j,0} & \text{if } l+1 = q, \end{cases}$$

and like for $\tilde{\sigma}_i$, for each $j \in \mathbb{N}$ we extend the permutation $\tilde{\tau}_j$ of Q_j to a permutation τ_j of $\mathcal{A}$ by stipulating

$$\tau_j(a) := \begin{cases} \tilde{\tau}_j(a) & \text{if } a \in Q_j, \\ a & \text{otherwise.} \end{cases}$$

Now, we define the group G of permutations of $\mathcal{A}$ by requiring

$$\phi \in G \quad \textit{if and only if} \quad \phi = \sigma \circ \tau\,, \tag{1}$$

with

$$\sigma = \prod_{i \in \mathbb{N}} \sigma_i^{k_i} \quad \text{where for each } i \in \mathbb{N},\ k_i \in \{0, \ldots, p-1\}$$

and

$$\tau = \prod_{j \in \mathbb{N}} \tau_j^{l_j} \quad \text{where for each } j \in \mathbb{N},\ l_j \in \{0, \ldots, q-1\}\,.$$

Let $\mathcal{F}$ be the normal filter on G generated by the subgroups

$$\mathrm{fix}_G(E) = \big\{\phi \in G : \forall a \in E\,(\phi\, a = a)\big\} \quad \text{where } E \in \mathrm{fin}(\mathcal{A}),$$

and let $\boldsymbol{\mathcal{V}_{p+q}}$ be the class of all hereditarily symmetric sets. Then, as mentioned above, $\boldsymbol{\mathcal{V}_{p+q}}$ is a permutation model.

Below we shall prove that $\boldsymbol{\mathcal{V}_{p+q}} \models \neg \mathsf{cC}_{p+q} \wedge \neg \mathsf{C}_{p+q} \wedge \mathsf{qC}_{p+q}$. For this, we first prove that cC_{p+q} and C_{p+q} fail in $\boldsymbol{\mathcal{V}_{p+q}}$.

LEMMA 6.2. $\boldsymbol{\mathcal{V}_{p+q}} \models \neg \mathsf{cC}_{p+q} \wedge \neg \mathsf{C}_q \wedge \neg \mathsf{C}_p \wedge \neg \mathsf{C}_{p+q}$.

Proof. Let $\mathscr{F}_q := \{Q_j : j \in \mathbb{N}\}$, let $\mathscr{F}_p := \{P_i : i \in \mathbb{N}\}$, and let $\mathscr{F}_{p+q} := \{P_i \cup Q_j : i, j \in \mathbb{N}\}$. Then $\mathscr{F}_q$ is an infinite family of q-element sets, $\mathscr{F}_p$ is an infinite family of p-element sets, and $\mathscr{F}_{p+q}$ is an infinite family of $(p+q)$-element sets.

First of all note that $\mathscr{F}_q, \mathscr{F}_p, \mathscr{F}_{p+q}$ are sets in $\boldsymbol{\mathcal{V}_{p+q}}$, because $\emptyset$ is a support for all these sets. Now we show that in $\boldsymbol{\mathcal{V}_{p+q}}$, neither of $\mathscr{F}_q, \mathscr{F}_p, \mathscr{F}_{p+q}$ has a choice function (*i.e.*, $\mathsf{C}_q, \mathsf{C}_p, \mathsf{C}_{p+q}$ fail in $\boldsymbol{\mathcal{V}_{p+q}}$), and finally we show that also cC_{p+q} fails in $\boldsymbol{\mathcal{V}_{p+q}}$.

Assume towards a contradiction that there exists a function $f\colon \mathscr{F}_q \to \bigcup \mathscr{F}_q$ in $\boldsymbol{\mathcal{V}_{p+q}}$, such that for each $Y \in \mathscr{F}_q$, $f(Y) \in Y$. Since $f \in \boldsymbol{\mathcal{V}_{p+q}}$, there exists a support $E_f \in \mathrm{fin}(\mathcal{A})$ of f. Let $j_0 \in \mathbb{N}$ be such that $Q_{j_0} \cap E_f = \emptyset$. Since E_f is finite, such a $j_0 \in \mathbb{N}$ exists. Without loss of generality assume that $f(Q_{j_0}) = b_{j_0,0}$ and consider the permutation τ_{j_0}, which belongs to $\mathrm{fix}_G(E_f)$. By definition we have $\tau_{j_0}(Q_{j_0}) = Q_{j_0}$ and $\tau_{j_0}(b_{j_0,0}) = b_{j_0,1}$, where $b_{j_0,0} \neq b_{j_0,1}$. Since $\tau_{j_0} \in \mathrm{fix}_G(E_f)$, we must have $\tau_{j_0}(f) = f$. On the one hand, we have

$$\tau_{j_0}\big(f(Q_{j_0})\big) = \tau_{j_0}(b_{j_0,0}) = b_{j_0,1}\,,$$

on the other hand, since $\tau_{j_0} \in \mathrm{fix}_G(E_f)$, we have

$$f\big(\tau_{j_0}(Q_{j_0})\big) = \tau_{j_0}\big(f(Q_{j_0})\big),$$

but

$$f\big(\tau_{j_0}(Q_{j_0})\big) = f(Q_{j_0}) = b_{j_0,0} \neq b_{j_0,1} = \tau_{j_0}(b_{j_0,0}) = \tau_{j_0}\big(f(Q_{j_0})\big)\,.$$

This shows that there is no support of a choice function $f\colon \mathscr{F}_q \to \bigcup \mathscr{F}_q$, or in other word, there is no choice function for $\mathscr{F}_q$ in $\boldsymbol{\mathcal{V}_{p+q}}$, and since $\mathscr{F}_q$ is a family of q-element sets, this implies that C_q fails in $\boldsymbol{\mathcal{V}_{p+q}}$.

With similar arguments, using the families $\mathscr{F}_p$ and $\mathscr{F}_{p+q}$, we can show that also C_p and C_{p+q} fail in $\boldsymbol{\mathcal{V}_{p+q}}$.

Now, let us assume towards a contradiction that $\boldsymbol{\mathcal{V}_{p+q}} \models \mathsf{cC}_{p+q}$. So there exists a function ζ in $\boldsymbol{\mathcal{V}_{p+q}}$ which assigns to every $Y \in \mathscr{F}_{p+q}$ a cyclic order ζ_Y such that for all $x \in Y$,

$$\zeta_Y^k(x) = x \;\Rightarrow\; (p+q) \mid k.$$

Let $E_\zeta \in \mathrm{fin}(\mathcal{A})$ be a support of ζ. Let $j_0 \in \mathbb{N}$ be such that $Q_{j_0} \cap E_\zeta = \emptyset$ and let $Y_0 \in \mathscr{F}_{p+q}$ be such that $Q_{j_0} \subseteq Y_0$. Since E_ζ is a support of ζ and therefore $\mathrm{fix}_G(E_\zeta) \subseteq \mathrm{sym}_G(\zeta)$ we have that

$$\tau_{j_0} \circ \zeta_{Y_0} = \zeta_{\tau_{j_0}(Y_0)} = \zeta_{Y_0}. \tag{2}$$

Let $a := \zeta_{Y_0}(b_{j_0,0})$. If $a \in Q_{j_0}$ we have that by (2)

$$a = \tau_{j_0}^q(a) = \tau_{j_0}^q \circ \zeta_{Y_0}(b_{j_0,0}) = \tau_{j_0}^{q-1}(\tau_{j_0} \circ \zeta_{Y_0}(b_{j_0,0})) = \tau_{j_0}^{q-1} \circ \zeta_{Y_0}(b_{j_0,0}) = \tau_{j_0}^{q-1}(a) \neq a.$$

This is a contradiction and therefore we have that $a \notin Q_{j_0}$. Let $2 \leq k_0 \leq p+1$ be minimal such that

$$\zeta_{Y_0}^{k_0}(b_{j_0,0}) \in Q_{j_0}$$

and let $k_1 \leq q-1$ be minimal with

$$\tau_{j_0}^{k_1}(\zeta_{Y_0}^{k_0}(b_{j_0,0})) = b_{j_0,0}.$$

Note that $k_1 \geq 1$ since $\zeta_{Y_0}^{k_0}(b_{j_0,0}) \neq b_{j_0,0}$. By (2) we get that

$$b_{j_0,0} = \tau_{j_0}^{k_1}(\zeta_{Y_0}^{k_0}(b_{j_0,0})) = \zeta_{Y_0}^{k_0}(b_{j_0,0}).$$

So, the exponent k_1 is not minimal, which is a contradiction. Hence, there is no function in $\boldsymbol{\mathcal{V}_{p+q}}$ which defines a cyclic order on each $Y \in \mathscr{F}_{p+q}$, which shows that cC_{p+q} fails in $\boldsymbol{\mathcal{V}_{p+q}}$. ⊣

Before we can show that $\boldsymbol{\mathcal{V}_{p+q}} \models \mathsf{qC}_{p+q}$, we have to prove a few facts.

LEMMA 6.3. *Let $S \in \boldsymbol{\mathcal{V}_{p+q}}$, let $E \in \mathrm{fin}(\mathcal{A})$ be a support of S, and for each $x \in S$ let*

$$[x] := \big\{x' \in S : \exists \phi \in \mathrm{fix}_G(E)(\phi\, x = x')\big\}.$$

Then for each $x \in S$, $[x]$ belongs to $\boldsymbol{\mathcal{V}_{p+q}}$. Moreover, the set $\{[x] : x \in S\}$ can be well-ordered in $\boldsymbol{\mathcal{V}_{p+q}}$, i.e., there exists a well-ordering of $\{[x] : x \in S\}$ in $\boldsymbol{\mathcal{V}_{p+q}}$.

Proof. Notice first that for any $x, x' \in S$, the relation

$$x \sim x' :\Longleftrightarrow \exists \phi \in \mathrm{fix}_G(E)(\phi\, x = x')$$

is an equivalence relation. Now, take an arbitrary $x \in S$. Since E is a support of S, for each $\phi \in \mathrm{fix}_G(E)$ we have $\phi\, x \in S$. In particular, for each $\phi \in \mathrm{fix}_G(E)$ we have $\phi\, x \in [x]$. This shows that E is a support of $[x]$, *i.e.*, for all $\phi \in \mathrm{fix}_G(E)$, $\phi([x]) = [x]$. Hence, $[x] \in \boldsymbol{\mathcal{V}_{p+q}}$.

In order to show that there is a well-ordering of $\{[x] : x \in S\}$ in $\boldsymbol{\mathcal{V}_{p+q}}$, recall that the ground model $\boldsymbol{\mathcal{M}}_{p+q}$ was a model of $\mathsf{ZFA} + \mathsf{AC}$. So, in $\boldsymbol{\mathcal{M}}_{p+q}$ there is bijection w between an ordinal α and $\{[x] : x \in S\}$, *i.e.*, $w\colon \alpha \to \{[x] : x \in S\}$. Notice also that since α is in the kernel $\mathbf{V}$, by Fact 6.1, for every $\beta \in \alpha$ and for each $\phi \in G$ we have $\phi\, \beta = \beta$. Now, since for all $\phi \in \mathrm{fix}_G(E)$ and every $x \in S$ we have $\phi([x]) = [x]$, for each $\beta \in \alpha$ we have

$$w(\phi\, \beta) = w(\beta) = \phi\big(w(\beta)\big).$$

This shows that E is a support of w, and hence, $w \in \boldsymbol{\mathcal{V}_{p+q}}$. ⊣

Below we show that every $x \in \boldsymbol{\mathcal{V}_{p+q}}$ has a unique *least closed support*. For this, we introduce first the notion of *closed supports*.

For a finite set $E \in \mathrm{fin}(\mathcal{A})$ we say that E is *closed*, if for all $i, j \in \mathbb{N}$,

$$P_i \cap E \neq \emptyset \to P_i \subseteq E \quad \text{and} \quad Q_j \cap E \neq \emptyset \to Q_j \subseteq E\,.$$

In other words, $E \in \mathrm{fin}(\mathcal{A})$ is closed if and only if E is the union of finitely many blocks P_i and Q_j. Notice that the filter generated by the groups $\mathrm{fix}_G(E^*)$, where E^* is closed, is the same as $\mathscr{F}$. Therefore, every set $x \in \boldsymbol{\mathcal{V}_{p+q}}$ has a closed support. We can even prove that every set has a smallest closed support. This smallest closed support will be called canonical support.

LEMMA 6.4. *If E_x and E'_x are two closed finite supports of some $x \in \boldsymbol{\mathcal{V}_{p+q}}$, then also $E_x \cap E'_x$ is a closed finite support of x. Furthermore, for every $S \in \boldsymbol{\mathcal{V}_{p+q}}$ there is a function in $\boldsymbol{\mathcal{V}_{p+q}}$ which assigns to every set $x \in S$ a canonical closed finite support of x.*

Proof. First notice that the intersection of two closed finite sets is closed. So, it remains to show that if E_x and E'_x are two closed finite supports of x, then also $E_x \cap E'_x$ is a support of x. Let $\phi \in \mathrm{fix}_G(E_x \cap E'_x)$ be an arbitrary permutation. By definition of G, $\phi = \sigma \circ \tau$. First, let $\sigma_1, \tau_1 \in \mathrm{fix}_G(E_x)$ be such that

$$\sigma_1|_{\mathcal{A}\setminus E_x} = \sigma|_{\mathcal{A}\setminus E_x}$$

and

$$\tau_1|_{\mathcal{A}\setminus E_x} = \tau|_{\mathcal{A}\setminus E_x}\,.$$

Furthermore, let $\sigma_2, \tau_2 \in \mathrm{fix}_G(E'_x)$ be such that

$$\sigma_2|_{E_x\setminus E'_x} = \sigma|_{E_x\setminus E'_x} \quad \text{and} \quad \sigma_2 \text{ is the identity on } \mathcal{A}\setminus(E_x\setminus E'_x)\,,$$

and

$$\tau_2|_{E_x\setminus E'_x} = \tau|_{E_x\setminus E'_x} \quad \text{and} \quad \tau_2 \text{ is the identity on } \mathcal{A}\setminus(E_x\setminus E'_x)\,.$$

Then $\sigma\tau = \sigma_2\tau_2\sigma_1\tau_1$. So we can write ϕ as a product of permutations of $\mathrm{fix}_G(E_x) \cup \mathrm{fix}_G(E'_x)$. Hence, since $\phi \in \mathrm{fix}_G(E_x \cap E'_x)$ was arbitrary, this shows that $E_x \cap E'_x$ is a support of x.

Now, let $S \in \boldsymbol{\mathcal{V}_{p+q}}$ be an arbitrary set and let E_S be a support of S. Look at the function which assigns to every set $x \in S$ the set

$$\bigcap\big\{E \in \mathrm{fin}(\mathcal{A}) : E \text{ is a closed support of } x\big\}.$$

Then E_S is a support of this function and therefore, the function is in $\boldsymbol{\mathcal{V}_{p+q}}$. In order to see this, we have to show that if E is a support of x, $\phi(E)$ is a support of $\phi(x)$ for every $\phi \in \mathrm{fix}_G(E_S)$. Let $\psi \in \mathrm{fix}_G(\phi(E))$. For every $e \in E$ we have that $\psi \circ \phi(e) = \phi(e)$. So,

$$\phi^{-1}\circ\psi\circ\phi(e) = \phi^{-1}\circ\phi(e) = e.$$

So, $\phi^{-1}\circ\psi\circ\phi \in \mathrm{fix}_G(E)$. Since E is a support of x, we have that

$$\phi^{-1}\circ\psi\circ\phi(x) = x \;\Rightarrow\; \psi\circ\phi(x) = \phi(x).$$

Therefore, $\psi \in \mathrm{sym}_G(\phi(x))$. So, $\phi(E)$ is indeed a support of $\phi(x)$. ⊣

LEMMA 6.5. *Let $S \in \boldsymbol{\mathcal{V}_{p+q}}$ with support E_S, let $x_0 \in S$, $x, x' \in [x_0]$, where $[x_0]$ is as in Lemma 6.3, and suppose that x and x' have the same canonical support E.*

(a) There is a $\phi \in \mathrm{fix}_G(E_S)$ such that $\phi(x) = x'$, and for every $\phi \in \mathrm{fix}_G(E_S)$ with $\phi(x) = x'$ we have $\phi(E) = E$.

(b) For each $\phi \in \mathrm{fix}_G(E_S)$ with $\phi(E) = E$ we have

$$\phi(x) \neq x \;\leftrightarrow\; \phi(x') \neq x'.$$

Proof. (a) Since $x, x' \in [x_0]$, there is a $\phi \in \mathrm{fix}_G(E_S)$ with $\phi(x) = x'$, and since x and x' have the same canonical support E, for every $\phi \in \mathrm{fix}_G(E_S)$ with $\phi(x) = x'$ we must have $\phi(E) = E$.

(b) For all $\vartheta \in \mathrm{fix}_G(E_S)$, all $F \subseteq \mathcal{A}$, and each $a \in \mathcal{A}$ we define

$$\vartheta|_F(a) := \begin{cases} \vartheta(a) & \text{if } a \in F, \\ a & \text{otherwise.} \end{cases}$$

Let $\phi \in \mathrm{fix}_G(E_S)$ with $\phi(E) = E$ and $\phi(x) = x$. By (a), there is a $\psi \in \mathrm{fix}_G(E_S)$ such that $\psi(x) = x'$ and $\psi(E) = E$. Furthermore, $\psi|_E$ and $\phi|_E$ are permutations of E. So,

$$\phi = \phi|_E \circ \phi|_{\mathcal{A}\setminus E} \quad \text{and} \quad \psi = \psi|_E \circ \psi|_{\mathcal{A}\setminus E}$$

with $\phi|_{\mathcal{A}\setminus E}, \psi|_{\mathcal{A}\setminus E} \in \mathrm{fix}_G(E)$. Since G is a commutative group, we have that

$$x' = \psi \circ \phi \circ \psi^{-1}(x') = \psi|_E \circ \phi|_E \circ \psi|_E^{-1}(x') = \phi|_E \circ \psi|_E \circ \psi|_E^{-1}(x') = \phi|_E(x'),$$

and since $\phi|_{\mathcal{A}\setminus E} \in \mathrm{fix}_G(E)$, this shows that

$$x' = \phi|_E(x') = \phi|_{\mathcal{A}\setminus E} \circ \phi|_E(x') = \phi(x'),$$

which completes the proof. ⊣

In order to prove the main result of this section, we have to define an order on the set of closed supports. For this, we define first a total order on the set of blocks $\{P_i : i \in \mathbb{N}\} \cup \{Q_j : j \in \mathbb{N}\}$.

Let A and B be two distinct elements of $\{P_i : i \in \mathbb{N}\} \cup \{Q_j : j \in \mathbb{N}\}$. We define

$$A < B :\Longleftrightarrow \begin{cases} A = P_i \wedge B = P_{i'} \wedge i < i', \text{ or} \\ A = Q_j \wedge B = Q_{j'} \wedge j < j', \text{ or} \\ A = P_i \wedge B = Q_j. \end{cases}$$

If $A, B \in \{P_i : i \in \mathbb{N}\} \cup \{Q_j : j \in \mathbb{N}\}$, then, by the definition of the group G, for any $\phi \in G$ we have

$$A < B \iff \phi A < \phi B\,.$$

Hence, the relation "$<$" belongs to $\boldsymbol{\mathcal{V}_{p+q}}$.

Now, if $E = \bigcup\{F_1, \ldots, F_n\}$ and $E' = \bigcup\{F'_1, \ldots, F'_m\}$ are both unions of finitely many blocks, then we say that $E \prec E'$ if either $n < m$, or $n = m$ and the $<$-least block of the symmetric difference $\{F_1, \ldots, F_n\} \Delta \{F'_1, \ldots, F'_m\}$ belongs to E. In particular, "$\prec$" defines a total order on the set of closed supports.

Now, we are ready to prove the following

PROPOSITION 6.6. *If p and q are two different primes, then $\boldsymbol{\mathcal{V}_{p+q}} \models \mathsf{q}\mathsf{C}_{p+q}$.*

Proof. Without loss of generality we can assume that $q < p$, because we have that

$$m\mathsf{C}_{m+n} \iff n\mathsf{C}_{m+n}$$

for all natural numbers $n > m$. Let $\mathscr{F} = \{Y_\iota : \iota \in \Lambda\}$ be a family of $(p+q)$-element sets which belongs to $\boldsymbol{\mathcal{V}_{p+q}}$, let $E_{\mathscr{F}}$ be the canonical support of $\mathscr{F}$, and let $\mathscr{X} := \bigcup \mathscr{F}$. By Lemma 6.3, there is a well-ordering of $\{[x] : x \in \mathscr{X}\}$, *i.e.*, there is an ordinal α and a bijection

$$w\colon \alpha \to \{[x] : x \in \mathscr{X}\},$$

where $[x] = \big\{x' \in \mathscr{X} : \exists \phi \in \mathrm{fix}_G(E_{\mathscr{F}})(\phi\, x = x')\big\}$. Recall that since "$\sim$" (defined in the proof of Lemma 6.3) is an equivalence relation, for any $x, x' \in \mathscr{X}$, either $[x] = [x']$ or $[x] \cap [x'] = \emptyset$. Now, take an arbitrary $Y \in \mathscr{F}$. We have to define a function in $\boldsymbol{\mathcal{V}_{p+q}}$ which chooses a non-empty subset of Y which contains at most q elements. If we choose, for example, $\{x, x'\} \subseteq Y$, then, for any $\phi \in \mathrm{fix}_G(E_{\mathscr{F}})$, we choose $\phi\big(\{x, x'\}\big)$ from $\phi(Y)$. So, the function we define with respect to a particular $Y \in \mathscr{F}$ has to be stable with respect to all permutations $\phi \in \mathrm{fix}_G(E_{\mathscr{F}})$. Because then $E_{\mathscr{F}}$ is a support of the function.

For every $\beta \in \alpha$ let

$$\mu_\beta := |w(\beta) \cap Y|\,.$$

Notice that $E_{\mathscr{F}} \cup E_Y$ is a support of $\{w(\beta) \cap Y : \beta \in \alpha\}$, which shows that this set belongs to $\boldsymbol{\mathcal{V}_{p+q}}$. Since $|Y| = p+q$, we have $\sum_{\beta\in\alpha} \mu_\beta = p+q$. Let β_0 be the least ordinal such that $\mu_{\beta_0} > 0$ is not a multiple of q. Notice that this choice is stable with respect to all $\phi \in \mathrm{fix}_G(E_{\mathscr{F}})$.

If $\mu_{\beta_0} \leq q$, then $w(\beta_0) \cap Y$ contains at most q elements and we are done; and if $p \leq \mu_{\beta_0} < p+q$, then $Y \setminus w(\beta_0)$ is a non-empty subset of Y containing less than q elements and we are done.

So, it remains to consider the case when $q < \mu_{\beta_0} < p$ with $q \nmid \mu_{\beta_0}$ or when $\mu_{\beta_0} = p+q$. Let $x_1, \ldots, x_{\mu_{\beta_0}} \in Y$ be such that

$$\{x_1, \ldots, x_{\mu_{\beta_0}}\} = w(\beta_0) \cap Y\,.$$

By definition of $w(\beta_0)$, for any n, n' with $1 \leq n, n' \leq \mu_{\beta_0}$ there is a $\phi \in \mathrm{fix}_G(E_{\mathscr{F}})$ such that $\phi\, x_n = x_{n'}$. For each $1 \leq n \leq \mu_{\beta_0}$, let E_n be the canonical support of x_n and for every $E \in \{E_n : 1 \leq n \leq \mu_{\beta_0}\}$ let

$$\eta(E) := \{n : E = E_n\}\,.$$

Then there are $E, E', E'', \ldots \in \{E_n : 1 \leq n \leq \mu_{\beta_0}\}$ such that the corresponding sets $\eta(E), \eta(E'), \eta(E''), \ldots$ are pairwise disjoint and $|\eta(E)| + |\eta(E')| + |\eta(E'')| + \ldots = \mu_{\beta_0}$. Since μ_{β_0} is not a multiple of q there is a $\prec$-least closed support E_{n_0} such that

$q \nmid |\eta(E_{n_0})|$. Let $s_0 := \eta(E_{n_0})$ and let $x_{m_1}, \ldots, x_{m_{s_0}} \in Y \cap w(\beta_0)$ be such that for all $1 \leq t \leq s_0$, E_{n_0} is the canonical support of x_{m_t}.

If $1 \leq s_0 \leq q$, then $\{x_{m_1}, \ldots, x_{m_{s_0}}\}$ is a non-empty subset of Y which contains at most q elements and we are done. Similarly, if $p \leq s_0 < p + q$, then

$$Y \setminus \{x_{m_1}, \ldots, x_{m_{s_0}}\}$$

is a non-empty set which contains at most q elements and we are done.

So, assume that $q < s_0 < p$ or $s_0 = p + q$, and let

$$y_{-1} := \{x_{m_1}, \ldots, x_{m_{s_0}}\} \subseteq Y \cap w(\beta_0).$$

Notice that since $y_{-1} \subseteq w(\beta_0)$, for all $x, x' \in y_{-1}$ there is a permutation $\phi \in \mathrm{fix}_G(E_{\mathscr{F}})$ such that $\phi(x) = x'$, which shows that $E_{\mathscr{F}}$ is not a support of any $x \in y_{-1}$. In particular, we get that that $E_{n_0} \setminus E_{\mathscr{F}} \neq \emptyset$ (recall that E_{n_0} is a support of each $x \in y_{-1}$). So, let $P_{i_0} < \ldots < P_{i_{u-1}} < Q_{j_u} < \ldots < Q_{j_{u+v-1}}$ be such that

$$E_{n_0} \setminus E_{\mathscr{F}} = \bigcup \{P_{i_0}, \ldots, P_{i_{u-1}}, Q_{j_u}, \ldots, Q_{j_{u+v-1}}\}.$$

Define

$$\tilde{G} := \left\{ \prod_{0 \leq k < u} \sigma_{i_k}^{\kappa_{i_k}} \circ \prod_{0 \leq l < v} \tau_{j_{u+l}}^{\lambda_{j_{u+l}}} : \forall k < u \; \forall l < v \; \left(0 \leq \kappa_{i_k} < p \wedge 0 \leq \lambda_{j_{u+l}} < q\right) \right\}.$$

Let $\phi = \sigma_{i_0}^{\kappa_{i_0}} \circ \cdots \circ \sigma_{i_{u-1}}^{\kappa_{i_{u-1}}} \circ \tau_{j_u}^{\lambda_{j_u}} \circ \cdots \circ \tau_{j_{u+v-1}}^{\lambda_{j_{u+v-1}}} \in \tilde{G}$. Define

$$\phi|_r := \kappa_{i_r} \text{ if } 0 \leq r < u \text{ and } \phi|_r := \lambda_{j_r} \text{ if } u \leq r < u + v.$$

The elements in $\tilde{G}$ can be ordered lexicographically (induced by the linear ordering on the blocks and the exponents of σ and τ). The ordering on $\tilde{G}$ is denoted by "$\leq_{\tilde{G}}$". For all $x, x' \in y_{-1}$ and all $0 \leq r < u + v$ define

$$\mathrm{dist}_r(\langle x, x' \rangle) := \phi|_r,$$

where ϕ is the $\leq_{\tilde{G}}$-smallest element in $\tilde{G}$ with $\phi(x) = x'$.

Claim 1: For all $x, x', x'' \in y_{-1}$ and all $0 \leq r < u + v$ we have that

$$\mathrm{dist}_r(\langle x, x' \rangle) +_w \mathrm{dist}_r(\langle x', x'' \rangle) = \mathrm{dist}_r(\langle x, x'' \rangle),$$

where $w = p$ if $0 \leq r < u$, $w = q$ if $u \leq r < u + v$, and $+_w$ denotes addition modulo w.

Proof of Claim 1. Let $\phi_0, \phi_1, \phi \in \tilde{G}$ be $\leq_{\tilde{G}}$-minimal with

$$\phi_0(x) = x', \quad \phi_1(x') = x'' \quad \text{and} \quad \phi(x) = x''.$$

Assume towards a contradiction that $\phi \neq \phi_1 \circ \phi_0$. This implies $\phi^{-1} \circ \phi_1 \circ \phi_0 \neq \mathrm{id}$, and by definition we have

$$\phi^{-1} \circ \phi_1 \circ \phi_0(x) = x.$$

Let $0 \leq r < u + v$ be the largest number such that

$$\phi^{-1} \circ \phi_1 \circ \phi_0|_r \neq 0.$$

Without loss of generality we assume that $0 \leq r < u$ (*i.e.*, $w = p$). Then let $m \in \mathbb{N}$ with

$$(\phi^{-1} \circ \phi_1 \circ \phi_0)^m|_r = 1.$$

Note that $(\phi^{-1} \circ \phi_1 \circ \phi_0)^m \neq \sigma_{i_r}$ because otherwise we would have that $\sigma_{i_r}(x) = x$ which is a contradiction to the fact that E_{n_0} is the canonical support of x. So, there is a $\varphi \in \tilde{G} \setminus \{\mathrm{id}\}$ with

$$(\phi^{-1} \circ \phi_1 \circ \phi_0)^m = \varphi \circ \sigma_{i_r} \quad \text{and} \quad \varphi <_{\tilde{G}} \sigma_{i_r}.$$

Then $\varphi \circ \sigma_{i_r}(x) = x \Rightarrow \sigma_{i_r}(x) = \varphi^{-1}(x)$. Note that $\varphi^{-1} <_{\tilde{G}} \sigma_{i_r}$. Furthermore, we have $\phi_0|_r \neq 0$ or $\phi_1|_r \neq 0$ or $\phi|_r \neq 0$. Without loss of generality we assume that $\phi_0|_r \neq 0$ (the other cases are similar). Then

$$\phi_0 \circ \sigma_{i_r}^{-1} \circ \varphi^{-1} <_{\tilde{G}} \phi_0$$

and

$$\phi_0 \circ \sigma_{i_r}^{-1} \circ \varphi^{-1}(x) = \phi_0 \circ \sigma_{i_r}^{-1} \circ \sigma_{i_r}(x) = \phi_0(x) = x'.$$

This contradicts the minimality of ϕ_0. $\dashv_{\text{Claim 1}}$

For all non-empty sets $\tilde{y} \subseteq y_{-1}$, all $x \in \tilde{y}$ and all $0 \leq r < u + v$ define

$$\chi_r(x, \tilde{y}) := \{\mathrm{dist}_r(\langle x, x' \rangle) \mid x' \in \tilde{y}\}.$$

These sets have the following properties:

Claim 2: For all $\tilde{y} \subseteq y_{-1}$ and all $x, x' \in \tilde{y}$ we have that

1. $1 \leq |\chi_r(x, \tilde{y})| \leq p$ for all $0 \leq r < u$ and $1 \leq |\chi_r(x, \tilde{y})| \leq q$ for all $u \leq r < u+v$;
2. for all $0 \leq r < u + v$ there is a $k_r \in \mathbb{N}$ such that $\chi_r(x, \tilde{y}) = \chi_r(x', \tilde{y}) +_w k_r$, where $w = p$ if $0 \leq r < u$ and $w = q$ if $u \leq r < u + v$;
3. $|\chi_r(x, \tilde{y})| = |\chi_r(x', \tilde{y})|$;
4. if $x \neq x'$ there is an $0 \leq r < u + v$ such that $\chi_r(x, \tilde{y}) \neq \chi_r(x', \tilde{y})$.

Proof of Claim 2. 1. Note that $0 \in \chi_r(x, \tilde{y})$ since $\mathrm{dist}_r(\langle x, x \rangle) = 0$.

2. Set $k_r := \phi|_r$, where ϕ is $\leq_{\tilde{G}}$-minimal with $\phi(x) = x'$ and use Claim 1.

3. This follows from 2.

4. Let $x, x' \in \tilde{y}$ and let ϕ be $\leq_{\tilde{G}}$-minimal with $\phi(x) = x'$. If $\chi_r(x, \tilde{y}) = \chi_r(x', \tilde{y})$ for all $0 \leq r < u + v$ it follows that $\phi|_r = k_r = 0$ for all $0 \leq r < u + v$. So $\phi = \mathrm{id}$ and therefore $x = x'$. $\dashv_{\text{Claim 2}}$

We define an ordering $\preceq$ on the sets $\chi_r(x,\tilde{y})$ as follows: $\chi_r(x,\tilde{y}) \preceq \chi_r(x',\tilde{y})$ if and only if $\chi_r(x,\tilde{y}) = \chi_r(x',\tilde{y})$ or the smallest integer in the symmetric difference $\chi(x,\tilde{y})\Delta\chi_r(x',\tilde{y})$ belongs to $\chi_r(x,\tilde{y})$.

For all non-empty sets $\tilde{y} \subseteq y_{-1}$, all $0 \leq r < u+v$ and all natural numbers n define $\lambda_{r,n}(\tilde{y})$ as follows: Let $\lambda_{r,0}(\tilde{y}) := \emptyset$ and for every $n \in \mathbb{N} \setminus \{0\}$ let

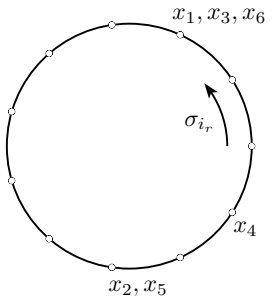
$$\lambda_{r,n}(\tilde{y}) := \left\{ x \in \tilde{y} \setminus \bigcup_{i=0}^{n-1} \lambda_{r,i}(\tilde{y}) : \forall x' \in \tilde{y} \setminus \bigcup_{i=0}^{n-1} \lambda_{r,i}(\tilde{y}) \Big(\chi_r(x,\tilde{y}) \preceq \chi_r(x',\tilde{y}) \Big) \right\}.$$

In other words, $\lambda_{r,1}(\tilde{y})$ is the set of all $x \in \tilde{y}$ such that $\chi_r(x,\tilde{y})$ is $\preceq$-minimal, $\lambda_{r,2}(\tilde{y})$ is the set of all $x \in \tilde{y}$ such that $\chi_r(x,\tilde{y})$ is the second smallest set with respect to $\preceq$ and so on. Note that the union of all $\lambda_{r,n}(\tilde{y})$ is equal to $\tilde{y}$. Note that $\bigcup_{n\in\omega} \lambda_{r,n}(\tilde{y}) = \tilde{y}$ and only finitely many $\lambda_{r,n}(\tilde{y})$ are non-empty.

To illustrate the construction, we consider the following example:

Let $p = 11$, $0 \leq r < u$, $\tilde{y} = \{x_1, \ldots, x_6\}$, and

$$\begin{aligned} \chi_r(x_1,\tilde{y}) = \chi_r(x_3,\tilde{y}) = \chi_r(x_6,\tilde{y}) &= \{0,6,8\}, \\ \chi_r(x_2,\tilde{y}) = \chi_r(x_5,\tilde{y}) &= \{0,2,5\}, \\ \chi_r(x_4,\tilde{y}) &= \{0,3,9\}. \end{aligned}$$



Then we have, for example, $\{0,6,8\} +_{11} 3 = \{0,3,9\}$ and $\{0,3,9\} +_{11} 2 = \{0,2,5\}$. Moreover, $\lambda_{r,1}(\tilde{y}) = \{x_2, x_5\}$, $\lambda_{r,2}(\tilde{y}) = \{x_4\}$, $\lambda_{r,3}(\tilde{y}) = \{x_1, x_3, x_6\}$ and $\lambda_{r,n} = \emptyset$ for all $n \geq 4$.

In the last step, we choose at most q elements from Y, which is done by induction on r. For each $0 \leq r < u+v$ we define a non-empty set $y_r \subseteq y_{-1}$ with $q \nmid |y_r|$ and show that y_{u+v-1} contains at most q elements. Notice that $q \nmid |y_{-1}|$.

Assume that for some r with $0 \leq r < u+v-1$, y_{r-1} with $q \nmid |y_{r-1}|$ is already defined. Then there are three cases:

Case 1: $0 \leq r < u$ *and* $|\chi_r(x,y_{r-1})| \neq p$, *or* $u \leq r < u+v$ *and* $|\chi_r(x,y_{r-1})| \neq q$.

In this case we define

$$y_r := \lambda_{r,n_0}(y_{r-1}),$$

where n_0 is the least positive integer such that $\lambda_{r,n_0}(y_{r-1}) \neq \emptyset$ and $|\lambda_{r,n_0}(y_{r-1})|$ is not a multiple of q. Notice that since $q \nmid |y_{r-1}|$ and

$$\sum_{i=1}^{\infty} |\lambda_{r,i}(y_{r-1})| = |y_{r-1}|,$$

the integer n_0 is well-defined.

Case 2: $u \leq r < u+v$ *and for all* $x \in y_{r-1}$, $|\chi_r(x, y_{r-1})| = q$.

In this case, let $l := |y_{r-1}|$. Notice that $q \nmid l$ and that by definition of $\chi_r(x, y_{r-1})$ we have $q < |y_{r-1}|$. So, there exists a unique natural number $m \leq q$ and pairwise disjoint sets $Z_1, \ldots, Z_m \subseteq y_{r-1}$ with

$$\sum_{i=1}^{m} |Z_i| = l,$$

such that for every $1 \leq i \leq m$, all $x, x' \in Z_i$ the $\leq_{\tilde{G}}$-smallest function $\phi \in \tilde{G}$ with $\phi(x) = x'$ satisfies

$$\phi|_r = 0.$$

If there is a set Z_i (for some $1 \leq i \leq m$) such that $|Z_i| = 1$, we define

$$W_0 := \{Z_i : 1 \leq i \leq m \ \wedge \ |Z_i| = 1\}.$$

Then, since $m \leq q < |y_{r-1}|$, W_0 is a proper subset of the set of all Z_i's. Otherwise let

$$W_0 := \{Z_i : 1 \leq i \leq m \ \wedge \ q \nmid |Z_i|\}.$$

Then W_0 is a proper subset of the set of all Z_i's. If $|W_0| = 1$, let y_r be the unique set which belongs to W_0. Now, if $|W_0| > 1$, then for each $1 \leq i, j \leq m$ such that $Z_i, Z_j \in W_0$ define

$$d_i := \min\{\phi|_r : \text{there is a } j \in \{1, \ldots, m\} \setminus \{i\} \text{ such that for all } z_i \in Z_i \text{ there is a } z_j \in Z_j \text{ such that } \phi \text{ is } \leq_{\tilde{G}} \text{-minimal with } \phi(z_i) = z_j\}.$$

Define $d := \min\{d_i : 1 \leq i \leq m \ \wedge \ Z_i \in W_0\}$. Then the set

$$W_1 := \{Z_i \in W_0 : d_i = d\}$$

is a proper non-empty subset of W_0. If $|W_1| > 1$, then we repeat this process, starting with the set W_1 instead of W_0, and obtain a non-empty set W_2 with $|W_2| < |W_1|$. After repeating this process at most m times, we finally obtain a set $W = \{Z_{i_0}\}$ which contains a unique set Z_{i_0} (for some $i_0 \in \{1, \ldots, m\}$) with $q \nmid Z_{i_0}$ and we define

$$y_r := Z_{i_0}.$$

Case 3: $0 \leq r < u$ *and for all* $x \in y_{r-1}$, $|\chi_r(x, y_{r-1})| = p$.

In this case, first notice that since $|\chi_r(x, y_{r-1})| = p$ we have $p \leq |y_{r-1}|$. Now, if $p \leq |y_{r-1}| < p + q$, then the set $y_{-1} \setminus y_{r-1}$ contains at most q elements and we are done. So, we can assume that $|y_{r-1}| = p + q$, and we can argue similar as in Case 2.

Finally, we consider y_{u+v-1}, which is a subset of Y, and show that y_{u+v-1} contains at most q elements. For this, let

$$\{x_0, x_1, \ldots, x_q\} \subseteq y_{u+v-1}.$$

We show that at least two of the x_i's are equal, *i.e.*, y_{u+v-1} does not contain a $(q+1)$-element subset. Let $\phi \in \tilde{G}$ be $\leq_{\tilde{G}}$-minimal such that there is a $k \in \{1, \ldots, q\}$ with

$$\phi(x_0) = x_k.$$

By construction of y_{u+v-1}, for each r with $0 \leq r < u+v$ we have $\phi|_r = 0$. Therefore, $\phi = \tau_{j_v}^{l_k}$ for an $l_k \in \{1, \ldots, q-1\}$. Moreover, for each $i \in \{1, \ldots, q\}$ there is an $l_i \in \{1, \ldots, q-1\}$ with

$$\tau_{j_v}^{l_i}(x_0) = x_i.$$

Since there are more i's than l_i's, there must be distinct $i, i' \in \{1, \ldots, q\}$ with

$$l_i = l_{i'}.$$

Therefore, $x_i = \tau_{j_v}^{l_i}(x_0) = \tau_{j_v}^{l_{i'}}(x_0) = x_{i'}$, which shows that $x_i = x_{i'}$. ⊣

The following theorem summarizes the preceding results.

THEOREM 6.7. *For all primes* p *and* q *with* $p \neq q$, $\neg\mathsf{cC}_{p+q} \wedge \neg\mathsf{C}_{p+q} \wedge \neg\mathsf{C}_p \wedge \neg\mathsf{C}_q \wedge \mathsf{qC}_{p+q}$ *is relatively consistent with* ZF.

Proof. By Lemma 6.2 and Proposition 6.6 we have

$$\boldsymbol{\mathcal{V}_{p+q}} \models \neg\mathsf{cC}_{p+q} \wedge \neg\mathsf{C}_{p+q} \wedge \neg\mathsf{C}_p \wedge \neg\mathsf{C}_q \wedge \mathsf{qC}_{p+q}\,.$$

So, by Pincus [9, §4B, p. 737], there exists a model $\mathbf{V}$ of ZF such that

$$\mathbf{V} \models \neg\mathsf{cC}_{p+q} \wedge \neg\mathsf{C}_{p+q} \wedge \neg\mathsf{C}_p \wedge \neg\mathsf{C}_q \wedge \mathsf{qC}_{p+q}\,,$$

which shows that the statement $\neg\mathsf{cC}_{p+q} \wedge \neg\mathsf{C}_{p+q} \wedge \neg\mathsf{C}_p \wedge \neg\mathsf{C}_q \wedge \mathsf{qC}_{p+q}$ is relatively consistent with ZF. ⊣

As an immediate consequence we get

COROLLARY 6.8. *If* p *and* q *are two different primes, then* qC_{p+q} *implies neither* cC_{p+q} *nor* C_{p+q}.

References

[1] Andreas Blass, *Existence of bases implies the axiom of choice*, in ***Axiomatic Set Theory*** (James E. Baumgartner, Donald A. Martin, and Saharon Shelah, eds.), Contemporary Mathematics, vol. 31, American Mathematical Society, Providence, RI, 1984, pp. 31–33.

[2] Lorenz J. Halbeisen, ***Combinatorial set theory, with a gentle introduction to forcing***, 2nd ed., [Springer Monographs in Mathematics], Springer-Verlag, London, 2017.

[3] James D. Halpern, *Bases in vector spaces and the axiom of choice*, ***Proceedings of the American Mathematical Society***, vol. 17 (1966), 670–673.

[4] Wilfrid Hodges, *Krull implies Zorn*, ***J. London Math. Soc. (2)***, vol. 19 (1979), no. 2, 285–287.

[5] Paul Howard and Jean E. Rubin, ***Consequences of the axiom of choice***, Mathematical Surveys and Monographs, vol. 59, American Mathematical Society, Providence, RI, 1998.

[6] Thomas J. Jech, ***The Axiom of Choice***, North-Holland Publishing Co., Amsterdam-London; Amercan Elsevier Publishing Co., Inc., New York, 1973, Studies in Logic and the Foundations of Mathematics, Vol. 75.

[7] Wolfgang Krull, *Idealtheorie in Ringen ohne Endlichkeitsbedingung*, ***Mathematische Annalen***, vol. 101 (1929), 729–744.

[8] Hans Läuchli, *Coloring infinite graphs and the Boolean prime ideal theorem*, ***Israel Journal of Mathematics***, vol. 9 (1971), 422–429.

[9] David Pincus, *Zermelo-Fraenkel consistency results by Fraenkel-Mostowski methods*, ***The Journal of Symbolic Logic***, vol. 37 (1972), 721–743.

[10] Richard P. Stanley, *Zero square rings*, ***Pacific J. Math.***, vol. 30 (1969), 811–824.

[11] Martin M. Zuckerman, *Choosing l-element subsets of n-element sets*, ***Pacific Journal of Mathematics***, vol. 96 (1981), 247–250.