Canonical Set Theory for Classic Mathematics

A Linear Order On Finite Groups and Structures, with a Natural Extension to Infinite Structures

Juan Pablo Ramírez Ramírez

Abstract We provide an axiomatic base for the set of natural numbers, that has been proposed as a canonical construction, and use this definition of $\mathbb{N}$ to find several results on finite group theory. Every finite group G, is well represented with a natural number N_G; if $N_G = N_H$ then H, G are in the same isomorphism class. We have a linear order on all finite groups, that is well behaved with respect to cardinality. In fact, if H, G are two finite groups such that $|H| = m < n = |G|$, then $H < \mathbb{Z}_n \leq G$. There is also a canonical order for the elements of G and we can define equivalent objects of G. This allows us to find the automorphisms of G. The Cayley table of G takes canonical block form, and a minimal set of independent equations that define the group is obtained. We show how to find all groups of order n, and order them. Examples are given using all groups with order smaller than 10. The canonical block form of the symmetry group Δ_4 is given and we find its automorphisms. These results are extended to the infinite case. A real number is an infinite set of natural numbers. A real function is a set of real numbers, and a sequence of real functions $f_1, f_2, \ldots$ is well represented by a set of real numbers, as well. We make brief comments on treating the calculus of real numbers. In general, we represent mathematical objects using the smallest possible data-type. In the last section, mathematical objects are well assigned to tree structures. We conclude with brief comments on type theory and future work on computational and physical aspects of these representations.

Keywords Structuralism · Set Theory · Type Theory · Arithmetic Model · Data Type · Tree · Group

PACS 02.10.v · 03.67.Lx · 03.67.a

Mathematics Subject Classification (2010) 03-04 · 03C55 · 03D75 · 03H15 · 03C13 · 05C05 · 06F15

Declarations

Funding

Not Applicable

Conflict of Interest Statement

This work has been carried out independently of any university, institution or grants and all material here contained has been rightfully and honestly developed by the author who claims full authorship, with no conflicts of interest. Some of the material has been presented at lectures in Universidad de Guanajuato/CIMAT; Universidad de Guadalajara; Second School of Logic and Set Theory (2013, UNAM, Morelia); National Congress of Mathematics (2019, Monterrey, México).

Availability of data and material

Not applicable

Code availability

Not applicable

Guadalajara, Jalisco, México
E-mail: juan.rmz236@gmail.com

Introduction

The present work is part of a broader attempt in proposing an optimal universe for classical mathematics. The construction presented in [Ramirez(2019)], is the first exposition of natural and real numbers, defined as *set numbers*. Here, we focus on finite structures, and group theoretic aspects of this proposal. The constructions are self contained. We provide a definition of operation, group, field and linear space that allow the constructions of the next sections. These definitions were explored in [Ramirez(2015)], but the exposition has been revised. In the second section, we proceed with a description of natural numbers as the set of hereditarily finite sets, **HFS**. This is an axiomatic treatment, and details for proofs not given in [Ramirez(2019)], are given here. An order $<$ and operation $\oplus$ are given, on **HFS**, isomorphic to the natural numbers $\mathbb{N}(<,+)$. This is a canonical representation of natural numbers in set theory. In particular, Von-Neumann and Zermelo-Fraenkel ordinals are embedded sub orders of our construction.

In the third section we provide a method of representing a finite function as a natural number. If A, B are two finite collections, and $f : A \to B$ a function, we assign a unique natural number N_f. We can do this whether the objects of f are abstract or concrete. We have an equivalence relation on the class of finite functions, and a linear order on the quotient space. This induces a linear order on the subset of all finite permutations, that is well defined with respect to cardinality. If η_m, η_n are permutations of $m < n$ objects, then $\eta_m < \mathbf{1}_n \leq \eta_n \leq \mathbf{id}_n$ where $\mathbf{1}_n$ is the one-cycle permutation of n objects and $\mathbf{id}_n$ is the identity permutation of n objects. This representation gives a good definition for equivalent functions; we can say when two functions are equivalent. Given a function, we will also be able to identify which objects of the function are equivalent.

Next, we focus on the formal definition of finite groups. We give the definition of canonical form for a group, where a single natural number is used to represent the group. This reduces the problem of proving two finite groups are isomomorphic, to finding the canonical representation of these groups and compare these natural numbers. We provide the method for finding all groups of order n, and finding their canonical representation. We find the linear order for all groups with $|G| < 10$ is

$$\mathbb{Z}_1 < \mathbb{Z}_2 < \mathbb{Z}_3 < \mathbb{Z}_4 < \mathbb{Z}_2^2 < \mathbb{Z}_5 < \mathbb{Z}_6 < D_6 < \mathbb{Z}_7 < \mathbb{Z}_8 < Q_8 < D_8 < \mathbb{Z}_2 \oplus \mathbb{Z}_4 < \mathbb{Z}_2^3 < \mathbb{Z}_9 < \mathbb{Z}_3^2 < \cdots,$$

where D_n is the Dihedral group and Q_8 is the quaternion group. In general, $\mathbb{Z}_n \leq G$ if $|G| = n$ so that the order is well behaved with respect to cardinality. The order induced on commutative groups of order n also behaves well with respect to factorization of n. Intuitively, a commutative group is larger than another if it is expressed in terms of more factors. For example, $\mathbb{Z}_8 < \mathbb{Z}_2 \oplus \mathbb{Z}_4 < \mathbb{Z}_2^3$. We also have $\mathbb{Z}_9 < \mathbb{Z}_3^2$. In this section we also provide the automorphisms for all groups $|G| < 10$. We also find the twenty four automorphisms of Δ_4.

Then we give an overview of the infinite case of these results, which is a model for real numbers. We mention a general outline on treating concepts of calculus, which will be described in full in a separate publication. The study of real numbers is reduced to the study of natural numbers. However, the gap (conceptual and practical) between these two kinds of objects is enormous, in most axiomatic treatments. Our construction of natural numbers, will allow us to express the continuum of real numbers as an extension of natural numbers. It is not necessary to build intermediate structures such as $\mathbb{Z}$ or $\mathbb{Q}$, although we do provide brief descriptions of these structures. Just as we are able to reduce a finite group to a natural number, we will have some similar results in the infinite case. For example, we are able to express a real function as a set of real numbers. More surprisingly, a sequence of real functions is also a set of real numbers. The general idea is that we can reduce the complexity of objects to its minimum possible. In the last section we express mathematical objects using tree structures. Natural numbers are finite trees, real numbers are infinite trees and we will give a general description of mathematical objects.

1 Groups, Fields and Linear Spaces

In most axiomatic constructions of numerical systems, the set of integers is defined in terms of a quotient space of $\mathbb{N} \times \mathbb{N}$. Then, the rational numbers are defined in terms of a quotient space of $\mathbb{Z} \times \mathbb{Z}$. We take an alternate approach by defining the operation of a group as a function $X \to (X \to X)$. A description of fields and linear spaces is also given. A linear space is defined as an abelian group $V(\oplus)$, together with a field of automorphisms $\mathscr{B}(\oplus, \circ) \subset \mathbf{Aut}\, V(\oplus)$, where $\oplus$ is addition of automorphisms induced by the operation of $V(\oplus)$ and $\circ$ is composition. The definitions and propositions, of this section, enable us to have trivial proofs in the theory of set numbers of Section 2.

Definition 1 *Let G a non empty set, and $\mathbf{Aut}\, G$ be the set of bijective functions of the form $G \to G$. A function $G \to \mathbf{Aut}(G)$ is called an operation on the set G. A set of functions $B \subseteq \mathbf{Aut}\, G$ is said to be balanced if $\mathbf{id}_G \in B$, and if $x \in B$ implies $x^{-1} \in B$. Let $* : G \to B$ a bijective function, for some balanced set B. If*

$$*(x) \circ *(y) = *(*(x)(y)), \tag{1}$$

for every $x, y \in G$, we say $*$ is a group structure.

The functions $*(x)$ are called *operation functions of* $*$. We remark that the expression $*(x)(y) \in G$ is the image of y under the action of $*(x)$. Thus, $*(*(x)(y)) \in \mathbf{Aut}\, G$ is the image of $*(x)(y) \in G$ under the action of $*$.

Theorem 1 *The definitions of group and group structure are equivalent.*

Proof Suppose we have a group structure. Then we can verify

- – Identity Element. There exists an object $e \in G$ such that $*(e) = \mathbf{id}_G$. Therefore, $*(e)(x) = x$ for all $x \in G$. This means $e * x = x$ for all $x \in G$. Now we have to prove $x * e = x$. We have $*(*(x)(e)) = *(x) \circ *(e) = *(x)$. Since $*$ is injective, $*(x)(e) = x$.
- – Inverse Element. Let $a \in G$, then there exists a unique $a^{-1} \in G$ such that $*(a^{-1}) = (*(a))^{-1}$ is the inverse function of $*(a)$. This is a direct consequence of the definition of balanced set. We must show $a * a^{-1} = a^{-1} * a = e$. It is enough to prove $a^{-1} * a = e$. We know $a^{-1} * a = *(a^{-1})(a) = (*(a))^{-1}(a)$. But, $*(a)(e) = a$. This means $(*(a))^{-1}(a) = e$.
- – Associativity.

$$
\begin{aligned}
x * (y * z) &= *(x)(y * z) \\
&= *(x)(*(y)(z)) \\
&= (*(x) \circ *(y))(z) \\
&= *(*(x)(y))(z) \\
&= (*(x)(y)) * z \\
&= (x * y) * z.
\end{aligned}
$$

For the the second part of this proof, we simply have to prove that a group G defines a group structure. The operation functions of the group structure are defined in terms of the cosets xG; define $*(x)$ by $g \mapsto_{*(x)} x * g$. We can easily verify $*$ is an injective function and it is onto a balanced set. The associative property implies (1). □

We use the equivalence of groups and group structures to find the basic properties of groups.

Theorem 2 *Let $G(*)$ a group with operation $*$. Then, we verify*

1. *Right cancellation; $*(a)(c) = *(b)(c)$ implies $a = b$.*
2. *Left cancellation; $*(c)(a) = *(c)(b)$ implies $a = b$.*
3. *Uniqueness of identity and inverse elements.*
4. *Inverse of inverse; $(x^{-1})^{-1} = x$.*
5. *Existence of unique solutions; given $a, b \in G$ there exists a unique $x \in G$ such that $*(a)(x) = b$, and a unique $y \in G$ such that $*(y)(a) = b$.*

Proof The first part requires to apply the function $*$, so that $*(*(a)(c)) = *(*(b)(c))$ which implies $*(a) \circ *(c) = *(b) \circ *(c)$. Right cancellation of functions gives $*(a) = *(b)$. We conclude $a = b$ because $*$ is bijective. We can similarly prove the second part if we use left cancellation of functions.

Let e_1, e_2 be identity elements. If we consider e_1 as identity we get $*(e_1)(e_2) = e_2$, and if we consider e_2 identity we get $*(e_1)(e_2) = e_1$. Therefore $e_1 = e_2$. The uniqueness of the inverse is trivial. If a_1, a_2 are inverse elements of a, then $*a(a_1) = e = *a(a_2)$ implies $a_1 = a_2$ because of left cancellation.

Let $y = x^{-1}$, so that $*(x)$ and $*(y)$ are inverse functions; $(*(x))^{-1} = *(y)$ and $(*(y))^{-1} = *(x)$. The inverse element of $y = x^{-1}$ is the object z such that $*(z)$ is the inverse function of $*(y)$. Therefore, x is the inverse of y and we conclude $(x^{-1})^{-1} = x$.

For the last part, consider a, b fixed. We know $*(a)$ is a bijective function $G \to G$ so that their exists a unique $x \in G$ such that $*(a)(x) = b$. On the other hand, we would like to find a function $*(y)$ that sends a to b. We see that $b * (a^{-1} * a) = b$, which can be rewritten as $(*(b) \circ *(a^{-1}))(a) = b$. The function $*(b * a^{-1}) = *(*(b)(a^{-1})) = *(b) \circ *(a^{-1})$ sends a to b so that $y = b * a^{-1}$ is our solution. Suppose we have a second object w that satisfies the property of y. Then $*(y)(a) = *(w)(a)$ which is equivalent to $y * a = w * a$ which in turn implies $y = w$ if we use right cancellation. □

Proposition 1 *A group structure, $*$, defines a new function $\bar{*} : G \to \mathbf{Aut}(G)$ such that $\bar{*}(a)(b) = *(b)(a) = b * a$. The function $\bar{*}$ is also a group structure. The two group structures $*, \bar{*}$ are equivalent in the sense that they generate isomorphic groups.*

Proof Let us first prove $\bar{*}$ is a group structure. We must show $\bar{*}$ is a function $\bar{*} : G \to B$, where the image $Im\,\bar{*} = B$ is a balanced subset of $\mathbf{Aut}(G)$. Every object $a \in G$ is assigned a unique function $\bar{*}(a)$, and $\bar{*}(e) = \mathbf{id}_G$ for exactly one object $e \in G$. Next we prove $\bar{*}(a)$ is bijective. First of all, it is injective. Take $\bar{*}(a)(x) = \bar{*}(a)(y)$ which is equivalent to the expression $x * a = y * a$, then $x = y$ because of right cancellation. This proves $\bar{*}(a)$ is injective. Let us prove $\bar{*}(a)$ is onto G. Let $b \in G$, then there exists a solution x to the equation $x * a = b$ which is equivalent to $\bar{*}(a)(x) = b$. This proves $\bar{*}(a)$ is a bijection. Now let us prove the inverse function of $\bar{*}(a)$ is equal to $(\bar{*}(a))^{-1} = \bar{*}(a^{-1}) \in Im(\bar{*})$. We know, by definition, $\bar{*}(a^{-1})(x) = x * a^{-1}$. We also know $\bar{*}(a)$ acts by $\bar{*}(a)(x * a^{-1}) = (x * a^{-1}) * a = x$, which implies the inverse function $(\bar{*}(a))^{-1}$ acts by $(\bar{*}(a))^{-1}(x) = x * a^{-1}$. This proves $\bar{*}(a^{-1}) = (\bar{*}(a))^{-1}$. So far, we have proven the image of $\bar{*}$ is a balanced set. To prove $\bar{*}$ is injective, take two objects $x, y \in G$ such that $\bar{*}(x) = \bar{*}(y)$. Then, $x = \bar{*}(x)(e) = \bar{*}(y)(e) = y$. Now we prove $\bar{*}$ satisfies the associative property. For all $a, b \in G$

$$
\begin{aligned}
\bar{*}(\bar{*}(a)(b))(x) &= \bar{*}(b * a)(x) \\
&= x * (b * a) \\
&= (x * b) * a \\
&= \bar{*}(a)(x * b) \\
&= \bar{*}(a)(\bar{*}(b)(x)) \\
&= (\bar{*}(a) \circ \bar{*}(b))(x),
\end{aligned}
$$

for all $x \in G$. This proves $\bar{*}$ is a group structure.

Let $G(*)$ be the group generated by $*$ and $G(\bar{\ast})$ the group generated by $\bar{\ast}$, then x^{-1} is the same inverse element under both operations. The inverse of $a*b$, under $*$, is equal to $b^{-1}*a^{-1}$. The inverse of $a*b = b\bar{\ast}a$, under $\bar{\ast}$, is equal to $a^{-1}\bar{\ast}b^{-1} = b^{-1}*a^{-1}$. These two groups are isomorphic by $x \mapsto x^{-1}$. To prove, take $\phi(a*b) = (a*b)^{-1} = b^{-1}*a^{-1} = \phi(b)*\phi(a) = \phi(a)\bar{\ast}\phi(b)$. □

Definition 2 *In general the functions $*(x)$ and $\bar{\ast}(x)$ are not equal. When they are equal, we say the object x commutes. A group is abelian if its two generating functions are equal, $* = \bar{\ast}$.*

Proposition 2 *Let $G(*)$ an operation on the set G. The following are equivalent statements.*

1. *The operation $*$ is associative.*
2. *$*(*(x)(y)) = *(x) \circ *(y)$ for all $x, y \in G$.*
3. *$*(x) \circ \bar{\ast}(y) = \bar{\ast}(y) \circ *(x)$ for all $x, y \in G$.*

Proof The equivalence of 1. and 2. was proven in Theorem 1. Now we prove the equivalence of 1. and 3. Let $z \in G$, then

$$
\begin{aligned}
(*(x) \circ \bar{\ast}(y))(z) &= *(x)(\bar{\ast}(y)(z)) \\
&= *(x)(z*y) \\
&= x*(z*y) \\
&= (x*z)*y \\
&= \bar{\ast}(y)(x*z) \\
&= \bar{\ast}(y)(*(x)(z)) \\
&= (\bar{\ast}(y) \circ *(x))(z)
\end{aligned}
$$

If we suppose 3. holds, then we can prove associativity,

$$
\begin{aligned}
x*(z*y) &= *(x)(z*y) \\
&= *(x)(\bar{\ast}(y)(z)) \\
&= (*(x) \circ \bar{\ast}(y))(z) \\
&= (\bar{\ast}(y) \circ *(x))(z) \\
&= \bar{\ast}(y)(*(x)(z)) \\
&= \bar{\ast}(y)(x*z) \\
&= (x*z)*y
\end{aligned}
$$

□

We have the following useful result, for consequent sections. It gives a practical means of proving associativity. If the elements of G commute and the operation functions also commute, then the operation is associative.

Proposition 3 *If $*$ is a commutative operation on the set G, and $*(x) \circ *(y) = *(y) \circ *(x)$, for all $x, y \in G$, then $*$ is associative.*

Proof Given our hypothesis, we have the equalities $*(x) \circ \bar{\ast}(y) = *(x) \circ *(y) = *(y) \circ *(x) = \bar{\ast}(y) \circ *(x)$. Our result follows from 3. and 1. of the last proposition. □

Definition 3 *Let $G(*)$ a group and let $H \subseteq G$ be a subset of the set G. Define $*_H$ as the function $*$ restricted to H. If $*_H$ is a group structure we say it is a subgroup of $G(*)$.*

For $H \subset G$ to be a subgroup of G it is necessary that the image of H, under the action of $*_H(h)$, be equal to H, for all $h \in H$. In short, $*_H(h)[H] = H$, for all $h \in H$. This means H *is closed under the operation* $*$.

Definition 4 *Given two groups $G_1(*_1)$ and $G_2(*_2)$, a homomorphism is a function $\phi : G_1(*_1) \to G_2(*_2)$ such that*

$$
\phi(*_1(a)(b)) = *_2(\phi(a))(\phi(b)).
$$

The set of all homomorphisms from $G_1(*_1)$ to $G_2(*_2)$ is represented by the notation $\mathbf{Hom}(G_1, G_2)$, when no confusion arises with respect to the operations of each group.

If the homomorphism is injective as function then we call it a monomorphism, and if it is surjective as function we call it an epimorphism. If the function is bijective we have an isomorphism, or automorphism, $\phi : G \to G$. The set of all automorphisms of $G(*)$ is represented with the notation $\mathbf{Aut}\, G(*)$.

We use the notation $\mathbf{Aut}(G)$ and $\mathbf{Aut}\, G(*)$ to differentiate between bijective functions and automorphisms.

Theorem 3 *Let X a set, then the composition operation $\circ$ is a group structure for the set of all bijective functions $\mathbf{Aut}\,X$. A subset $B \subseteq \mathbf{Aut}\,X$ that is balanced and closed under composition is a subgroup $B(\circ) \subset \mathbf{Aut}\,X$.*

A group structure $* : G \to B$, induces an isomorphism $* : G(*) \to B(\circ)$.

The composition operation is a group structure for the set of automorphisms $\mathbf{Aut}\,G(*)$. A balanced and closed subset, $\mathscr{B} \subseteq \mathbf{Aut}\,G(*)$, is a subgroup $\mathscr{B}(\circ) \subset \mathbf{Aut}\,G(*)$.

Proof For the first part, we have a function $\circ : \mathbf{Aut}\,X \to \mathbf{Aut}(\mathbf{Aut}\,X)$. If $f \in \mathbf{Aut}\,X$, then $\circ(f) : \mathbf{Aut}\,X \to \mathbf{Aut}\,X$ is the function that acts by $\circ(f)(g) = f \circ g$. We have to prove $\circ : \mathbf{Aut}\,X \to B$ is a bijective function, and the image $Im \circ = B \subset \mathbf{Aut}(\mathbf{Aut}\,X)$ is a balanced set. Every object in $\mathbf{Aut}\,X$ is assigned a function $\circ(f) \in \mathbf{Aut}(\mathbf{Aut}\,X)$. To see $\circ$ is injective, take two objects $f, g \in \mathbf{Aut}\,X$ and suppose $\circ(f) = \circ(g)$. This implies $f = f \circ \mathbf{id}_X = g \circ \mathbf{id}_X = g$. Now we focus on the image of $\circ$. We first prove the objects in the image are bijective functions $\mathbf{Aut}\,X \to \mathbf{Aut}\,X$. Suppose $\circ(f)(g) = \circ(f)(h)$, for two $g, h \in \mathbf{Aut}\,X$. That is to say, $f \circ g = f \circ h$ and because of cancellation of bijections, we have $g = h$. This means $\circ(f)$ is injective. To prove $\circ(f)$ is onto $\mathbf{Aut}\,X$, take any $g \in \mathbf{Aut}\,X$, and we find $\circ(f)(x) = f \circ x = g$ for $x = f^{-1} \circ g$. We also know the image of $\circ$ is balanced because $\circ(\mathbf{id}_G) \in \mathbf{Aut}(\mathbf{Aut}\,X)$ and $(\circ(f))^{-1} = \circ(f^{-1}) \in \mathbf{Aut}(\mathbf{Aut}\,X)$. The associative property is the usual associativity of composition of functions. This proves the first assertion of the first part. The second assertion of the first part is trivial. Take $B(\circ)$ balanced and closed under composition. This makes $B(\circ)$ a subgroup.

For the second part, we must prove $*$ is an isomorphism. From the first part of this theorem we know $B(\circ)$ is a group. We also know $*$ is a bijection. We use definition 4 and associativity, in G, to verify $*(*(x)(y)) = *(x) \circ *(y) = \circ(*(x))(*(y))$. This proves that the group structure $*$ produces an isomorphism $G(*) \to B(\circ)$, where $B(\circ)$ is the image of $*$ with the operation $\circ$.

The third part of this theorem is proven similarly to the first part of this theorem.   □

We define the *distributive property* for two operations on a single set. We also define rings and fields.

Definition 5 *Let $K(+)$ a group with identity 0; the set $K - \{0\}$ is represented by K_0. Let $\cdot : K_0 \to \mathscr{C} \subset \mathbf{Hom}(K, K)$ operation. We say $\cdot$ distributes over $K(+)$, because*

$$\cdot(x)(+(a)(b)) = +(\cdot(x)(a))(\cdot(x)(b)).$$

Let $R(+)$ an abelian group, and let $\cdot$ a second operation that distributes over $R(+)$. Suppose $\cdot$ is associative and suppose $\cdot 1 = \mathbf{id}_R$ for a unique non trivial element $1 \in R_0$. We say $R(+, \cdot)$ is a ring and if $\cdot$ is commutative, the ring is abelian.

Let $K(+, \cdot)$ a ring and suppose $Im(\cdot) = \mathscr{C} \subset \mathbf{Aut}\,K(+)$ is a balanced set of automoprhisms. Then $K(+, \cdot)$ is a skew field. If the ring $K(+, \cdot)$ is abelian, we say $K(+, \cdot)$ is a field.

We start using a new notation $*x$ for the operation function $*(x)$. The distributive property holds when we have a group $K(\cdot)$ whose operation functions $\cdot x$, are homomorphisms on the original group $K(+)$. Our conditions give us the relations $\cdot x(0) = 0$, for all $x \in K$. Therefore, we define $\cdot 0(x) = 0$. The operation function $\cdot 0$ is the trivial function $\mathbf{0} : K \to \{0\}$.

Corollary 1 *A field is an abelian group $K(+)$ together with a second abelian group $K(\cdot)$ that distributes over $K(+)$.*

Theorems 4 and 5, below, characterize linear spaces and modules. A linear space is an abelian group $V(\oplus)$, together with a field of automorphisms of $V(\oplus)$. Although these two theorems are not explicitly used in the following sections, it is useful for the last section on real numbers. Given an abelian group $V(\oplus)$, we can provide a second operation on $\mathbf{Hom}(V, V)$, apart from composition. The operation $\oplus$ of V naturally induces a closed operation on $\mathbf{Hom}(V, V)$. This allows us to define modules and linear spaces. Define addition of homomorphisms by $(f \oplus g)(x) = f(x) \oplus g(x)$. If $\mathscr{B} \subset \mathbf{Aut}\,V(\oplus)$ we write $\mathscr{B}(\oplus)$ to emphasize we are considering the set together with addition, not composition. The trivial function $\mathbf{e} : V \to \{e\}$ acts as an identity object under addition of homomorphisms, $f = f \oplus \mathbf{e} = \mathbf{e} \oplus f$. Let $f \in \mathbf{Aut}\,V(\oplus)$, and $-f \in \mathbf{Aut}\,V(\oplus)$ the automorphism defined by $-f(x) = -(f(x))$ where $-(f(x))$ is the additive inverse of $f(x)$; we use the notation $-x$ for the inverse of x under $\oplus$. We easily verify $f \oplus (-f) = \mathbf{e}$. A set of automorphisms $\mathscr{B}(\oplus)$ is balanced if $\mathbf{e} \in \mathscr{B}(\oplus)$, and if $f \in \mathscr{B}(\oplus)$ implies $-f \in \mathscr{B}(\oplus)$.

Lemma 1 *Let $V(\oplus)$ an abelian group with identity e, and $\mathscr{B}(\oplus) \subset \mathbf{Aut}\,V(\oplus)$ a balanced set. If $\mathscr{B}(\oplus)$ is closed under addition of automorphisms, then $\mathscr{B}(\oplus)$ is an abelian group with identity e.*

Proof This result is telling us an easy way of knowing if $\mathscr{B}(\oplus)$ is a group with addition of functions. We of course require that $\mathscr{B}(\oplus)$ be balanced. Under addition of automorphisms, the inverse of f is the function $-f$ that acts by $x \mapsto -(f(x))$. The inverse of $\mathbf{id}_V$ is $-\mathbf{id}_V$ that makes $x \mapsto -x$. Associativity in $V(\oplus)$ implies associativity in $\mathscr{B}(\oplus)$. The commutative property in $\mathscr{B}(\oplus)$ also follows from the commutative property in $V(\oplus)$.   □

Theorem 4 *Let $V(\oplus)$ an abelian group and suppose $\mathscr{B}(\circ) \subset \mathbf{Aut}\,V(\oplus)$ is a balanced, closed and commutative set of automorphisms with composition. Suppose $\mathscr{B}(\oplus)$ is balanced and closed with addition. Then $\mathscr{B}(\oplus, \circ)$ is a field. We say $V(\oplus)$ is a linear space over the field of automorphisms $\mathscr{B}$. The elements of $V(\oplus)$ are called vectors.*

Proof With respect to composition, it is sufficient to verify $\mathscr{B}(\circ)$ is balanced, closed and abelian. From the third part of Theorem 3, we conclude $\mathscr{B}(\circ)$ is an abelian subgroup of $\mathbf{Aut}\,V(\oplus)$. If the conditions of the Lemma hold, then $\mathscr{B}(\oplus)$ is a group. Now

we have to show the distributive property holds. This is the simple statement that $\circ f$ is a homomorphism on $\mathscr{B}(\oplus)$. This is expressed by $f \circ (g \oplus h) = (f \circ g) \oplus (f \circ h)$. Let $x \in V$, then

$$
\begin{aligned}
(f \circ (g \oplus h))(x) &= f(g(x) \oplus h(x)) \\
&= f(g(x)) \oplus f(h(x)) \\
&= (f \circ g)(x) \oplus (f \circ h)(x) \\
&= ((f \circ g) \oplus (f \circ h))(x)
\end{aligned}
$$

This proves $\mathscr{B}(\oplus, \circ)$ is a field. Now we shall prove we have the structure of a linear space, in the classic sense. The scalar product is simply the application of an automorphism to a vector. Let $f \in \mathscr{B}$, then the scalar product of f, with a vector $v \in V$, is defined as $f \cdot v = f(v)$. First, $(f \cdot g) \cdot v = (f \circ g)(v) = f(g(v)) = f \cdot (g \cdot v)$ because $\circ$ is the product of the field. Also, $f \cdot (u \oplus v) = (f \cdot u) \oplus (f \cdot v)$ because $f \in \textbf{Aut}\, V(\oplus)$. By definition of addition of functions, $(f \oplus g) \cdot v = (f \cdot v) \oplus (g \cdot v)$. This result is telling us is that a linear space is defined by an abelian group V and a set of automorphisms (of V) that form a field.   □

We similarly define a module M over a ring.

Theorem 5 *Let $M(\oplus)$ an abelian group and suppose $\mathscr{B}(\circ) \subset \textbf{Hom}(M, M)$ is a closed set of homomorphisms with composition, and $\textbf{id}_M \in \mathscr{B}(\circ)$. Suppose $\mathscr{B}(\oplus)$ is balanced and closed. Then $\mathscr{B}(\oplus, \circ)$ is a ring. We say $M(\oplus)$ is a module over the ring of homomorphisms $\mathscr{B}$.*

2 Finite Sets and Natural Numbers

Finding a mathematical collection of objects that behave under rules that we can interpret as the order and operation of addition for natural numbers, is not an easy task. This problem was taken up by many mathematicians at the beginning of the last century. When we talk about spacial geometry we understand we are referring to objects called *points, lines and planes*. In general we talk of collections of points, such as circles, or others. Just in the same way, if we wish to formalize the theories of arithmetic and analysis, we have to know what objects we are dealing with. The solution was found that we can formulate the statements of arithmetic, and later analysis, using an elementary concept, *set*. Attempts were then made to find set representations of numbers and to model the structure of natural numbers, using sets.

Being an elementary concept, we can not describe a set in terms of other mathematical objects. Rather, we describe all mathematical objects using the language of sets. A set can only be defined linguistically, as a *collection of objects*. But, it has been found that a definition this ambiguous, leads to more problems than it solves. The trick is to find a collection of sets that is well enough defined to serve our purposes, and that does not lead to conceptual paradoxes that have been pointed out in the literature. The problem is that considering arbitrary collections we can have strange sets such as $\{\{\{\cdots\{\{\cdots\}\}\cdots\}\}\}$ and other collections we do not need for the construction of $\mathbb{N}$. Although it has been found that we can incorporate such sets to an appropriate set theory, here we will take a different view. We will try to find the simplest possible representation of natural numbers and real numbers, as sets. The two most widely used models of mathematics begin by describing the natural numbers as *Hereditarily Finite Sets*. This collection of sets, which we denote **HFS**, consists of the sets obtained in the following procedure. We say the set with no objects, $\emptyset$, is in **HFS**. Also, if $x_1, x_2, \ldots, x_n$ are objects in **HFS**, then the collection of these, $\{x_1, x_2, \ldots, x_n\}$, is also in **HFS**. When we wish to make the statement, that an object x is in a set X we denote this with $x \in X$. Let us construct sets using these parameters. We immediately know the collection $\{\emptyset\}$ is an object in **HFS**. Now that we have $\emptyset$ and $\{\emptyset\}$ in **HFS**, we know that the collection of these two objects, $\{\emptyset, \{\emptyset\}\}$ is also in **HFS**. Then, we can take $\emptyset$ and $\{\emptyset, \{\emptyset\}\}$ to find $\{\emptyset, \{\emptyset, \{\emptyset\}\}\} \in$ **HFS**. We can also use the sets $\{\emptyset\}$ and $\{\emptyset, \{\emptyset\}\}$ to find $\{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \in$ **HFS**, etc. The first difficulty we have is ordering these sets so that we can model the order of natural numbers.

The solution Zermelo and Fraenkel found is to order a sub collection of **HFS**. Notice it is trivial to order the sets $\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\{\{\emptyset\}\}\}$, …. We can intuitively say that these sets are ordered by contention. If we only consider these sets, we have the order of natural numbers, $\mathbb{N}_< = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \ldots\}$. Then we have to find a way of defining addition of these sets, in such a way that it serves as a model of addition of natural numbers. This simply means, we have to find an operation on these sets, that is commutative, associative and has an identity element. Proving these statements is usually tedious and laborious. But, the real difficulty arises in understanding the constructions and objects used to describe more complicated structures such as the integer numbers, rational numbers, and real numbers. These have to be built in terms of each other. Integers are described in terms of natural numbers. Rational numbers are described in terms of integers, and real numbers are defined in terms of rational numbers. The last step, in building real numbers, gives objects that are difficult to describe and work with, leading to a gap in most undergraduate students' learning since most programs do not include these constructions. Even modern day efforts to describe the real number system do not provide an easy way to understand the nature of the object we call *real number*. The second approach taken in describing the order of natural numers is due to Von Neumann. He begins by ordering the sets $\emptyset < \{\emptyset\} < \{\emptyset, \{\emptyset\}\} < \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} < \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$. Here, we say that one of these sets, x, is smaller than an other, y, if $x \in y$. Of course, we can easily verify this order is transitive and anti symmetric. This approach has some advantages in simplifying some proofs for the order and addition of natural numbers. However, when building the later numerical structures, we have a similar situation as in the Zermelo-Fraenkel theory. The greater difficulty arises in building the real numbers. These constructions and their technical aspects can be consulted in [Bernays(1991)].

The fact that we have at least two different constructions, gave way to another question, formally referred to as Benaceraff's Identification Problem. It has a great deal to do more with the Philosophy of Mathematics, than the mathematical models in

use, but it still has wide implications. The main statement is set forth in a publication titled *"What Numbers Could Not Be"*, [Benacerraf(1965)]. The argument is made that numbers are actually not sets because there is no absolute way of describing them in terms of sets. In fact, numbers do not exist at all. We are simply taking abstract objects, and giving them properties we want them to satisfy. But, there is no entities satisfying these properties; we make it all up. For example, we can not know what object the number 3 is. Zermelo-Fraenkel say $3 = \{\{\{\emptyset\}\}\}$, but Von Neumann says $3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$. Who are we to believe? One school of thought says, nobody. This section is a proposal for a canonical set theory that allows us to identify what set any *number* is. We will do this for natural numbers and real numbers, and this will lead to a theory of types we briefly discuss in the conclusions for later work. We take the approach of defining natural numbers as objects in **HFS**. However, the main difference with the other two constructions is that we order all of the sets in **HFS**, thus proving $\mathbb{N} = $ **HFS**. An interesting thing happens. The sets used in Z-F and VN are sub orders of our construction of $\mathbb{N}$. Let us be precise with this. Z-F set theory assigns the numbers $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\{\emptyset\}\}$, $3 = \{\{\{\emptyset\}\}\}$, $4 = \{\{\{\{\emptyset\}\}\}\}$, etc. Our construction of natural numbers assigns the Z-F objects to the numbers $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\{\emptyset\}\}$, $4 = \{\{\{\emptyset\}\}\}$, $16 = \{\{\{\{\emptyset\}\}\}\}$, $2^{16} = \{\{\{\{\{\emptyset\}\}\}\}\}$, ...

Thus, we can say Z-F Fraenkel ordinals are the sub order $\{0, 1, 2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \ldots, 2^{2^{2^{\cdot\cdot\cdot}}}, \ldots\} \subset \mathbb{N}$. On the other hand, VN set theory assigns $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$, $3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, etc. Our construction of natural numbers assigns the VN objects to the numbers $0 = \emptyset$, $1 = \{\emptyset\}$, $3 = \{\emptyset, \{\emptyset\}\}$, $11 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, ... The VN ordinals are the sub order $\{0, 2^0, 2^0 + 2^{2^0}, 2^0 + 2^{2^0} + 2^{(2^0 + 2^{2^0})}, \ldots, n, n + 2^n, \ldots\} \subset \mathbb{N}$. Each of these constructions, Z-F and VN, order strict sub sets of $\mathbb{N}$. In this section we construct the structure of natural numbers using an order and addition operation on the set of all hereditarily finite sets. Our order and operation will be defined simultaneously in constructive manner.

2.1 Motivation

There is an intuitive motivation behind the axiomatic base given in this section. We discuss this now, to help understand the structure of order and addition of natural numbers, that we will be using. When adding numbers in base 10 (or base $b > 2$) we have to use sequences of digits to represent natural numbers. We must specify how many times we consider each power of b. But, with binary representation we use a more elementary language. It suffices to specify if the power is considered or not, $\in, \notin$. This means that a natural number is determined by a set of smaller natural numbers, that are those that appear as power in binary form. For example, the number $7 = 2^0 + 2^1 + 2^2$ is determined by the set $\{0, 1, 2\}$. This is commonly referred to as Ackermann Coding or BIT-predicate. This is an important part of the practical aspects this work has, since we are able to model mathematical systems directly in terms of classic computational processes. The Ackermann coding does not give a means for adding numbers in any special manner. We have the same means of operating. Namely, carry over algorithms. This happens because when we add numbers we treat them as a sequence.

Here, we define addition treating natural numbers as sets. Let us consider the following addition of numbers $7 + 13 = (2^0 + 2^1 + 2^2) + (2^0 + 2^2 + 2^3)$. We are going to consider two new sets, the powers that are not repeated $(2^1 + 2^3)$, and the powers that repeat $(2^0 + 2^2)$. In terms of sets, we are considering the symmetric difference $\{1, 3\}$ and the intersection $\{0, 2\}$. Here we make the following observation. To add a power of 2 with itself we simply add 1 to the power. So, we can consider the sum $7 + 19 = (2^1 + 2^3) + (2^{0+1} + 2^{2+1}) = (2^1 + 2^3) + (2^1 + 2^3)$. Iterate the process, so we have to add 1 to the repeated powers. This gives $7 + 9 = 2^{1+1} + 2^{3+1} = 2^2 + 2^4 = 20$. If A, B are two finite sets of natural numbers, we can add them using this method. Form two new sets $A' = A \triangle B$ and $B' = s(A \cap B)$, where s is a function that adds 1 to the elements of $A \cap B$. Then we have $A \oplus B = A' \oplus B'$. But, this alone does not get us anywhere. We have reduced the sum of two sets, $A \oplus B$, to the sum of two new sets $A' \oplus B'$. The sum $A' \oplus B'$ is in turn reduced to a sum $A'' \oplus B''$, etc. So basically, we have done nothing. However, this is not the case, since we can guarantee that in a finite number of iterations the intersection $A^{(n)} \cap B^{(n)} = \emptyset$ becomes the empty set. This yields our final answer $A^{(n+1)}$, because we have $A \oplus B = A^{(n+1)} \oplus B^{(n+1)} = A^{(n+1)} \oplus s(\emptyset) = A^{(n+1)}$. Let us apply this reasoning with another example, $15 + 23 = 38$, from Figure 1. We have the addition $A \oplus B = \{0, 1, 2, 3\} \oplus \{0, 1, 2, 4\}$ because $15 = 2^0 + 2^1 + 2^2 + 2^3$ and $23 = 2^0 + 2^1 + 2^2 + 2^4$. We find that $A' = A \triangle B = \{3, 4\}$ and $A \cap B = \{0, 1, 2\}$, so that $B' = \{0 + 1, 1 + 1, 2 + 1\} = \{1, 2, 3\}$. We iterate the process with $A'' = A' \triangle B' = \{1, 2, 4\}$ and $B'' = s(A \cap B) = \{3 + 1\} = \{4\}$. We can view this process as a Finite State Machine. A state is composed of two columns, each column is a finite configuration of energy-levels. A particle in the basic level is 1 unit, a particle in level 1 is worth 2 units. A particle in level 2 represents four units, etc. A finite configuration of particles in a column is representative of a set number in the obvious way so that each state is a pair of natural numbers. The initial state $\mathbf{S}(t_0)$ is given by the initial summands A, B. The next state, $\mathbf{S}(t_1)$ is again given by two columns. The configuration of the left column, is given by the energy levels that were not repeated in state $\mathbf{S}(t_0)$. The right column in $\mathbf{S}(t_1)$ is given by the objects that do repeat, but we displace these one level up. The configuration of state $\mathbf{S}(t_2)$ is defined similarly in terms of state $\mathbf{S}(t_1)$. The left column of state $\mathbf{S}(t_2)$ is given by the energy levels not repeated in state $\mathbf{S}(t_1)$. The configuration in the right column of state $\mathbf{S}(t_2)$ is given by the energy levels repeated in state $\mathbf{S}(t_1)$, but one level up. In a finite number of steps we reach a stable state with no occupation in the right column, giving us our result in the left column. It will not be difficult for the reader to prove the number of steps to reach stability is bounded above by $\max(A \cup B)$. For example, it takes at most $8 = \max(\{0, 1, 2, 3, 5, 6, 8\})$ states to find $\{0, 3, 6\} \oplus \{0, 1, 2, 5, 8\}$.

We will provide an addition operation for finite sets, and this operation is isomorphic to $\mathbb{N}_+$. The sum of two sets is expressed as the sum of two new sets, in a process that ends in finite steps. We take the view that an operation is a function whose domain is a space of functions itself; $* : A \to (AfA)$ where AfA is the set of all functions $A \to A$. This way, the operation $\oplus$ of sets is defined in terms of its functions $\oplus n$. Each function makes $\oplus n(x) = n \oplus x$. We begin by defining the function $\oplus 1$ which not only generates the hereditarily finite sets, it also generates the set of operation functions $\oplus n$. The family of functions $\oplus n$ is generated by a single function $\oplus 1$, all others being powers of composition, $\oplus 2 = \oplus 1 \circ \oplus 1$, $\oplus 3 = \oplus 1 \circ \oplus 1 \circ \oplus 1$, etc. In the forthcoming,
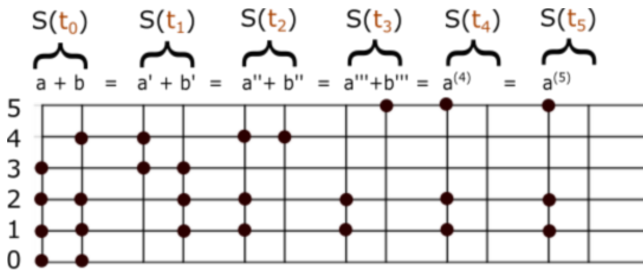
Fig. 1 Graphic Representation of $15 + 23 = 38$.

consider the usual symmetric difference of sets, $A \triangle B = (A \cup B)/(A \cap B)$, and the partition $A \cup B = (A \triangle B) \cup (A \cap B)$. We define two base cases $0 = \emptyset$ and $1 = \{\emptyset\}$, along with a recursive function $\oplus 1 : \textbf{HFS} \rightarrow \textbf{HFS}$ defined by

$$\oplus 1(A) = (A \triangle 1) \oplus s(A \cap 1), \tag{2}$$

where $s : \textbf{HFS} \rightarrow \textbf{HFS}$ sends every set $X = \{x\}_{x \in X}$ to the set $s(X) = \{\oplus 1(x)\}_{x \in X}$. Applying the function s to the set X simply means we apply $\oplus 1$ to every object of X. In the following calculations we use the fact that $s(\emptyset) = \emptyset$. Furthermore, we define $A \oplus \emptyset = \emptyset \oplus A = \emptyset$ which simply defines $\emptyset$ as the identity element.

First we have $\oplus 1(0) = (0 \triangle 1) \oplus s(0 \cap 1) = 1 \oplus s(\emptyset) = 1 \oplus \emptyset = 1$. The function $\oplus 1$ generates every element of **HFS** when applied successively.

$$
\begin{aligned}
2 &= \oplus 1(1) = (1 \triangle 1) \oplus s(1 \cap 1) = \emptyset \oplus s(1) = s(1) = \{\oplus 1(0)\} = \{1\} \\
3 &= \oplus 1(2) = (2 \triangle 1) \oplus s(2 \cap 1) = (\{1\} \triangle \{0\}) \oplus s(\{1\} \cap \{0\}) = \{0,1\} \oplus s(\emptyset) \\
&= \{0,1\} \oplus \emptyset = \{0,1\} \\
4 &= \oplus 1(3) = (3 \triangle 1) \oplus s(3 \cap 1) = \{1\} \oplus s(\{0\}) = 2 \oplus \{\oplus 1(0)\} = 2 \oplus \{1\} \\
&= 2 \oplus 2
\end{aligned}
$$

Here we come upon a new object. We must find a suitable definition for $2 \oplus 2$, and in general we will need to find a suitable definition for $A \oplus B$. We simply extend our definition in the obvious way,

$$A \oplus B = (A \triangle B) \oplus s(A \cap B).$$

This gives

$$2 \oplus 2 = (2 \triangle 2) \oplus s(2 \cap 2) = \emptyset \oplus s(2) = \{\oplus 1(1)\} = \{2\}.$$

Therefore,

$$4 = \{2\}.$$

This simply means the set $\{2\} = \{\{1\}\} = \{\{\{\emptyset\}\}\}$ is the object we know as *the number 4*. We continue to generate sets, by applying the function $\oplus 1$ to the result.

$$
\begin{aligned}
5 &= \oplus 1(4) = (4 \triangle 1) \oplus s(4 \cap 1) = \{0,2\} \oplus s(\emptyset) = \{0,2\} \\
6 &= \oplus 1(5) = (5 \triangle 1) \oplus s(5 \cap 1) = \{2\} \oplus s\{0\} = \{2\} \oplus \{1\} = (\{2\} \triangle \{1\}) \oplus s(\{2\} \cap \{1\}) = \{1,2\} \oplus s(\emptyset) = \{1,2\} \\
7 &= \oplus 1(6) = (6 \triangle 1) \oplus s(6 \cap 1) = \{0,1,2\} \oplus s(\emptyset) = \{0,1,2\} \\
8 &= \oplus 1(7) = (7 \triangle 1) \oplus s(7 \cap 1) = \{1,2\} \oplus s\{0\} = \{1,2\} \oplus \{1\} \\
&= (\{1,2\} \triangle \{1\}) \oplus s(\{1,2\} \cap \{1\}) = \{2\} \oplus s\{1\} = \{2\} \oplus \{2\} = (\{2\} \triangle \{2\}) \oplus s(\{2\} \cap \{2\}) = \emptyset \oplus s\{2\} = \emptyset \oplus \{3\} \\
&= (\emptyset \triangle \{3\}) \oplus s(\emptyset \cap \{3\}) = \{3\} \oplus s(\emptyset) = \{3\} \\
9 &= \oplus 1(8) = (8 \triangle 1) \oplus s(8 \cap 1) = \{0,3\} \oplus s(\emptyset) = \{0,3\} \\
10 &= \oplus 1(9) = (9 \triangle 1) \oplus s(9 \cap 1) = \{3\} \oplus s\{0\} = \{3\} \oplus \{1\} = (\{3\} \triangle \{1\}) \oplus s(\{3\} \cap \{1\}) = \{1,3\} \oplus s(\emptyset) = \{1,3\}.
\end{aligned}
$$

The set $\{\emptyset, \{\{\emptyset\}\}\}$ is the number 5. To find the set that is the number 6, we use the definition of addition of two sets to find $\{2\} \oplus \{1\} = \{1,2\} \oplus s(\emptyset) = \{1,2\} = \{\{\emptyset\}, \{\{\emptyset\}\}\}$. We notice, first of all, that the sum of two disjoint sets is the union, and secondly that every natural number is a set of *smaller* natural numbers. When we refer to hereditarily finite sets, in this manner, we call them *set numbers* because we give them the structure of natural numbers. Let N be a natural number with binary representation $\sum_{i=1}^{n} 2^{a_i}$, then N is the set number $\{a_1, a_2, \ldots, a_n\}$. For example, $5 = \{0,2\}$ because $5 = 2^0 + 2^2$, while $6 = \{1,2\}$ because $6 = 2^1 + 2^2$. We can easily find $11 = \{0,1,3\}$.

$$11 = 5 \oplus 6 = \{0,2\} \oplus \{1,2\} = \{0,1\} \oplus s(\{2\}) = \{0,1\} \oplus \{3\} = \{0,1,3\}.$$

We find

$$11 = 7 \oplus 4 = \{0,1,2\} \oplus \{2\} = \{0,1\} \oplus s(\{2\}) = \{0,1,3\}.$$

The fact that the binary representation is involved is not a coincidence. Let us look at this from another point of view, and consider the number 13. We wish to find its natural representation so we start with its binary elements $13 = \{0,2,3\}$. Then, $2 = \{1\}$ and $3 = \{0,1\}$. But, $1 = \{0\}$ so that we only need to assign $0 = \emptyset$ as the base case. We finally get $13 = \{\emptyset, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$ which is the same we obtain from $(11 \oplus 1) \oplus 1$. We give an adequate axiomatic base for proving thee statements. We construct mathematical sets, using hereditarily finite sets and the axioms we need are stated in the following subsection.

2.2 Axiomatic Base

We begin with the empty set and the set that contains that set, $0 = \emptyset$ and $1 = \{\emptyset\}$. Notice that using our definition of addition of sets allows to build all hereditarily finite sets. But, if we simply used union and intersection, we can not generate more sets beyond 0 and 1. So, our definition $A \oplus B = (A \triangle B) \oplus s(A \cap B)$ allows us to lift off the ground and generate new sets. We will have an axiom for the following statement. If x is a set, then the object $\oplus 1(x)$ is a set. If this axiom should be true we first need for the union and intersection of sets to be sets, because the function $\oplus 1$ is defined in terms of union and intersection of sets. This raises the following question. Why are we able to generate new sets, using $\oplus 1$, if it is defined in terms of $\cap, \cup$, which do not generate new sets? The reason is because $\oplus 1$ is also defined in terms of itself when we say $\oplus 1(0) = 1$ and $\oplus 1(1) = \{\oplus 1(0)\} = \{1\}$. Adding an object to the elements of a set is what allows us to find $2,3,4,\ldots$.

We give the axiomatic base for this model of $\mathbb{N}$. We assume the existence of the empty set $0 = \emptyset$ and the set that contains 0; the set $1 = \{\emptyset\}$. We also assume the union of sets and the intersection of sets, is a set. We will also assume any sub collection of a set, is a set. This will be the first part of our axioms. Our second axiom is the statement that $\oplus 1$ sends sets to sets. This axiom states that every set in **HFS** is obtained by applying the function $\oplus 1$ sufficiently many times. It simply states that no matter how many times we apply $\oplus 1$, we will always get a new object in **HFS**. These new objects we obtain from the function, are called sets and we find them in linear order. Once we have this, we use the union axiom to find $\mathbb{N} = \bigcup_n \oplus 1^n(0)$ is a set. It is the set that contains all the objects, generated by $\oplus 1$ and $0,1$. This is the set of natural numbers $\mathbb{N} = $ **HFS**. In this section we provide the axioms needed for the formal construction of $\mathbb{N}$. In a later section we will see that real numbers are infinite sets of natural numbers, and we will provide an additional axiom in order to construct larger sets.

Axiom 1 *The empty collection $\emptyset$ is a set, as is the collection $\{\emptyset\}$. If A, B are two sets then $A \cup B$ is a set, and $A \cap B$ is a set. If A is a set, then any sub collection $X \subset A$ is also a set.*

With this first axiom, we are not able to go beyond the sets $\emptyset$ and $\{\emptyset\}$. The following definition and axiom will allow us to build all hereditarily finite sets, in linear order.

Define the set operation $\oplus$ with $A \oplus B = (A \triangle B) \oplus \{x \oplus 1\}_{x \in A \cap B}$.

To make our definition good, we set $\oplus 0(x) = x$. We have seen in the last sub section, how to find $\oplus 1(1)$, $\oplus 1(2), \ldots$. When carrying out the calculations for $3 \oplus 1$ we recognized that it was necessary to know the value of $\oplus 2(2)$.

If we continue to apply $\oplus 1$, we encounter more calculations of the form $\oplus x(y)$. But, the operation function for $\oplus x$ is explicitly dependent of $\oplus 1$. The functions $\oplus x$ are defined as powers of $\oplus 1$, but to find $\oplus 1$ we also need to start finding $\oplus x$. The reason for this is that the operation functions build each other simultaneously, as we have seen in the calculations above.

Axiom 2 *The operation function $\oplus 1$ generates all **HFS** when applied successively to 0. The order in which sets are generated is an order of **HFS**, equivalent to the order of natural numbers $\mathbb{N}_{\leq}$.*

This axiom states that every set in **HFS** is obtained by applying the function $\oplus 1$ successively to 0. That is to say, every hereditarily finite set is of the form $(\oplus 1 \circ \oplus 1 \circ \cdots \circ \oplus 1)(0) = 1 \oplus (1 \oplus (1 \oplus \cdots (1 \oplus 0)))$. Furthermore, our construction of finite sets is at the same time providing an order because we construct the finite sets *in order*,

$$0 \to_{\oplus 1} 1 \to_{\oplus 1} 2 \to_{\oplus 1} 3 \to_{\oplus 1} 4 \to_{\oplus 1} \cdots.$$

That is to say, hereditarily finite sets are ordered in terms of the order of construction. The order in which we find the elements of **HFS** is the natural order given to these. An important difference between this construction, and the Von-Neumann Ordinals and the Zermelo-Fraenkel Ordinals is that we order all **HFS**, while the latter two order transitive subsets of **HFS**. We have given an order $<$ and operation $\oplus$, on **HFS**, that are isomorphic to $\mathbb{N}(\leq)$ and $\mathbb{N}(+)$, respectively. The commutative property of $\oplus$ is trivial because symmetric difference and intersection are commutative.

$$\begin{aligned} A \oplus B &= (A \triangle B) \oplus s(A \cap B) \\ &= (B \triangle A) \oplus s(B \cap A) \\ &= B \oplus A \end{aligned}$$

The easiest way to prove associative property of set sum is to prove the functions $\oplus x$ and $\bar{\oplus}y$ commute, for every set numbers x, y. Given that commutativty holds, we know $\oplus y = \bar{\oplus}y$. It is sufficient to prove the commutative property holds for operation functions, $\oplus x \circ \oplus y = \oplus y \circ \oplus x$, because of Proposition 3.

Proposition 4 *The associative property holds for $\oplus$.*

Proof Let $a \in \mathbb{N}$, our second axiom states that to add n we must apply $\oplus 1$ a total of n times, $\oplus n(a) = \oplus 1^n(a)$. This proves the operation functions $\oplus m, \oplus n$ commute,

$$
\begin{aligned}
(\oplus n \circ \oplus m)(a) &= \oplus n(\oplus m(a)) \\
&= \oplus 1^n(\oplus 1^m(a)) \\
&= \oplus 1^m(\oplus 1^n(a)) \\
&= \oplus m(\oplus n(a)) \\
&= (\oplus m \circ \oplus n)(a).
\end{aligned}
$$

We are simply using the fact that $f^n \circ f^m = f^m \circ f^n$ for any bijection f. $\square$

Now we give the following result which provides a practical way of defining the natural order of **HFS**, and which will allow us to define our order of finite groups, among other applications such as real analysis which we will see briefly at the end. Take two distinct natural numbers A, B and consider their symmetric difference $A \triangle B$ which is not empty and is bounded. That is to say, $\max(A \triangle B)$ exists. Furthermore, this maximum is in exactly one of the two sets, not in both. We compare two sets in terms of this object, $\max(A \triangle B)$. The set that contains this object is the largest of the two. For example, $15 = \{0, 1, 2, 3\} < \{4\} = 16$ because $A \triangle B = \{0, 1, 2, 3, 4\}$ and the maximum of this set is in $16 = \{4\}$.

Theorem 6 *If A, B are two set numbers, then $A < B$ if and only if $\max(A \triangle B) \in B$.*

Before proving this theorem, let us provide some examples. The set number $A = \{1, 5, 6\} = 96$ is smaller than the set number $B = \{0, 7\} = 129$ because $\max(A \triangle B) = 7 \in B$. For a second example, consider $A = \{2, 3, 6, 7\}$ and $B = \{0, 1, 2, 3, 6, 7\}$.

Proof Let $A = \{a_1, a_2, \ldots, a_n\}$ be a set number, and suppose B is a set number such that $A < B$. From the second axiom we know that the set number B is obtained by successively adding 1 to the set number A. This means $B = \oplus 1^n(A)$ for some $n \in \mathbb{N}$. We shall prove $\max(A \triangle B) \in B$ for every $B > A$. In this proof we will use the fact that $A \oplus B = A \cup B$ if $A \cap B = \emptyset$; this is a direct consequence of the addition of the definition of addition for set numbers. We start with $A \oplus 1 = \{a_1, a_2, \ldots, a_n\} \oplus \{0\}$. There are two cases; $0 \notin A$ or $0 \in A$. In the first case, $A \oplus 1 = \{0, a_1, a_2, \ldots a_n\}$ which implies $\max(A \triangle (A \oplus 1)) = \max\{0\} = 0 \in A \oplus 1$. Now consider the second case; suppose $a_1 = 0$. Then we have $A \oplus 1 = \{0, a_2, \ldots, a_n\} \oplus \{0\} = \{a_2, a_3, \ldots, a_n\} \oplus \{1\}$. We have two sub cases; $1 \notin A$ or $1 \in A$. In the first case, $A \oplus 1 = \{1, a_2, a_3, \ldots, a_n\}$ and we are done, $\max(A \triangle (A \oplus 1)) = \max\{0, 1\} = 1 \in A \oplus 1$. In the second case we have $a_2 = 1$ and this implies $A \oplus 1 = \{a_3, a_4, \ldots, a_n\} \oplus \{2\}$.

More generally, suppose k is the smallest number not in A. Then, we have $A = \{0, 1, \ldots, k-1, a_{k+1}, a_{k+2}, \ldots, a_n\}$, where $k < a_{k+1} < a_{k+2} < \ldots < a_n$. Applying $\oplus 1$ yields

$$
A \oplus 1 = \{k, a_{k+1}, a_{k+2}, \ldots, a_n\}.
$$

Then $\max(A \triangle (A \oplus 1)) = k$, which proves $\max(A \triangle (A \oplus 1)) \in A \oplus 1$. If we apply $\oplus 1$ again, we get

$$
A \oplus 2 = \{k, a_{k+1}, a_{k+2}, \ldots, a_n\} \oplus \{0\} = \{0, k, a_{k+1}, a_{k+2}, \ldots, a_n\}.
$$

This means $A \triangle (A \oplus 2) = \{1, 2, \ldots, k\}$ and the maximum of this set is $k \in A \oplus 2$. We can add a unit again, to get $A \oplus 3 = \{1, k, a_{k+1}, a_{k+2}, \ldots, a_n\}$ which gives us the symmetric difference $A \triangle (A \oplus 3) = \{0, 2, 3, \ldots, k\}$ with maximum in $A \oplus 3$. Then we have $A \oplus 4 = \{0, 1, k, a_{k+1}, a_{k+2}, \ldots, a_n\}$ and symmetric difference $A \triangle (A \oplus 4) = \{2, 3, 4, \ldots, k\}$. We continue in this manner, applying $\oplus 1$, until we have applied it $2^k - 1$ times. Thus far, we have proven $\max(A \triangle B) \in B$ if $A < B < A \oplus 2^k$. If we apply $\oplus 1$ once more, we are simply adding the singleton $2^k = \{k\}$, to A. The result is $A \oplus 2^k = \{0, 1, \ldots, k, a_{k+1}, a_{k+2}, \ldots, a_n\}$ because k is the smallest object not in A. This implies $\max(A \triangle (A \oplus 2^k)) = \max\{k\} = k \in A \oplus 2^k$. We conclude $\max(A \triangle B) \in B$ if $A < B \leq A \oplus 2^k$. Now we fall into repetition of what we have done up to this point. When we apply $\oplus 1$ to $A \oplus 2^k$, we are going to substitute all the elements $0, 1, \ldots, k$ with $k \oplus 1$; we are using $2^{k+1} = 1 + (1 + 2 + 4 + 8 + \cdots + 2^k)$. There are two cases; $k \oplus 1 \notin A$ or $k \oplus 1 \in A$. In the first case, $\max(A \triangle (A \oplus 2^k \oplus 1)) = k \oplus 1 \in A \oplus 2^k \oplus 1$ because $A \oplus 2^k \oplus 1 = \{k \oplus 1, a_{k+1}, a_{k+2}, \ldots, a_n\}$. In the second case, $a_{k+1} = k \oplus 1$ so that

$$
A \oplus 2^k \oplus 1 = \{k \oplus 1, a_{k+2}, \ldots, a_n\} \oplus \{k \oplus 1\}.
$$

We proceed as before, finding the second smallest number not in A. Let $p \in A$ the smallest number in $A - \{k\}$. The numbers k, p are the two smallest numbers not in A, so that $A = \{0, 1, \ldots, k-1, k+1, k+2, \ldots, p-1, a_{n-p+1}, a_{n-p+2}, \ldots, a_n\}$. This implies $(A \oplus 2^k) \oplus 1 = \{p, a_{n-p+1}, a_{n-p+2}, \ldots, a_n\}$. The symmetric difference, with A, is $\{0, 1, \ldots, k-1, k+1, k+2, \ldots, p-1, p\}$. The maximum of the symmetric difference is $p \in (A \oplus 2^k) \oplus 1$. This proves $\max(A \triangle B) \in B$ if $A < B \leq (A \oplus 2^k) \oplus 1$. The symmetric difference of $(A \oplus 2^k \oplus 1) \oplus 1 = \{0, p, a_{n-p+1}, a_{n-p+2}, \ldots, a_n\}$ with A, is $\{1, 2, \ldots, k-1, k+1, k+2, \ldots, p-1, p\}$. The maximum of the symmetric difference is $p \in (A \oplus 2^k) \oplus 2$. This proves $\max(A \triangle B) \in B$, if $A < B \leq (A \oplus 2^k) \oplus 2$.

We have $(A \oplus 2^k) \oplus 3 = \{1, p, a_{n-p+1}, a_{n-p+2}, \ldots, a_n\}$, which again gives $p = \max(A \triangle (A \oplus 2^k \oplus 3)) \in A \oplus 2^k \oplus 3$. Continue in this manner. Apply $\oplus 1$ to $A \oplus 2^k$ a total of $2^k - 1$ times before we reach

$$(A \oplus 2^k) \oplus 2^k = \{0, 1, \ldots, k-1, p, a_{n-p+1}, a_{n-p+2}, \ldots, a_n\}.$$

Here, we have symmetric difference $A \triangle ((A \oplus 2^k) \oplus 2^k) = \{k+1, k+2, \ldots, p\}$, and the maximum is $p \in (A \oplus 2^k) \oplus 2^k$. This proves $\max(A \triangle B) \in B$, if $A < B \le A \oplus 2^k \oplus 2^k$. If we add 1 again, we obtain $A \oplus 2^k \oplus 2^k \oplus 1 = \{k, p, a_{n-p+1}, \ldots, a_n\}$. The symmetric difference with A is the set $\{k, p\}$. We have $\max\{k, p\} = p \in A \oplus 2^k \oplus 2^k \oplus 1$. Keep adding 1, until we reach $(A \oplus 2^k) \oplus 2^p = \{0, 1, \ldots, q-1, a_{n-q+1}, a_{n-q+2}, \ldots, a_n\}$ where $A = \{0, 1, \ldots, k-1, k+1, \ldots, p-1, p+1, \ldots, q-1, a_{n-q+2}, a_{n-q+3}, \ldots, a_n\}$ and $q > p$ is the third smallest number not in A. We continue, for all $k, p, q, \ldots, r$ not in A. We reach the largest number $r \notin A$ such that $r < a_n$. This proves $\max(A \triangle B) \in B$ if $A < B < A \oplus 2^k \oplus 2^p \cdots \oplus 2^r$. When we add 1 to $A \oplus 2^k \oplus 2^p \oplus \cdots \oplus 2^r = \{0, 1, \ldots, a_n\}$, the result is the singleton $\{a_n + 1\}$. Now it is trivial that the maximum of the symmetric difference is in $A \oplus 2^k \oplus 2^p \cdots \oplus 2^r \oplus 1$, since $\max(A) < \max(A \oplus 2^k \oplus 2^p \cdots \oplus 2^r \oplus 1)$. Observe that adding 1 to X leaves the maximum of X equal or larger by one, for any set number X. We conclude the result also holds for any $X > A \oplus 2^k \oplus 2^p \cdots \oplus 2^r \oplus 1$ because

$$\max(X) \ge \max(A \oplus 2^k \oplus 2^p \cdots \oplus 2^r \oplus 1) > \max(A)$$

.

Proving the second implication is easy. We use the following observation from the first part of this proof. Given $A = \{a_1, a_2, \ldots, a_n\}$ and any number $x \notin A$, we can find a set number N such that $A \oplus N = \{x, a_i, a_j, \ldots, a_n\}$; of course if $x > A$ we have $A \oplus N = \{x\}$. Let $M = \max(A \triangle B) \in B$, then we add 1 to A, until we obtain the result $A \oplus N = \{M, a_{i_1}, a_{i_2}, \ldots, a_n\}$, where $a_{i_1}, a_{i_2}, \ldots, a_n$ are the elements of A that are greater than M. If $a_n < M$, we simply have $A \oplus N = \{M\}$. Now we need to add P to $A \oplus N$, where $P = \{b_1, b_2, \ldots, b_\alpha\}$ is the set of objects in B that are smaller than M. The result is $B = (A \oplus N) \oplus P = A \oplus (N \oplus P)$ which implies $A < B$. $\qquad\square$

Let us carry out an example of finding which of two different set numbers is largest. Let $A = \{2, 5, 6, 8, 9\}$ and $B = \{0, 1, 7, 8, 9\}$. The largest of the two is the set that contains $\max\{0, 1, 2, 5, 6, 7\} = 7$, so that $A < B$. In the next sections we will have to find the order of set numbers given in a different form. For example, we may write a set number in the form $A = \{\{3, 5\}, \{1, 2\}, \{4, 6\}\} = 2^{2^3 + 2^5} + 2^{2^1 + 2^2} + 2^{2^4 + 2^6}$. Let us compare it with $B = \{\{3, 4\}, \{1, 2\}, \{5, 6\}\} = 2^{2^3 + 2^4} + 2^{2^1 + 2^2} + 2^{2^5 + 2^6}$. Obviously $A < B$ since $\max(A) = \{4, 6\} < \{5, 6\} = \max(B)$.

2.3 Product of Set Numbers

The product is easy to define. We have already defined multiplication by 2. In binary representation, we have $2^n + 2^n = 2^{n+1}$, so here we have a corresponding rule. If a power is repeated we add 1 to that power. Therefore, to multiply by 2 is to apply the function $\odot 2 = s$ that adds 1 to the elements of the argument. Multiplication by 4 is $s \circ s$ which adds 2 to the elements of the argument. In general, multiplication of B by 2^k is equal to $s^k(B)$. If $B = \{b_1, \ldots, b_n\}$ then $2^k \odot B$ is equal to the set $\{b \oplus k\}_{b \in B} = \{b_1 \oplus k, \ldots, b_n \oplus k\}$. The product of a set number B with 2^k, in our graphic representation, consists of displacing the objects of the set, k units up. We say $2^k \odot B$ is the *k-displacement of B*. We define the general product $A \odot B$ in terms of displacements of the *base B*, and the *pivot A*.

$$A \odot B = \bigoplus_{a \in A} \{b \oplus a\}_{b \in B}. \tag{3}$$

This means we add displacements of B, one for each object of the pivot A. If $a \in A$ then the a-displacement of B is one of the displacements in our sum. We notice that multiplication by 0 results in the empty set, $0 \odot X = X \odot 0 = 0$. It is also trivial to find $1 \odot X = X \odot 1 = X$. To show that $2 = \{1\}$ is commutative under multiplication,

$$\begin{aligned}
\{1\} \odot X &= \{x \oplus 1\}_{x \in X} \\
&= \bigcup_{x \in X} \{x \oplus 1\} \\
&= \bigoplus_{x \in X} \{1 \oplus x\} \\
&= X \odot \{1\}.
\end{aligned}$$

This means $2 \odot X = X \odot 2 = X \oplus X$. Before proving general properties, let us calculate $3 \odot 5 = \{0, 1\} \odot \{0, 2\}$ in two different ways to verify these numbers commute. We first make $A = 3$ and $B = 5$ so that we will add two displacements of $B = \{0, 2\}$. The first displacement is $\{0 \oplus 0, 2 \oplus 0\} = \{0, 2\}$, and our second displacement is $\{0 \oplus 1, 2 \oplus 1\} = \{1, 3\}$. We add the two and obtain $\{0, 2\} \oplus \{1, 3\} = \{0, 1, 2, 3\} = 15$. Now we take $A = 5$ and $B = 3$, so that we will add two displacements of $3 = \{0, 1\}$, each corresponding to an element of $5 = \{0, 2\}$. Our displacements of 3 are the 0-displacement, $\{0 \oplus 0, 1 \oplus 0\} = \{0, 1\}$, and the 2-displacement, $\{0 \oplus 2, 1 \oplus 2\} = \{2, 3\}$. Adding these two displacements results in $\{0, 2\} \oplus \{1, 3\} = \{0, 1, 2, 3\} = 15$. Let us give an example in terms of powers of 2, to illustrate this procedure. To find the product $(2^0 + 2^1)(2^0 + 2^2)$ we distribute $2^0(2^0 + 2^2) + 2^1(2^0 + 2^2)$. Then, we have $(2^{0+0} + 2^{2+0}) + (2^{0+1} + 2^{2+1}) = (2^0 + 2^2) + (2^1 + 2^3)$.
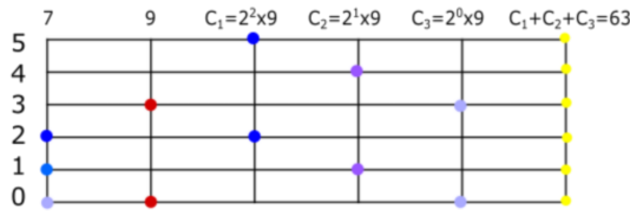
Fig. 2 We find the product $7 \odot 9$. The first and second columns are the pivot and base, respectively. The next three columns correspond to the displacements of our base. The last column is the sum of the displacements. The result is equal to $63 = \{0, 1, 2, 3, 4, 5\}$.

In Figure 2 we have the visual representation of $7 \odot 9$. To formalize this, we first verify $\odot 2$ is a morphism for addition of set numbers, $s(A \oplus B) = s(A) \oplus s(B)$. We know $X \oplus X = s(X)$, so that $s(A \oplus B) = (A \oplus B) \oplus (A \oplus B) = (A \oplus A) \oplus (B \oplus B) = s(A) \oplus s(B)$. Of course this implies

$$s^k(A \oplus B) = s^k(A) \oplus s^k(B), \tag{4}$$

for every $k \in \mathbb{N}$. To prove the distributive property use (4) and the commutative and associative properties of addition of sets.

$$
\begin{aligned}
A \odot (B \oplus C) &= \bigoplus_{a \in A} \{x \oplus a\}_{x \in B \oplus C} \\
&= \bigoplus_{a \in A} s^a(B \oplus C) \\
&= \bigoplus_{a \in A} (s^a(B) \oplus s^a(C)) \\
&= \bigoplus_{a \in A} s^a(B) \oplus \bigoplus_{a \in A} s^a(C) \\
&= (A \odot B) \oplus (A \odot C)
\end{aligned}
$$

Now we prove multiplication is commutative. Let $a \in A$ fixed, then the set $\{b \oplus a\}_{b \in B} = \{b_1 \oplus a, b_2 \oplus a, \ldots, b_n \oplus a\}$ can be expressed as a sum of disjoint singletons, $\bigoplus_{b \in B} \{b \oplus a\}$

$$
\begin{aligned}
A \odot B &= \bigoplus_{a \in A} \{b \oplus a\}_{b \in B} \\
&= \bigoplus_{a \in A} \bigoplus_{b \in B} \{b \oplus a\} \\
&= \bigoplus_{b \in B} \bigoplus_{a \in A} \{a \oplus b\} \\
&= \bigoplus_{b \in B} \{a \oplus b\}_{a \in A} \\
&= B \odot A.
\end{aligned}
$$

We have proven the distributive and commutative properties, so that we have also proven

$$(A \oplus B) \odot C = (A \odot C) \oplus (B \odot C). \tag{5}$$

Now, we wish to prove that multiplication is associative. We need the following proposition.

Proposition 5 *The operation function $\odot N$ acts on sets by $\odot N(X) = \oplus X^N(0)$.*

Proof This is proven by mathematical induction. We know it is true for 1, since $1 \odot X = X$. Suppose it is true for N, then using the distributive property of (5)

$$
\begin{aligned}
\odot (N \oplus 1)(X) &= \odot N(X) \oplus \odot 1(X) \\
&= \oplus X^N(0) \oplus X \\
&= \oplus X(\oplus X^N(0)) \\
&= \oplus X^{N+1}(0).
\end{aligned}
$$

$\square$

Now we can prove the associative property holds for the product of set numbers. Because of Proposition 3, it is sufficient to verify the operation functions of $\odot$ commute. We will use the notation $\bigoplus_{i=1}^{N} X$ to represent the number $\oplus X^N(0)$. This way, the expression $\bigoplus_{j=1}^{A}\left(\bigoplus_{i=1}^{B} X\right)$ means we add X a number of B times to obtain the number $B \odot X$, and then we add $B \odot X$ a total of A times to obtain $A \odot (B \odot X)$. We are really adding X a total number of $A \odot B = B \odot A$ times. It is as if we have a rectangular matrix of size $A \times B$ and every entry is equal to X, then we add all the entries. Considering the matrix of size $B \times A$ and proceeding is equivalent to rearranging the order of the sum. To prove associativity of product we apply Proposition 5 twice, then we use commutativity and associativity of addition to find the third equality. Then we apply Proposition 5 again.

$$(\odot A \circ \odot B)(X) = \odot A\left(\bigoplus_{i=1}^{B} X\right)$$
$$= \bigoplus_{j=1}^{A}\left(\bigoplus_{i=1}^{B} X\right)$$
$$= \bigoplus_{i=1}^{B}\left(\bigoplus_{j=1}^{A} X\right)$$
$$= \odot B\left(\bigoplus_{i=1}^{A} X\right)$$
$$= (\odot B \circ \odot A)(X)$$

To prove the properties of multiplication, we have expressed them in terms of addition, where we have proven the commutative, associative and distributive properties. In [Ramirez(2019)], there is a description of subtraction, division and powers of set numbers.

2.4 Integers

We do not require the structure of integers, to construct the structure of real numbers. However, we provide a construction of $\mathbb{Z}$ because it introduces methods and concepts of previous and later sections. We use operation functions and their inverse functions to describe integers. A positive integer $\mathbf{n} \in \mathbb{Z}$ is an operation function $\oplus n$, while its negative integer $\mathbf{-n} \in \mathbb{Z}$ is the inverse function $(\oplus n)^{-1}$. We notice one important fact. Negative integers can easily be distinguished from positive integers. A negative integer is a function of the form $\mathbf{-n} : \{n, n \oplus 1, n \oplus 2, \ldots\} \to \mathbb{N}$, while a positive integer is a function of the form $\mathbf{n} : \mathbb{N} \to \{n, n \oplus 1, n \oplus 2, \ldots\}$. This will have to be considered when defining addition of integers; it does not represent any difficulty but we must be careful. The integer $\mathbf{0}$ is the identity function of $\mathbb{N}$. We represent the set of negative integers with the symbol $-\mathbb{N}$. We say $X \subset \mathbb{Z}$ is a *non negative subset of* $\mathbb{Z}$ if $-\mathbb{N} \cap X = \emptyset$, and the like.

The sum of integers is defined in the obvious way, using composition. Let $\mathbf{m} = \oplus m$ and $\mathbf{n} = \oplus n$ positive integers. The composition of these is a positive integer. We define the addition of two positive integers, $\mathbf{m+n} = \oplus m \circ \oplus n$. The sum, $\mathbf{-m-n}$, of negative integers $\mathbf{-m} = (\oplus m)^{-1}$ and $\mathbf{-n} = (\oplus n)^{-1}$, is defined as the composition $(\oplus m)^{-1} \circ (\oplus n)^{-1} = (\oplus n \circ \oplus m)^{-1}$. We have $\oplus n \circ \oplus m = \oplus m \circ \oplus n$, so that $\mathbf{-m-n}$ is equal to the negative integer $(\oplus m \circ \oplus n)^{-1} = \mathbf{-(m+n)}$. The sum of one negative integer $\mathbf{-m}$ and one positive integer $\mathbf{n}$ is defined as follows. We can have two cases. If the corresponding natural numbers satisfy $m < n$, we know there is a natural number x such that $n = m + x$. We define $\mathbf{-m+n} = \mathbf{x}$, where $\mathbf{x} = \oplus x : \mathbb{N} \to \{n - m, n - m + 1, n - m + 2, \ldots\}$. In the contrary case that the natural numbers satisfy $n < m$, we have $m = n + x$ for some natural number x. We define addition of these integers by $\mathbf{-m+n} = \mathbf{-x}$, where $\mathbf{-x} = (\oplus x)^{-1} : \{m - n, m - n + 1, m - n + 2, \ldots\} \to \mathbb{N}$. The order relation between m, n determines if $\mathbf{-m+n}$ is a positive integer or a negative integer. In both cases, we have $\mathbf{-m+n} = (\oplus m)^{-1} \circ \oplus n$. But, what happens if we try to define $\mathbf{n-m}$? Consider the composition $\oplus n \circ (\oplus m)^{-1}$. In both cases, $m < n$ or $n < m$, the composition is $\oplus n \circ (\oplus m)^{-1} : \{m, m+1, \ldots\} \to \{n, n+1, \ldots\}$. Although $\oplus n \circ (\oplus m)^{-1}$ is a well defined composition, it is not an integer. The functions $\oplus n \circ (\oplus m)^{-1}$ and $(\oplus m)^{-1} \circ \oplus n$ are not the same function. However, in the intersection of the domains, these compositions are equal functions. Thus, we are justified in defining the sum of integers as commutative, $\mathbf{n-m} = \mathbf{-m+n}$. To prove addition of integers is associative, let $\mathbf{x}, \mathbf{y}, \mathbf{z}$ integers. We have to consider two cases; y is positive or negative. Suppose first, y is positive. Then we have $\mathbf{x+y} = \oplus x \circ \oplus y$. Consider two sub cases. If z is positive, the associative property holds for $\mathbf{(x+y)+z} = \mathbf{x+(y+z)}$ because the associative property holds for composition of functions. Suppose z is negative. Then $\mathbf{(x+y)+z} = \mathbf{z+(x+y)} = \mathbf{z+(y+x)} = \mathbf{(z+y)+x} = \mathbf{x+(z+y)} = \mathbf{x+(y+z)}$. Go back to our assumption of y. Now, suppose y is negative and x is positive. We have $\mathbf{(x+y)+z} = \mathbf{(y+x)+z} = \mathbf{(y+x)+z} = \mathbf{y+(x+z)} = \mathbf{y+(z+x)} = \mathbf{(y+z)+x} = \mathbf{x+(y+z)}$. If $\mathbf{x}$ and $\mathbf{y}$ are negative, then $\mathbf{x+y} = \oplus x \circ \oplus y$. This implies $\mathbf{(x+y)+z} = (\oplus x \circ \oplus y) \circ \oplus z = \oplus x \circ (\oplus y \circ \oplus z) = \mathbf{x+(y+z)}$. This proves addition of integers is associative. The addition of integers $\mathbf{5-3}$ is equal to the function $\oplus 2$, while the result of $\mathbf{3-5}$ is $(\oplus 2)^{-1}$.

Ordering integers is natural, in this context. Two integers $\mathbf{x}, \mathbf{y}$ satisfy the inequality $\mathbf{x} < \mathbf{y}$ if and only if $\mathbf{x}(n) < \mathbf{y}(n)$, for any $n \in \mathbb{N}$. For example, $\mathbf{-5} < \mathbf{2}$ because $\mathbf{-5}(5) = 0 < 7 = \mathbf{2}(5)$. Of course, the order is well defined so that there is no natural number n such that $\mathbf{2}(n) < \mathbf{-5}(n)$. Let us prove $\mathbf{-6} < \mathbf{-3}$. We need a set number that is in the domain of $\mathbf{-3}$ and $\mathbf{-6}$, say 6. Then, $\mathbf{-6}(6) = 0 < 3 = \mathbf{-3}(6)$.

3 Finite Functions and Permutations

In this section we will build the set of finite functions on $\mathbb{N}$, and provide an injective function from this set, into the set of natural numbers. The important quality of this representation is that functions are equivalent if and only if they are represented by the same number. We find a way to assign natural numbers to abstract functions as well. There will be a distinct difference when we are working with an abstract function or a concrete function. When working with abstract functions, two functions are defined to have the same *structure* if they are assigned the same natural number. Concrete functions, on the other hand, can have the same structure but different numeric representation. For example, consider the functions f, g defined by

$$
\begin{array}{ll}
f(a) = b & g(a) = a \\
f(b) = a & g(b) = c \\
f(c) = c & g(c) = b
\end{array}
$$

These two abstract functions have the same structure, and have the same numeric representation; they will be considered to be the same function. However, if the objects are not abstract, $a, b, c \in \mathbb{N}$, then f, g are concrete functions and they will be represented by distinct numbers. In our example, let $a = 3$, $b = 5$ and $c = 0$. The functions f, g defined by $f(3) = 5$, $f(5) = 3$, $f(0) = 0$, and $g(3) = 3$, $g(5) = 0$, $g(0) = 5$ are different and they will be represented by different numbers.

In this section we order the set of finite functions of natural numbers. Then we give an equivalence definition for abstract finite functions, which simultaneously orders these equivalence classes. In the process we are able to provide a canonical order for the elements of a given abstract finite function, and we can say which objects of the function can be considered to be equivalent. In our example, the objects a, b, are equivalent in the function f, while c is not equivalent to another object. The objects b, c are equivalent in the function g, and a is not equivalent to another object.

3.1 Ordered Pairs

If we wish to represent finite functions as natural numbers, we will first find a way of representing ordered pairs as natural numbers. An ordered pair of natural numbers should be an object (m, n) from which you can determine two natural numbers in a predetermined order. This means that we do not want (m, n) and (n, m) to be the same object. The first ordered pair, (m, n), means we have two natural numbers. First m, then n. The second ordered pair (n, m) means we have first n, then m. A set of two natural numbers $\{X, Y\}$ is not an ordered pair because we it simply tells us we have two objects, without a pre determined order; we simply have objects X, Y and they are not ordered.

To solve this, we give a method of coding an ordered pair of natural numbers using odd/even numbers to represent the first/second component respectively. Given any set number X, we can associate to it the odd number $s(X) \oplus 1$, and the even number $s(X \oplus 1)$. For example, 0 is associated to the odd number $s(0) \oplus 1 = 1$ and the even number $s(0 \oplus 1) = 2$. The number 1 is associated the odd number $s\{0\}1 = \{1\} \oplus 1 = 2 \oplus 1 = 3$ and the even number $s(1 \oplus 1) = s(2) = 4$. In general, the number k is associated to the $k + 1$-st odd and even numbers $2k + 1$ and $2(k + 1)$, as shown in the table 1.

Table 1 Every natural number can be uniquely represented as an odd and even number.

X	Odd	Even
0	1	2
1	3	4
2	5	6
3	7	8
4	9	10
5	11	12
⋮	⋮	⋮

An odd number is a set number A with $0 \in A$. To transform a set number X to its odd representation, displace the objects of X one unit up, to get $s(X)$. Then add the object 0 to the set $s(X)$, to obtain $s(X) \oplus 1 = s(X) \cup \{0\}$. When we apply $\oplus 1$ to $s(X)$, we simply add the object 0 to the set $s(X)$ because $0 \notin s(X)$. The set number $5 = \{0, 2\}$ is sent to the odd number $s(5) \oplus 1 = \{0 \oplus 1, 2 \oplus 1\} \oplus 1 = \{1, 3\} \oplus \{0\} = \{0, 1, 3\}$. Take another example, the set number $13 = \{0, 2, 3\}$ is sent to the odd representation $s(13) \oplus 1 = \{0 \oplus 1, 2 \oplus 1, 3 \oplus 1\} \oplus \{0\} = \{1, 3, 4\} \oplus \{0\} = \{1, 3, 4\}$. Given an odd number A, we can easily see what set number it represents. To find the set number X such that $A = s(X) \oplus 1$, take away the object 0, from A, and displace the rest of the objects one unit down. Doing this to the odd number $\{0, 1, 3, 4\}$, of our last example, we get $13 = \{1 - 1, 3 - 1, 4 - 1\} = \{0, 2, 3\}$. An even number is a set number B such that $0 \notin B$. The set number X is represented by the even number $s(X \oplus 1)$. For example, the set number $7 = \{0, 1, 2\}$ is assigned the even number $16 = s(\{0, 1, 2\} \oplus 1) = s(\{0, 1, 2\} \oplus \{0\}) = s\{3\} = \{3 \oplus 1\} = \{4\}$. If B is an even number, we can find the set number X it is representing. Displace the objects of B one unit down. This means B is representing the predecessor of $X \oplus 1$. For example, the number $10 = \{1, 3\}$ is the even representation of $4 = 5 - 1$ because $\{1 - 1, 3 - 1\} = \{0, 2\} = 5$. We can go back an forth between a set number X and its odd/even representation.

The ordered pair (m,n) is a set number of one odd and one even number, $\{2m+1, 2(n+1)\}$. This allows us to differentiate the two components. We will use the convention that the odd number is the first component of the ordered pair, while the even number is used for the second component of the ordered pair. If $P = \{A, B\}$ is an ordered pair, we use the convention that the *first component* is given by the odd number, A, and the *second component* is given by the even number, B. If $P = \{2k+1, B\}$ then it represents an ordered pair with k in the first component, $P = (k,n)$. We use even numbers to represent the second component. If $P = \{A, 2(k+1)\}$ then it represents an ordered pair with k in the second component, $P = (m,k)$. An ordered pair (m,n), of natural numbers m,n, is defined as the set number $2^{2m+1} + 2^{2(n+1)} = \{2m+1, 2(n+1)\}$, where $m,n \in \mathbb{N}$. The set number representing $(0,0)$ is $\{1,2\} = 2^{2(0)+1} + 2^{2(0+1)} = 6$. For another example, the ordered pair $(4,5)$ is represented by the natural number $2^{2(4)+1} + 2^{2(5+1)} = 2^9 + 2^{12}$. In summary, $P = \{A, B\} \in \mathbb{N}$, with $0 \in A$ and $0 \notin B$, represents the ordered pair (m,n), where $m,n \in \mathbb{N}$ are the unique natural numbers that satisfy $s(m) \oplus 1 = A$ and $s(n \oplus 1) = B$. We find $m = \frac{A-1}{2}$ and $n = \frac{B}{2} - 1$, where $\frac{X}{2} = s^{-1}(X)$. The function s^{-1} sends the elements of X to their predecessor, $s^{-1}(X) = \{x-1\}_{x \in X}$. There exists a numeric table describing this rule, in general.

Definition 6 *We define a family of sets,*

$$(0,) = \{6, 18, 66, 258, 1026, \ldots, 2 + 2^{2(n+1)}, \ldots\}$$
$$(1,) = \{12, 24, 72, 264, 1032, \ldots, 8 + 2^{2(n+1)}, \ldots\}$$
$$(2,) = \{36, 48, 96, 288, 1056, \ldots, 32 + 2^{2(n+1)}, \ldots\}$$
$$\vdots \quad \vdots$$
$$(m,) = \{2^{2m+1} + 4, 2^{2m+1} + 16, \ldots, 2^{2m+1} + 2^{2(n+1)}, \ldots\}. \tag{6}$$

Any element $x \in \bigcup_i (i,)$, in the above family of sets, is an ordered pair. The ordered pair (m,n) is the $n+1$-st element of the set $(m,)$. A finite relation is a finite subset $R \subset \bigcup_i (i,)$; elements of R are called components.

There are a few important remarks to be made. Every ordered pair of natural numbers is identified with a unique natural number. Two ordered pairs are the same if and only they are represented by the same set number. And, every natural number representing an ordered pair is a multiple of 6 (the converse is obviously not true). We have an easy way of knowing what number represents (m,n). An ordered pair $(0,n)$ is any element of the set $(0,)$. The ordered pair $(0,0)$ is represented by $6 = 2^{2(0)+1} + 2^{2(0+1)}$, and $(0,1)$ is $18 = 2^{2(0)+1} + 2^{2(1+1)}$. The third number of the set $(0,)$ represents the ordered pair $(0,2)$, etc. An element of $(1,)$ is an ordered pair of the form $(1,n)$. The ordered pair $(1,0)$ is represented by $12 = 2^{2(1)+1} + 2^{2(0+1)}$, the first object of $(1,)$. The ordered pair $(1,1)$ is $24 = 2^{2(1)+1} + 2^{2(1+1)}$, the second object of $(1,)$. The third object of $(1,)$ represents the ordered pair $(1,2)$, etc. Now, we are able to make an important jump. This is the second part of our definition, *relation*. A finite collection of ordered pairs is a natural number,

$$\{\{A_1, B_1\}, \ldots, \{A_n, B_n\}\} = 2^{2^{A_1} + 2^{B_1}} + \cdots + 2^{2^{A_n} + 2^{B_n}} \tag{7}$$

where A_i are odd and the B_i are even. Under this definition, a set of ordered pairs is a relation, as is usual. We are able to store the information of a finite relation in a single natural number, and the structure is again obtainable from that number. The relation $\{(0,0), (0,1), (0,2), (2,1)\}$ is represented by the natural number $2^{2^{2(0)+1} + 2^{2(0+1)}} + 2^{2^{2(0)+1} + 2^{2(1+1)}} + 2^{2^{2(0)+1} + 2^{2(2+1)}} + 2^{2^{2(2)+1} + 2^{2(1+1)}}$. Two finite relations are the same if and only if they are represented by the same natural number. For another example, take the relation $\{(2,1), (2,2), (4,2), (4,4)\}$ given by the natural number $2^{2^{2(2)+1} + 2^{2(1+1)}} + 2^{2^{2(2)+1} + 2^{2(2+1)}} + 2^{2^{2(4)+1} + 2^{2(2+1)}} + 2^{2^{2(4)+1} + 2^{2(4+1)}}$. Now we are able to describe finite functions as natural numbers.

3.2 Concrete Functions

In this section we use the definition of finite relation to represent a finite function of natural numbers. Going back to our definition of relation, we additionally require that no odd number is repeated. A finite function is represented by a set number of the form (7), where all the A_i are distinct.

Definition 7 *A function $f : A \to B$ is a natural number $f = \{\{A_1, B_1\}, \{A_2, B_2\}, \ldots, \{A_n, B_n\}\} = 2^{2^{A_1} + 2^{B_1}} + 2^{2^{A_2} + 2^{B_2}} + \cdots + 2^{2^{A_n} + 2^{B_n}}$, where all the A_i are distinct odd numbers and B_i are even numbers. A function is called bijective if, additionally, all the B_i are distinct. Every element of f is an arrow component. The function f maps $m \mapsto n$ if and only if $2^{2m+1} + 2^{2(n+1)} \in f$.*

A permutation $\{0,1,2,\ldots,n\} \to \{0,1,2,\ldots,n\}$ is particularly easy to identify. It is a set of $n+1$ ordered pairs, in which every element of $\{1,2,3,4,\ldots,2n, 2n+1, 2(n+1)\}$ appears in exactly one ordered pair. Examples of permutations are

$$\{\{1,2\}, \{3,4\}\} = 2^{2^1 + 2^2} + 2^{2^3 + 2^4}$$
$$\{\{1,3\}, \{2,4\}\} = 2^{2^1 + 2^3} + 2^{2^2 + 2^4}$$
$$\{\{1,2\}, \{3,4\}, \{5,6\}, \{7,8\}\} = 2^{2^1 + 2^2} + 2^{2^3 + 2^4} + 2^{2^5 + 2^6} + 2^{2^7 + 2^8}$$
$$\{\{1,6\}, \{3,8\}, \{5,2\}, \{7,4\}\} = 2^{2^1 + 2^6} + 2^{2^3 + 2^8} + 2^{2^5 + 2^2} + 2^{2^7 + 2^4}$$
$$\{\{1,4\}, \{3,10\}, \{5,6\}, \{7,8\}, \{9,2\}\} = 2^{2^1 + 2^4} + 2^{2^3 + 2^{10}} + 2^{2^5 + 2^6} + 2^{2^7 + 2^8} + 2^{2^9 + 2^2}$$
$$\{\{1,6\}, \{3,8\}, \{5,2\}, \{7,10\}, \{9,4\}\} = 2^{2^1 + 2^6} + 2^{2^3 + 2^8} + 2^{2^5 + 2^2} + 2^{2^7 + 2^{10}} + 2^{2^9 + 2^4}$$

The first permutation is the identity permutation $(0)(1)$. The second set number is representing the one-cycle permutation $(0,1)$. The third and fourth numbers represent $(1)(2)(3)(4)$ and $(0,2)(1,3)$, respectively. The fifth and sixth permutations are $(0,1,4,)(2)(3)$, and $(0,2)(1,3,4)$. We provide a linear order to the set of finite functions, and in particular permutations.

This order is well behaved in several ways. If $f : \{0,1,2,\ldots,m\} \to \{0,1,2,\ldots,m\}$, and $g : \{0,1,2,\ldots,n\} \to \{0,1,2,\ldots,n\}$ are permutations and $m < n$, then the representation of f is smaller than the representation of g. For now, we conclude this section with the following remark. This representation is not very good if we want a representation that measures how much movement a permutation causes. This manner of assigning natural numbers to functions makes a distinction between functions with the same structure. For example, the functions f, g defined by $f(0) = 0$ and $g(1) = 1$ have the same structure but are assigned different numbers. In the following section we address this issue. We assign a natural number to any abstract finite function, in such a way that two functions are represented by the same number if and only if they have the same structure (this will be our definition of equivalent structure between two functions). This gives us a *modulo-structure* representation of concrete functions. We *forget* the numerical values of the objects of the concrete function, turning it into an abstract function. Then we find the number representation of that abstract function.

3.3 Abstract Functions

Consider the permutations $(1,2)(3,4)$ and $(1,3)(2,4)$. These will be represented by the numbers $2^{2^3+2^6} + 2^{2^5+2^4} + 2^{2^7+2^{10}} + 2^{2^9+2^8}$ and $2^{2^3+2^8} + 2^{2^7+2^4} + 2^{2^5+2^{10}} + 2^{2^9+2^6}$, respectively. These numbers are different. We would like to make a good definition, modulo the structure, so that the two functions above are assigned the same natural number. It would be advantageous to number finite functions in such a manner that functions with the same structure will be represented by the same natural number. Let $f : A \to B$ a concrete function, where $A, B \in \mathbb{N}$. Our first step is to forget the numeric value assigned to the elements of the components. This means that the sets A, B are no longer thought of as set numbers. We will think of the elements of A and B as abstract objects with a function defined on them. We need to know how many distinct elements are in $A \cup B$. For example, the function f defined by

$$f(2) = 2$$
$$f(5) = 6$$
$$f(6) = 5$$
$$f(8) = 6$$
$$f(10) = 15$$

depends on the distinct objects $2, 5, 6, 8, 10, 15$ and it will be considered an abstract function f^* defined by

$$f^*(a) = a$$
$$f^*(b) = c$$
$$f^*(c) = b \tag{8}$$
$$f^*(d) = c$$
$$f^*(p) = q$$

Now, we must find a way of assigning a natural number N_{f^*} to the abstract function f^*, in a sufficiently reasonable manner. To do this, we must go back to the realm of numeric values. Let us take a fixed bijection $\eta : \{a,b,c,d,p,q\} \to \{0,1,2,3,4,5\}$, and call it a *naming function of f^**. Using the procedure of the last section, we have a representation $N_{f^*}(\eta) \in \mathbb{N}$ that depends on the naming function η and the abstract function f^*. Now consider the set of all representations $\{N_f(\eta)\}_\eta$; let η variable over all possible naming functions. In our example we have 6! possibilities.

To find the modulo-structure representation of a concrete function f, we first find the abstract function f^* corresponding to f, then we proceeded to find all the possible naming functions of f^*. There is a total of $\#(A \cup B)!$ naming functions. Each naming function η provides a representation $N_{f^*}(\eta)$, so that we have a set of representations $\{N_{f^*}(\eta)\}_\eta$.

Definition 8 *Let f be a concrete function and f^* its corresponding abstract function. Their exists at least one naming, ρ, such that $N_{f^*}(\rho)$ is equal to the maximum element of the set $\{N_{f^*}(\eta)\}_\eta$. This maximum is the modulo-structure representation of f, and we use the symbol $N_{f^*} = N_{f^*}(\rho)$.*

Let f^* and g^* abstract functions such that $N_{f^*}(\eta) = N_{g^*}(\mu)$, for some naming functions η of f^* and μ of g^*. Then $f^* = g^*$ and we say η, μ are *equivalent naming functions for f^**. The sets of representations for f^*, g^* are disjoint if f^*, g^* are different functions; $f^* \neq g^*$ implies $\{N_{f^*}(\eta)\}_\eta \cap \{N_{g^*}(\mu)\}_\mu = \emptyset$. This is a good representation of abstract functions as natural numbers, because $\{N_{f^*}(\eta)\}_\eta$ is a natural number and two functions are assigned different numbers if and only if they have different structure. Therefore, we have a linear order for finite functions. The representation of a function is a large natural number because $\#\{N_{f^*}(\eta)\}_\eta = (\#(Dom(f^*) \cup Im(f^*)))!$. If f^* is a permutation of k objects, the representation of f^* is a natural number that is the sum of $k!$ distinct powers of 2. The representation of a permutation of 10 objects would be a natural number somewhere close to $10^{10^{230}}$. We can make this representation smaller, and the order of the functions will be invariant. In Definition 8,

we use the fact that sets of representations are disjoint for different functions, to our advantage. We choose to represent the function f with the maximum of the set of representations, for the following reason. Let $A \cap B = \emptyset$, then the order relation of the maximum elements, $\max(A) < \max(B)$, determines the order relation $A < B$. We conclude that representing f with the set of representations, $\{N_{f^*}(\eta)\}_\eta$, or with the maximum element, $N_{f^*} = \max\{N_{f^*}(\eta)\}_\eta$, gives us the same order.

Now we define equivalent objects of a finite function $f : A \to B$ of n objects; $n = \#(A \cup B)$. Suppose we have two canonical naming functions $\rho_1, \rho_2 : (A \cup B) \to \{0, 1, 2, \ldots, n-1\}$ so that $N_{f^*} = N_{f^*}(\rho_1) = N_{f^*}(\rho_2)$. We are supposing the naming functions are not equal, so that we have $\rho_1(x) \neq \rho_2(x)$, for some $x \in A \cup B$. Also, naming functions are bijections, so we know there exists $y \neq x$ such that $\rho_1(y) = \rho_2(x)$. We will say x, y are equivalent objects because there are two distinct canonical naming functions ρ_1, ρ_2 that assign the same numerical value to x, y.

Definition 9 *Let $f : A \to B$ a finite function. Two objects $x, y \in A \cup B$ are equivalent if there exist canonical naming functions ρ_1, ρ_2 such that $\rho_1(x) = \rho_2(y)$. This is an equivalence relation on the set of objects $A \cup B$.*

This method has given us two things. We are able to number the set of all finite functions (modulo structure), and we are also provided with a canonical naming function on the objects $Dom(f) \cup Im(f)$. We can order the set of abstract finite permutations. We can also order the elements of any abstract finite permutation, and we know which objects of f are equivalent. Most importantly these orders are well behaved in several ways. In this work, we focus on the ordering of finite permutations, and a general exposition of finite functions is left for future work. Nonetheless, we do some examples of general functions. Let us find the representation of the first finite functions, to get an intuitive grasp of how functions are ordered.

Our first example is of course the trivial function f_0 that sends $a \to a$. This function depends of a single object so we use the set $\{0\}$ to name the set of objects $\{a\}$. We have to recall the definition of ordered pair, and specifically we said the ordered pair $0 \to 0$ is represented by the number $6 = 2^1 + 2^2$. We use the odd number to represent the preimage and the even number to represent the image; a 0 in the preimage means 1 is an element of the ordered pair and a 0 in the image means 2 is an element of the ordered pair. Our function consists of one component. Its only element is 6, so $N_{f_0} = 2^{2^1 + 2^2}$. Let us continue to represent functions. We will try to construct all finite functions in order of their representation, so the next logical choice is the function f_1 defined by one component, $f_1(a) = b$. In this case we have two objects so a naming of this function is a bijection $\{a, b\} \to \{0, 1\}$. If we choose the naming $a = 0$ and $b = 1$ we get the representation $2^{2^1 + 2^4}$. If we give instead the naming $a = 1$ and $b = 0$ then the representation is $2^{2^3 + 2^2}$. We conclude that the canonical representation of f_1 is the number $N_{f_1} = 2^{2^1 + 2^4}$ corresponding to the first naming function $a = 0$ and $b = 1$. These are the only two possible abstract functions of one component; namely $f_0(0) = 0$ (trivial function) and $f_1(0) = 1$ (one object sent to a different object).

Now let us consider functions of two components. Bur first let us recall what it is we are trying to do. We know finite functions are ordered isomorphic to $\mathbb{N}$; every finite function is assigned a unique natural number. We can state this in the following simple manner. There is a set of natural numbers $\{N_f\}_{f:\text{finite function}} = \{N_0, N_1, N_2, \ldots\}$ and we say an element of this set is a finite function. Let us find the first few functions $f_0, f_1, \ldots$ represented by the first numbers $N_0, N_1, \ldots$. So far we know the first two functions are the one component functions $N_0 = 2^{2^1 + 2^2}$ and $N_1 = 2^{2^1 + 2^4}$ from above. If we want to find the next function, $f_2 = N_2$, we will have to add a component but we do not want to use more than two objects because that would give us a function represented by a larger number. Consider finite functions of two components, and two objects. There is a total of 3 functions that satisfy this conditions and they are the functions N_2, N_3, N_4. The function N_2 is given by two components that switch the objects in the domain, $f_2(a) = b$ and $f_2(b) = a$. This is the first time we encounter two equivalent objects for a function. If we give the naming $a = 0, b = 1$ or the naming $a = 1, b = 0$ we get the same representation $N_2 = 2^{2^1 + 2^4} + 2^{2^2 + 2^3}$. The next function in order is the identity function on two objects, $f_3(a) = a$ and $f_3(b) = b$. Again, both objects are equivalent and they give the representation $N_3 = 2^{2^1 + 2^2} + 2^{2^3 + 2^4}$. The function N_4 is the *trivial function* that sends two objects to one of the two; the components are $f_4(a) = a$ and $f_4(b) = a$. The canonical representation $N_4 = 2^{2^1 + 2^4} + 2^{2^3 + 2^4}$ is given by the naming $a = 1$ and $b = 0$. The first summand represents $f_4(0) = 1$ and the second summand represents $f_4(1) = 1$. We can easily verify the alternative naming function would give us a smaller representation. If we give the naming $a = 0$ and $b = 1$, the corresponding representation of f_4 is $2^{2^1 + 2^2} + 2^{2^3 + 2^2}$. Notice that the function that seems to cause more movement, f_2, is represented by the smallest number of the three. The function that sends everything to a is the largest of the three, and the identity is the middle number. This observation will be important in the special case of ordering permutations.

Now we can consider functions of two components and three objects, the next functions in our order N_5, N_6, N_7. We give each function with its canonical naming, and then some of the other non canonical representations.

$f_5(a) = b$, $f_5(b) = c$ has canonical naming $a = 1$, $b = 2$, $c = 0$ giving ordered pairs $(1, 2), (2, 0)$ with representation

$$N_5 = 2^{2^3 + 2^6} + 2^{2^5 + 2^2}.$$

Other, non canonical, representations are $a = 0$, $b = 1$, $c = 2$ with representation $2^{2^1 + 2^4} + 2^{2^3 + 2^6}$; $a = 0$, $b = 2$, $c = 1$ with representation $2^{2^1 + 2^6} + 2^{2^5 + 2^4}$; $a = 1$, $b = 0$, $c = 2$ with representation $2^{2^3 + 2^2} + 2^{2^1 + 2^6}$; $a = 2$, $b = 1$, $c = 0$ with representation $2^{2^5 + 2^4} + 2^{2^3 + 2^2}$; $a = 2$, $b = 0$, $c = 1$ with representation $2^{2^5 + 2^2} + 2^{2^1 + 2^4}$, etc.

$f_6(a) = c$, $f_6(b) = c$ has canonical naming $a = 0$, $b = 1$, $c = 2$ giving the ordered pairs $(0, 2), (1, 2)$ with representation

$$N_6 = 2^{2^1 + 2^6} + 2^{2^3 + 2^6}.$$

The naming $a = 1$, $b = 0$, $c = 2$ is also canonical; a, b are equivalent objects of f. Other, non canonical, representations are $a = 2$, $b = 1$, $c = 0$ with representation $2^{2^5 + 2^2} + 2^{2^3 + 2^2}$; $a = 2$, $b = 0$, $c = 1$ with representation $2^{2^5 + 2^4} + 2^{2^1 + 2^4}$. etc.

$f_7(a) = a$, $f_7(b) = c$ has canonical naming $a = 2$, $b = 0$, $c = 1$ giving the ordered pairs $(2, 2), (0, 1)$ with representation

$$N_7 = 2^{2^1+2^4} + 2^{2^5+2^6}.$$

Other, non canonical, naming functions are $a = 2$, $b = 1$, $c = 0$ with representation $2^{2^3+2^2} + 2^{2^5+2^6}$; $a = 0$, $b = 1$, $c = 2$ with representation $2^{2^1+2^2} + 2^{2^3+2^6}$; $a = 0$, $b = 2$, $c = 1$ with representation $2^{2^1+2^2} + 2^{2^5+2^4}$; etc.

So far, we have found the first eight numbers $N_0, N_1, \ldots, N_7$. We wish to find the next numbers representing functions. Here, we have to be careful. There is one function of two components and four objects. However, it is not next in order, because the functions of three components and three objects have smaller representation. We see that the order of functions is determined first in terms of objects. Let $f : A \to B$ and $g : C \to D$ finite functions and suppose $\#(A \cup B) < \#(C \cup D)$, then $f < g$. If $\#(A \cup B) = \#(C \cup D)$, we check the number of components. The function with more components has larger representation; $\#(f) < \#(g)$ implies $f < g$. Let A_n^m a finite function of n objects and m components. The following inequalities hold.

$$A_1^1 < A_2^1 < A_2^2 < A_3^2 < A_3^3 < A_4^2 < A_4^3 < A_4^4 < A_5^3 < A_5^4 < A_5^5 < A_6^3 < A_6^4 < A_6^5 < A_6^6 < \cdots$$

The table below states the number of functions with n objects and m components. There is one function of one object and one component ($a \to a$). There is one function of two objects and one component ($a \to b$). There are three functions of two objects and two components. We found three functions of three objects and two components, etc. This is shown in Table 2.

Table 2 The first column indicates how many distinct functions of n objects and m components. There is no general way of calculating the number of functions, except to find all possible functions and to determine which ones are equivalent.

# Functions	# Objects	# Components
1	1	1
1	2	1
3	2	2
3	3	2
7	3	3
1	4	2
9	4	3
	4	4
3	5	3
	5	4
	5	5
1	6	3
	6	4
	6	5
	6	6
$\vdots$	$\vdots$	$\vdots$

If f, g have the same number of objects, and the same number of components, then we have to find their canonical representation and the order relation $N_f < N_g$ determines the order relation $f < g$. Therefore, to compare two finite functions, it is sufficient to compute their canonical representations and compare these numbers. If, however, we wish to find the index k such that $N_k = N_f$, we have a slightly more complicated situation. We know how to find the canonical representation N_f of f, but if we want to know its position in the order we need more information than just its canonical representation. We have to know how many functions there are of less objects, and how many functions of the same number of objects but of less components. Then, we need to find the canonical representation of all functions with the same number of objects and same number of components. In the table above, we state there are seven functions of three components and three objects. We now provide these seven functions, and for simplicity of lecture and exposition we give arrows defining these functions. For example, the function defined by the three components $f(a) = f(b) = f(c) = a$ is the set of arrows of the last column. These are shown in Table 3.

Table 3 There is a total of seven functions of three objects and three components.

N_8	N_9	N_{10}	N_{11}	N_{12}	N_{13}	N_{14}
$a \to b$	$a \to b$	$a \to a$	$a \to a$	$a \to a$	$a \to a$	$a \to a$
$b \to c$	$b \to a$	$b \to c$	$b \to b$	$b \to a$	$b \to a$	$b \to a$
$c \to a$	$c \to a$	$c \to b$	$c \to c$	$c \to c$	$c \to b$	$c \to a$

Any function of three components and three objects is equivalent to one of these seven. These functions are next in the canonical ordering of finite functions; they are represented by the numbers $N_8, N_9, \ldots, N_{14}$. To know which of these seven functions is N_8, we have to find the canonical representation of all seven and the one with smallest canonical representation is the function N_8, then the function N_9 is the function with second smallest representation, etc. Of these seven functions, the one with largest representation is the function N_{14}. Here we give them in order from smallest to largest (left to right). We leave as an exercise for the reader to verify the canonical representations of these functions.

$$N_8 = 2^{2^1+2^4} + 2^{2^3+2^6} + 2^{2^5+2^2}$$
$$N_9 = 2^{2^1+2^6} + 2^{2^3+2^6} + 2^{2^5+2^4}$$
$$N_{10} = 2^{2^1+2^4} + 2^{2^3+2^2} + 2^{2^5+2^6}$$
$$N_{11} = 2^{2^1+2^2} + 2^{2^3+2^4} + 2^{2^5+2^6}$$
$$N_{12} = 2^{2^1+2^2} + 2^{2^3+2^6} + 2^{2^5+2^6}$$
$$N_{13} = 2^{2^1+2^4} + 2^{2^3+2^6} + 2^{2^5+2^6}$$
$$N_{14} = 2^{2^1+2^6} + 2^{2^3+2^6} + 2^{2^5+2^6}$$

To find the canonical representation of N_8, we observe the objects are all equivalent. Let $a = 2$, then we obviously have to make $b = 0$ and $c = 1$, because we have to maximize the term where a is image. The naming functions $b = 2, a = 1, c = 0$ and $c = 2, b = 1, a = 0$ also give the canonical representation. The canonical naming function of N_9 is also easy to find. We start by naming $a = 2$, since a is the most frequent object. Then we make $b = 1$ because b is the object that has more relations with a. In N_{10} we first make $a = 2$ because a is a fixed point; this ensures we have the term $2^5 + 2^6$. The objects b, c are equivalent in the function N_{10} because we have the two canonical naming functions $a = 2, b = 1, c = 0$ and $a = 2, b = 0, c = 1$. The rest of the canonical naming functions are easily found.

Now consider the function of two components and four objects defined by $f_{15}(a) = c$ and $f_{15}(b) = d$. The objects in the image have priority for being assigned larger numbers, so we start with naming $c = 3$ because c is in the image. Now, things change between choosing a, b, d for the value 2. Instead of assigning 2 to d, which is also in the image, we want to use the object that is related to $c = 3$. That would be the object $a = 2$. Then, assign the values $d = 1$ and $b = 0$. The components of the function are the ordered pairs $(2, 3)$ and $(0, 1)$ stating $f_{15}(2) = 3$ and $f_{15}(0) = 1$. The set of these ordered pairs is the canonical representation $N_{15} = 2^{2^1+2^4} + 2^{2^5+2^8}$; the summand $2^{2^1+2^4}$ represents the pair $(0, 1)$ and the second summand $2^{2^5+2^8}$ represents the pair $(2, 3)$. The naming function $d = 3, b = 2, c = 1, a = 0$ gives components $(0, 1)$ and $(2, 3)$ so that this is also a canonical naming function. Equivalent objects are those that can be assigned the same numerical value under different canonical naming functions. Therefore, a, b are equivalent and c, d are equivalent.

Next in order we have the functions of three components and four objects. Each of these nine functions is represented by one of the numbers $N_{16}, N_{17}, \ldots, N_{24}$. Any function of three components and four objects is equivalent to one of these nine. Table 4 provides these functions.

Table 4 There is a total of nine functions of four objects and three components.

N_{16}	N_{17}	N_{18}	N_{19}	N_{20}	N_{21}	N_{22}	N_{23}	N_{24}
$a \to c$	$a \to b$	$a \to b$	$a \to c$	$a \to d$	$a \to a$	$a \to a$	$a \to a$	$a \to a$
$b \to a$	$b \to a$	$b \to d$	$b \to c$	$b \to d$	$b \to c$	$b \to d$	$b \to b$	$b \to a$
$c \to d$	$c \to d$	$c \to d$	$c \to d$	$c \to d$	$c \to d$	$c \to d$	$c \to d$	$c \to d$

The smallest of these nine functions is $N_{16} = 2^{2^1+2^6} + 2^{2^5+2^8} + 2^{2^7+2^4}$ given by the canonical naming function $a = 2, b = 0$, $c = 3, d = 1$. The next function is $N_{17} = 2^{2^1+2^4} + 2^{2^5+2^8} + 2^{2^7+2^6}$ with canonical naming function $a = 3, b = 2, c = 0, d = 1$ and a, b are equivalent objects. The third is $N_{18} = 2^{2^1+2^6} + 2^{2^3+2^8} + 2^{2^5+2^8}$ under the naming $a = 0, b = 2, c = 1, d = 3$. Next is the function $N_{19} = 2^{2^3+2^8} + 2^{2^5+2^8} + 2^{2^7+2^2}$ with the naming function $a = 2, b = 1, c = 3, d = 0$ and a, b are equivalent objects. The function $N_{20} = 2^{2^1+2^8} + 2^{2^3+2^8} + 2^{2^5+2^8}$ has naming $a = 2, b = 1, c = 0, d = 3$ and a, b, c are equivalent objects. The function $N_{21} = 2^{2^3+2^6} + 2^{2^5+2^2} + 2^{2^7+2^8}$ is given by $a = 3, b = 1, c = 2, d = 0$. We have $N_{22} = 2^{2^1+2^6} + 2^{2^3+2^6} + 2^{2^7+2^8}$ with $a = 3, b = 1$, $c = 0, d = 2$ and b, c equivalent. The second largest is $N_{23} = 2^{2^1+2^4} + 2^{2^5+2^6} + 2^{2^7+2^8}$ with naming $a = 3, b = 2, c = 0, d = 1$ and a, b equivalent. Finally, we have $N_{24} = 2^{2^1+2^4} + 2^{2^5+2^8} + 2^{2^7+2^8}$ with $a = 3, b = 2, c = 0, d = 1$. By now we can see that is not trivial to find the canonical naming function of a finite function, in the general case. In this section we have to make careful observations to calculate the canonical naming functions, without having to find all possible representations. We will have two main problems to solve in the general case, and we will treat these computational strategies in future work. These are 1) finding the canonical naming function of any finite function, and 2) we need to know how many distinct abstract functions of n objects and m components. In the next section we will study the suborder of finite permutations, and it proves much easier to work with.

At this point the next functions in the order of all finite functions, are functions of four objects and four components. We leave the general analysis for future work, because finding all the possible distinct functions of four objects and four components is a little more laborious. Instead, let us find the functions that come after those; functions of three components and five objects. There is a total of three such functions.

$$\begin{array}{ccc} a \to a & a \to b & a \to d \\ b \to d & b \to d & b \to d \\ c \to p & c \to p & c \to p \end{array}$$

There is one function of three components and six objects.

$$a \to d$$
$$b \to p$$
$$c \to q$$

Let us find the representation of f^*, in example (8). We have five components, so our representation will be a set of five natural numbers. In the general case it is not possible to construct the largest representation, without constructing several possible representations. We know the canonical naming will have to assign $\eta(a) = 5$. This guarantees we have $2^{11} + 2^{12} \in N_{f^*}(\rho)$ representing $f^*(a) = a$. There is no object that has a relation with a, so we must find out which object, of the remaining objects b, c, d, p, q, will be assigned the value 4. If we make $\rho(c) = 4$ we maximize the representation because we will have two components with the power 2^{10}; namely the components $f^*(b) = c$ and $f^*(d) = c$. We choose $\rho(b) = 3$ instead of $\rho(d) = 3$ because b is related to c by two components. This leaves us with $\rho(d) = 2$. Now we have to assign $q = 1$ and $p = 0$. The canonical representation of

$$f^*(a) = a$$
$$f^*(b) = c$$
$$f^*(c) = b$$
$$f^*(d) = c$$
$$f^*(p) = q$$

under the canonical naming ρ is

$$N_{f^*} = 2^{2^1 + 2^4} 2^{2^5 + 2^{10}} + 2^{2^7 + 2^{10}} + 2^{2^9 + 2^8} + 2^{2^{11} + 2^{12}}$$

and there are no equivalent objects.

3.4 Finite Permutations

The suborder of permutations is easier to find, in part because it is well behaved with respect to cardinality (size). Let f a permutation on m objects and g a permutation on $n > m$ objects, then $N_f < N_g$. Furthermore, permutations are ordered by complexity. Given permutations f, g of the same size, then we can order these permutations and the interpretation is that a larger number is a simpler permutation. The identity permutation of size n has larger representation than all other permutations of size n. The one cycle permutation of n objects has the smallest representation. The number of distinct abstract permutations of size n, is equal to the number of additive partitions of n. Let us order the first few permutations. The unique permutation P_0, of size 1, is the function f_0 of one component, represented by $N_0 = 2^6$. There are two permutations of size 2, the functions N_2 and N_3. There is a total of three permutations of size 3. These are the functions N_8, N_{10}, N_{11}. The smallest of these three numbers, N_8, represents the one cycle permutation. The middle permutation, N_{10}, leaves one object fixed. The largest, N_{11}, represents the identity permutation. Call these first six permutations $P_0 = N_0, P_1 = N_2, P_2 = N_3, P_3 = N_8, P_4 = N_{10}, P_5 = N_{11}$. Let us order the five distinct permutations of size 4. These are given in order in Table 5.

Table 5 There is a total of five permutations of four objects.

P_6	P_7	P_8	P_9	P_{10}
$a \to b$	$a \to b$	$a \to a$	$a \to a$	$a \to a$
$b \to c$	$b \to a$	$b \to c$	$b \to b$	$b \to b$
$c \to d$	$c \to d$	$c \to d$	$c \to d$	$c \to c$
$d \to a$	$d \to c$	$d \to b$	$d \to c$	$d \to d$

If two objects are in the same cycle, then they are equivalent. The converse is not true. For example all objects of P_{10} are equivalent but they are all in different cycles. For P_6, we have the canonical naming function $a = 3, b = 1, c = 0, d = 2$. To find this naming function, observe all the objects are equivalent, so we choose $a = 3$, without loss of generality. Next, we have to maximize the term where a is in the image. Thus, we define $d = 2$. Then to maximize the term where a is in the preimage, we make $b = 1$. This leaves us with $c = 0$. In the second permutation a, b and c, d are pairs of equivalent objects and a canonical naming function is $a = 3, b = 2, c = 1, d = 0$. The third permutation has the naming $a = 3, b = 2, c = 0, d = 1$ and b, c, d are equivalent. Next we have the naming $a = 3, b = 2, c = 1$ $d = 0$ with c, d equivalent. Any naming function of P_{10} is canonical. Therefore, all objects are equivalent. The fact that all objects are equivalent does not imply every naming is the canonical naming. An example of this is P_6.

$$P_6 = 2^{2^1+2^6} + 2^{2^3+2^2} + 2^{2^5+2^8} + 2^{2^7+2^4}$$
$$P_7 = 2^{2^1+2^4} + 2^{2^3+2^2} + 2^{2^5+2^8} + 2^{2^7+2^6}$$
$$P_8 = 2^{2^1+2^4} + 2^{2^3+2^6} + 2^{2^5+2^2} + 2^{2^7+2^8}$$
$$P_9 = 2^{2^1+2^4} + 2^{2^3+2^2} + 2^{2^5+2^6} + 2^{2^7+2^8}$$
$$P_{10} = 2^{2^1+2^2} + 2^{2^3+2^4} + 2^{2^5+2^6} + 2^{2^7+2^8}$$

To find the maximum $N_f(\rho) = \max_\eta \{N_f(\eta)\}$, over all possible naming η, we must find the canonical naming providing the largest representation. We wish to maximize the set number $\{\{a, f(a)\}, \{b, f(b)\}, \{c, f(c)\}, \{d, f(d)\}\}$. We know $2^7 + 2^8 \in f$ if and only if $f(x) = x$ for some $x \in \{a, b, c, d\}$. If there are no fixed points we look for cycles of two objects, and continue looking for the smallest possible cycle, to assign the largest values of the naming. The largest possible set number that can represent an abstract permutation of four elements is $2^{2^1+2^2} + 2^{2^3+2^4} + 2^{2^5+2^6} + 2^{2^7+2^8}$, representing the identity permutation $(0)(1)(2)(3)$. The number N_f measures and compares the *movement* a permutation causes. If f has more movements than g, then $N_f > N_g$. The more complicated a permutation becomes the smaller its representation becomes (holding fixed the size). Intuitively, assigning larger values to objects in smaller cycles helps to maximize the representation.

We will give one more example of permutations before applying the same method to define groups. Let f be the permutation $(a)(b, c)(p, q, r)$ on the set of abstract objects $\{a, b, c, d, p, q, r\}$. We wish to find a canonical ordering of its elements, and the canonical representation N_f. It should result in $a = 5$, $b = 4$, $c = 3$, $p = 2$, $q = 0$, $r = 1$, or one of its equivalent numbering functions, and

$$N_f = 2^{2^1+2^4} + 2^{2^3+2^6} + 2^{2^5+2^2} + 2^{2^7+2^{10}} + 2^{2^9+2^8} + 2^{2^{11}+2^{12}}.$$

In all the equivalent numbering functions, we have $a = 0$. We can change $b = 3$ and $c = 4$. We can also change the values of the objects in the 3-cycle. If we make $q = 2$ then we have $p = 1$ and $r = 0$. If $r = 2$, then $q = 1$ and $p = 0$.

4 Finite Groups

Using the results from the previous sections, we can represent finite groups as natural numbers. A finite group $G(*)$ is a bijection that assigns permutations, of the set G, to objects of G. Operation functions are the elements in the image of $* : G \to Aut(G)$. Consider a naming η of the set G. Then the objects of G, and the operation functions of G are set numbers. Thus, we can say $*$ is a function of the form $M \to N$, where $\max(M) < \min(N)$. If the group has k elements, the domain $M = Dom(*)$ is the set number $\{0, 1, 2, \dots, k-1\} = 2^k - 1$. The image $N = Im(*)$ is the set number $\{*0, *1, *2, \dots, *k\}$, where $*x$ are concrete permutations of $\{0, 1, 2, \dots, k-1\}$. Notice that the operation functions N_{*x} do not have canonical form because they are concrete functions. We turned the operation function $*x$ into a natural number $N_{*x}(\eta)$, by providing the naming function η. The definition of group we provide satisfies the definition of function, given above. Every finite group is a set number whose elements are ordered pairs. The ordered pairs are sets of two objects; one odd and one even. The first components are odd numbers $2i + 1$, for every $i \in \{0, 1, 2, \dots, k-1\}$. The second components are even numbers representing permutations, $2(N_{*x} + 1)$. Every naming function η defines a natural number $N_G(\eta)$, that depends on the group and the naming function of that group. There is a finite number of these representations. The maximum representation is the canonical representation $N_G = \max\{N_G(\eta)\}_\eta$ of the group G. This canonical representation gives us a canonical ordering of the elements of G, as well. It behaves much like the representations of permutations. Here we assign the largest value to the identity element, $e = k - 1$.

A group is a set number of the form

$$2^{2^{2(k-1)+1}+2^{2\left(2^{(2^1+2^2)}+2^{(2^3+2^4)}+\cdots+2^{(2^{2k-1}+2^{2(k-1+1)})}+1\right)}} + 2^{2^{2(k-2)+1}+2^{2\left(2^{(2^1+2^a)}+2^{(2^3+2^b)}+\cdots+2^{(2^{2k-1}+2^{2(k-2+1)})}+1\right)}} +$$
$$+ 2^{2^{2(k-3)+1}+2^{2\left(2^{(2^1+2^c)}+2^{(2^3+2^d)}+\cdots+2^{(2^{2k-1}+2^{2(k-3+1)})}+1\right)}} + 2^{2^{2(k-4)+1}+2^{2\left(2^{(2^1+2^x)}+2^{(2^3+2^y)}+\cdots+2^{(2^{2k-1}+2^{2(k-4+1)})}+1\right)}} + \dots$$
$$\dots + 2^{2^{2(0)+1}+2^{2\left(2^{(2^1+2^z)}+2^{(2^3+2^w)}+\cdots+2^{(2^{2k-1}+2^{2(0+1)})}+1\right)}},$$

where the $k-1$ numbers $a, b, \dots$ are distinct elements of $\{2, 6, 8, \dots, 2k-6, 2k-4, 2k\}$, the $k-1$ numbers $c, d, \dots$ are distinct elements of $\{2, 4, 8, \dots, 2k-6, 2k-2, 2k\}$, the $k-1$ numbers $x, y, \dots$ are distinct elements of $\{2, 4, 8, \dots, 2k-8, 2k-4, 2k-2, 2k\}$. The numbers $z, w, \dots$ are distinct elements of $\{4, 6, \dots, 2k\}$. Also, the $a, c, x, z, \dots$ are different; all the $b, d, y, w, \dots$ are different, etc. The first term, $2^{2^{2(k-1)+1}+2^{2\left(2^{(2^1+2^2)}+2^{(2^3+2^4)}+\cdots+2^{(2^{2k-1}+2^{2(k-1+1)})}+1\right)}}$, tells us that $e = k - 1$ is assigned to the identity function. Not all natural numbers of this form are groups. We additionally require the associative property. Later in this section we will see that verifying the associative property is a straightforward process; we are able to verify this through numeric computation. For that end, we will study the composition of functions, numerically. But before that, we give our main result. With abstract permutations we had a canonical representation, given by a canonical naming of the objects. This naming had equivalent naming functions, if we had equivalent objects. Here we have the same situation, now in the context of groups.

Theorem 7 *Given a finite group G of order k, We have a naming function* $\rho : G \to \{0,1,2,\ldots,k-1\}$ *and a canonical represen-tation* $N_G = \max_{\eta} N_G(\eta) = N_G(\rho)$. *We say that* ρ *is the canonical ordering of G, and* $\rho(e) = k-1$. *Two distinct group objects* x,y *are equivalent if their exists two distinct canonical orderings* ρ_1, ρ_2 *such that* $\rho_1(x) = \rho_2(y)$.

This gives a well defined linear order on the set of finite groups. Two groups have the same canonical representation if and only if they are isomorphic. This linear order is well behaved with respect to cardinality; $|G| < |H|$ *implies* $N_G < N_H$.

We will also speak of the order of a group element, $|g|$, as the smallest power n such that $g^n = e$. We will have to assign the identity element to $k-1$, in order to maximize our representation. Then we must identify the objects of smallest order, in G; this number is the smallest prime number that divides $|G|$. We will assign $k-2$ to one of these objects. To know how we proceed further, we will illustrate by constructing and representing the groups of the first few orders.

We start with the trivial group of one object. The group G_0 is determined by the relation $*a(a) = a$. We have the trivial naming $a = 0$ and the operation function N_{*0} is the one component function $P_0 = N_0 = 2^{2^1 + 2^2}$. The canonical representation is

$$G_0 = 2^{2^{2(0)+1} + 2^{2\left(2^{2^1+2^2}+1\right)}} = 2^{2^1 + 2^2\left(2^6+1\right)}.$$

This number has 10^{19} decimal digits. It does not matter, how large it is, because we are able to easily manipulate and interpret these large numbers in terms of simple operations and functions for much smaller numbers. Simply said, we can work with these large representations.

Before continuing on to more groups, we clarify the use of a table notation, based on the fact that we are trying to represent a set of permutations. We will use the same notation of a column of arrows to represent a single permutation, but now we will ignore the arrows. For example, the permutation $(a,b)(c)(d)$ can be written as

$$a \ b$$
$$b \ a$$
$$c \ c$$
$$d \ d$$

If we wish to represent several permutations of the same size, we can do this in a single rectangular grid. For this, we need to use one column as a pivot for the rest. For example, the set of permutations $\{(a,b)(c)(d), \ (a,b,c,d), \ (a)(c,b)(d), (a)(b)(c)(d)\}$ can be written as a single rectangular grid of $4+1$ columns. The first (left-most) column serves as pivot by which all other columns are defined. The second column represents the permutation $(a,b)(c)(d)$, the third column represents the permutation (a,b,c,d), the fourth column is $(a)(b,c)(d)$ and the fifth column is $(a)(b)(c)(d)$.

$$c \ c \ d \ b \ c$$
$$a \ b \ b \ a \ a$$
$$b \ a \ c \ c \ b$$
$$d \ d \ a \ d \ d$$

In the particular case of groups, the table is square and rows and columns do not repeat objects. Additionally, we need to have one column equal to the identity permutation, so we have the following convention. The left-most column will represent the identity permutation and we only need to write it once. The identity object will be in the upper left hand corner. The second column is representing the operation function of the second object in the first column. The third column represents the operation function of the third object in the first column. In general, if a is the $k-th$ object in the first column, then the operation function $*a$ is represented in the $k-th$ column table. This simply means that we will write an operation in the usual table form, so that the following table has products such as $e*e = e$, $a*e = a$, $b*b = e$, $a*c = e$, and the like.

$$e \ a \ b \ c$$
$$a \ b \ c \ e$$
$$b \ c \ e \ a$$
$$c \ e \ a \ b$$

This simply means that given any fixed position, the object in that position is expressed in terms of the first objects of that row and column. This form of writing the operation functions coincides with the multiplication table of the group. If x is the $k-th$ object in the first row, then the $k-th$ column gives the function $*x$.

In our process of finding representations and naming functions of groups, we will also need to verify the associative property holds. This is given by a simple rule on the table. Let x be any object in a group G of order n. We know x appears in the table exactly n times; once in each column/row. Each one of the positions where x appears, gives us an expression for x in terms of two objects; a factorization $x = y*z$. Given a table representing a set of operation functions, the operation satisfies the associative property table if and only if $*x = *y \circ *z$, for every factorization $x = y*z$ of every $x \in G$. In the table example above, we have $b = a*a$ so that we need to verify $*b = *a \circ *a$. To verify this is true, we have to verify $*b(g) = (*a \circ *a)(g)$ for every $g \in G$. To find $b*c = *b(c)$, we have the arrows $c \to_{*a} e \to_{*a} a$. We also have $b*a = *b(a)$ given by the arrows $a \to_{*a} b \to_{*a} c$. For another example, take the product $e = c*a$. This means we have to verify $*c \circ *a$ is the identity function. Let us find $(*c \circ *a)(b)$. We have the arrows $b \to_{*a} c \to_{*c} b$. We also have $(*c \circ *a)(a)$ given by $a \to_{*a} b \to_{*c} a$, etc.

We continue with the construction of groups, having in mind the above rules. Let us start with a group of two objects.

$$e \ g_1$$
$$g_1$$

We know, g_1 has an inverse $\neq e$, so we must have $g_1 * g_1 = e$,

$$e \ g_1$$
$$g_1 \ e$$

The canonical naming function is trivial to find. In order to maximize our representation, we make $e = 1$, $g_1 = 0$. The group has numeric table

$$1 \ 0$$
$$0 \ 1$$

Let us find the canonical representation of this group. Our group is an operation. This operation is a concrete function of two components. The first component is $*(1) = \mathbf{id}$, that sends 1 to the identity function. The second component of our operation is $*(g_1) = (0,1)$, that sends the object 0 to the concrete permutation $(0,1)$. The canonical representation has two terms. The first term representing the first component is $2^{2^{2(1)+1}+2^2\left(2^{2^3+2^4}+2^{2^1+2^2}+1\right)}$. The second component is given by the expression $2^{2^{2(0)+1}+2^2\left(2^{2^3+2^2}+2^{2^1+2^4}+1\right)}$. The canonical representation of $\mathbb{Z}_2$ is

$$
\begin{aligned}
G_{\mathbb{Z}_2} &= 2^{2^{2(1)+1}+2^2\left(2^{2^3+2^4}+2^{2^1+2^2}+1\right)} + 2^{2^{2(0)+1}+2^2\left(2^{2^3+2^2}+2^{2^1+2^4}+1\right)} \\
&= 2^{2^3+2^2\left(2^6+2^{24}+1\right)} + 2^{2+2^2\left(2^{18}+2^{12}+1\right)}.
\end{aligned}
\tag{9}
$$

Why do we say (9) is the canonical representation? The canonical representation is the maximum of the representations. In this case we have two possible representations, one for each naming function. If we had used the naming $e = 0$ and $g_1 = 1$, we would have the representation

$$2^{2^{2(0)+1}+2^2\left(2^{2^3+2^4}+2^{2^1+2^2}+1\right)} + 2^{2^{2(1)+1}+2^2\left(2^{2^3+2^2}+2^{2^1+2^4}+1\right)}$$

because now 0 is assigned to the identity function, while 1 is assigned the permutation $(0,1)$. This representation is smaller than the canonical representation above. The reader should understand why this is true, before moving on to the next examples. Remember, we will always assign the largest number of the naming, to the identity object because this maximizes our representation. We will see how to name the rest of the objects, to obtain the canonical representation.

If we wish to make a distinction, we say a *term* is a number representing a component $x \rightarrow_* *x$. The upper terms are the numbers representing components of the operation functions; we call them *sub terms*. For example, $2^{2^3+2^2}$ is a sub term of the term $2^{2^{2(0)+1}+2^2\left(2^{2^3+2^2}+2^{2^1+2^4}+1\right)}$. Terms are ordered pairs; they are elements of the set $\bigcup_i (i,)$, defined at the beginning of section 4.1. Notice in the second equality, that sub terms are also ordered pairs. For example, the sub term $2^{2^3+2^2}$ and the term $2^3 + 2^2\left(2^6+2^{24}+1\right)$ are both numbers of the form $2^{2m+1} + 2^{2(n+1)}$. They are both concrete arrows.

4.1 $|G| = 3$

Next we have the groups of three objects. We start with our table

$$e \ g_1 \ g_2$$
$$g_1$$
$$g_2$$

All objects of G have to satisfy $|g| \mid 3$, so that we have $|g| = 3$ for all $g \in G$. This means $g_1^2 \neq e$. Since g_1 is not the identity element, we also know $g_1^2 \neq g_1$. Therefore g_1^2 is a new object g_2, and $g_1 * g_2 = g_1^3 = e$.

$$e \ g_1 \ g_2$$
$$g_1 \ g_2$$
$$g_2 \ e$$

Use the associative rule to find the column of g_2. We know $g_2 = g_1^2$ so that $*g_2$ is the function $*g_1 \circ *g_1$. To find $*g_2(g_1)$ we follow the arrows $g_1 \rightarrow_{*g_1} g_2 \rightarrow_{*g_1} e$ so that $g_2 * g_1 = e$. In the same way, we find $g_2 \rightarrow_{*g_1} e \rightarrow_{*g_1} g_1$ so that $g_2^2 = g_1$.

$$e \ g_1 \ g_2$$
$$g_1 \ g_2 \ e$$
$$g_2 \ e \ g_1$$

This is the group $\mathbb{Z}_3$. We wish to find the canonical naming function. We start with $e = 2$. One of the non trivial objects g_1, g_2 will have to be assigned the value 1 and the other will be assigned the value 0. We wish to know which of the two objects will be assigned the value 1 and which will be assigned the value 0. Let us say $a \in \{g_1, g_2\}$ is the object that is assigned $a = 1$, and say $b \in \{g_1, g_2\}$ is the object that will be assigned $b = 0$. If we list these objects in table form,

$$
\begin{array}{ccc}
e & a & b \\
a & & \\
b & &
\end{array}
$$

then the complete table

$$
\begin{array}{ccc}
e & a & b \\
a & b & e \\
b & e & a
\end{array}
$$

is already determined. This means, it does not matter who we choose to be a or b; they are equivalent objects. We have two different canonical naming functions. These are $\rho_1 : e = 2, g_1 = 1, g_2 = 0$, and $\rho_2 : e = 2, g_1 = 0, g_2 = 1$. Either of these naming functions will give the numerical table

$$
\begin{array}{ccc}
2 & 1 & 0 \\
1 & 0 & 2 \\
0 & 2 & 1
\end{array}
\tag{10}
$$

The canonical representation of the group is a concrete function of three components. We can use either of the two canonical naming functions to find it. The first component is the ordered pair that assigns 2 to the identity permutation $(1)(2)(3)$ because $e = 2$ is the identity object. This ordered pair is represented by the number

$$
2^{2^{2(2)+1}+2^{2\left(2^{2^5}+2^6+2^{2^3}+2^4+2^{2^1}+2^2+1\right)}}.
$$

The second component assigns $a = 1$ to the concrete permutation $(2, 1, 0)$ because this is the permutation represented by the column of 1, in (10). This component is given by

$$
2^{2^{2(1)+1}+2^{2\left(2^{2^5}+2^4+2^{2^3}+2^2+2^{2^1}+2^6+1\right)}}.
$$

The object $b = 0$ is assigned the permutation $(2, 0, 1)$ because this is the permutation given by the column of 0, in table (10). The third term is the number

$$
2^{2^{2(0)+1}+2^{2\left(2^{2^5}+2^2+2^{2^3}+2^6+2^{2^1}+2^4+1\right)}}.
$$

The canonical representation is the number

$$
G_{\mathbb{Z}_3} = 2^{2^{2(2)+1}+2^{2\left(2^{2^5}+2^6+2^{2^3}+2^4+2^{2^1}+2^2+1\right)}} + 2^{2^{2(1)+1}+2^{2\left(2^{2^5}+2^4+2^{2^3}+2^2+2^{2^1}+2^6+1\right)}} + 2^{2^{2(0)+1}+2^{2\left(2^{2^5}+2^2+2^{2^3}+2^6+2^{2^1}+2^4+1\right)}}
$$
$$
= 2^{2^5+2^{2\left(2^6+2^{24}+2^{96}+1\right)}} + 2^{2^3+2^{2\left(2^{66}+2^{12}+2^{48}+1\right)}} + 2^{2^1+2^{2\left(2^{18}+2^{72}+2^{36}+1\right)}}
$$

This number is approximately as large as $10^{10^{10^{28}}}$.

4.2 $|G| = 4$

Before moving on to finding groups of four objects, we bring one more thing to attention. Given a finite group G, the list of all the operations $a * b$ is a system of equations that defines the group. Our procedure for finding a group of order n, will provide us with a *minimal set of independent equations* that determine the group. The complete list of operations is not needed; we minimize the number of expressions. The group $\mathbb{Z}_2$ is determined by the expression $a^2 = e$ (trivial expressions, $e^2 = e$ and $e * x = x * e = x$ do not have to be written down). So, we can say $\mathbb{Z}_2$ is a group determined by one equation. The group $\mathbb{Z}_3$ is given by the expressions $a^2 = b$ and $a^3 = e$. From these two equation, we can derive the complete list of operations of the group. We will try to find all groups with less than ten objects. For each, we will give the the minimum independent set of equations, the canonical naming functions of its elements, the set of automorphisms, the canonical table and canonical numeric representation. We will also compare canonical numeric representations to find the linear order of the first few groups.

Klein 4-Group. We start with a set $\{e, g_1, g_2, g_3\}$. There is at least one object with order equal to the smallest prime divisor of 4; suppose $g_1^2 = e$, without loss of generality.

$$
\begin{array}{cccc}
e & g_1 & g_2 & g_3 \\
g_1 & e & g_3 & g_2 \\
g_2 & g_3 & & \\
g_3 & g_2 & &
\end{array}
\tag{11}
$$

Now we can make $g_2^2 = e$ or $g_2^2 = g_1$. Suppose we have the first case. Then the Klein four-group, $K(4)$, is determined. Any group of of four elements e, g_1, g_2, g_3 such that $e = g_1^2 = g_2^2$, is isomorphic to $K(4)$.

$$
\begin{array}{cccc}
e & g_1 & g_2 & g_3 \\
g_1 & e & g_3 & g_2 \\
g_2 & g_3 & e & g_1 \\
g_3 & g_2 & g_1 & e
\end{array}
$$

Let us find the canonical naming functions. Start with $e = 3$; their are three remaining objects $a = 2, b = 1, c = 0$. To find a, b, and c, start with the list of objects in table form. All the non trivial objects are second order objects.

$$
\begin{array}{cccc}
e & a & b & c \\
a & e & & \\
b & & e & \\
c & & & e
\end{array}
$$

whoever a, b, c may be. This determines the group,

$$
\begin{array}{cccc}
e & a & b & c \\
a & e & c & b \\
b & c & e & a \\
c & b & a & e
\end{array}
$$

This means that any naming function with $e = 3$ is a canonical naming function. The objects g_1, g_2, g_3 are all equivalent, so that $K(4)$ has a total of six canonical naming functions. The object $a = 2$ can be chosen from three possible options. The object $b = 1$ can be chosen from the remaining two objects and $c = 0$ is determined as the remaining object. A naming function will be represented by a sequence. For example, the naming function $e = 3$, $g_1 = 2$, $g_2 = 1$, $g_3 = 0$ is written as (e, g_1, g_2, g_3). The six naming functions are

$$
\begin{array}{ccc}
(e, g_1, g_2, g_3) & (e, g_2, g_1, g_3) & (e, g_3, g_1, g_2) \\
(e, g_1, g_3, g_2) & (e, g_2, g_3, g_1) & (e, g_3, g_2, g_1)
\end{array}
$$

Any naming function with $e = 3$, gives the numeric table

$$
\begin{array}{cccc}
3 & 2 & 1 & 0 \\
2 & 3 & 0 & 1 \\
1 & 0 & 3 & 2 \\
0 & 1 & 2 & 3
\end{array}
$$

and canonical representation

$$
N_{K(4)} = 2^{2^7 + 2^{2\left(2^{(2^7+2^8)} + 2^{(2^5+2^6)} + 2^{(2^3+2^4)} + 2^{(2^1+2^2)} + 1\right)}} + 2^{2^5 + 2^{2\left(2^{(2^7+2^6)} + 2^{(2^5+2^8)} + 2^{(2^3+2^2)} + 2^{(2^1+2^4)} + 1\right)}}
$$
$$
+ 2^{2^3 + 2^{2\left(2^{(2^7+2^4)} + 2^{(2^5+2^2)} + 2^{(2^3+2^8)} + 2^{(2^1+2^6)} + 1\right)}} + 2^{2^1 + 2^{2\left(2^{(2^7+2^2)} + 2^{(2^5+2^4)} + 2^{(2^3+2^6)} + 2^{(2^1+2^8)} + 1\right)}}.
$$

The first term is the component that sends 3 to the identity function $(1)(2)(3)(4)$, while the second term is the component that sends 2 to the permutation $(0, 1)(2, 3)$, etc.

We bring something new to attention. The group $K(4)$ has a total of six automorphisms, and we have found a total of six distinct canonical naming functions. This in not coincidental. Each of these six naming functions determines an automorphism of $K(4)$. We simply need to hold one of these fixed as *pivot*. For example, take the pivot $A = (e, g_3, g_1, g_2)$ which will be held fixed. Choose a second canonical naming function $B = (e, g_1, g_3, g_2)$. The function that sends the first component of A to the first component of B, and the second component of A to the second component of B, etc. is called a *component function*. The component function $\phi : A \to B$ is an automorphism, for every canonical naming function B. That is to say, ϕ that acts by $e \mapsto e$, $g_1 \mapsto g_3$, $g_2 \mapsto g_2$, $g_3 \mapsto g_1$ is an automorphism of $K(4)$. If we choose $B = A$ then we obviously are describing the identity automorphism. We let B be any of the of the canonical naming functions to obtain all six automorphisms. Our initial choice of A is inconsequential; any choice for A gives the same set of component functions.

Cyclic group $\mathbb{Z}_4$. Going back to table (11), consider the second case, $g_2^2 = g_1$. This determines the table

$$
\begin{array}{cccc}
e & g_1 & g_2 & g_3 \\
g_1 & e & g_3 & g_2 \\
g_2 & g_3 & g_1 & e \\
g_3 & g_2 & e & g_1
\end{array}
$$

This is the cyclic group $\mathbb{Z}_4$, determined by the equations $g_1^2 = e$ and $g_2^2 = g_1$. To find the canonical representation, we are careful assigning the values. We will assign the values $2, 1, 0$ to the objects a, b, c, respectively. We do not know which object of $\mathbb{Z}_4$ is a, b, c. If we assign $a = 2$ to one of the objects g_2, g_3, we will have the numeric table

$$
\begin{array}{l}
3\ 2\ 1\ 0 \\
2\ 1 \\
1 \\
0
\end{array}
$$

On the other hand, if $a = 2$ is assigned to the second order object, g_1, we have the table

$$
\begin{array}{l}
3\ 2\ 1\ 0 \\
2\ 3 \\
1 \\
0
\end{array}
$$

The latter maximizes the representation. Intuitively, we are trying to assign the larger numbers by giving priority to the left-most columns. Within a column we are giving priority to the objects of upper rows. we place larger numbers further to the left and then further to the top of the table. The rest of the table is determined.

$$
\begin{array}{l}
3\ 2\ 1\ 0 \\
2\ 3\ 0\ 1 \\
1\ 0\ 2\ 3 \\
0\ 1\ 3\ 2
\end{array}
$$

Any naming function with $e = 3$, $g_1 = 2$ is a canonical naming function. One canonical naming function is $e = 3$, $g_1 = 2$, $g_2 = 1$, $g_3 = 0$ which is written as (e, g_1, g_2, g_3). The other canonical naming function is (e, g_1, g_3, g_2). This implies g_2, g_3 are equivalent objects. We have two automorphisms. Fix $A = (e, g_1, g_3, g_2)$. If we consider $B = (e, g_1, g_2, g_3)$ we have determined the automorphism with components $e \mapsto e$, $g_1 \mapsto g_1$, $g_2 \mapsto g_3$, $g_3 \mapsto g_2$. If we make $B = A$ we have determined the identity automorphism. The canonical representation is

$$
N_{\mathbb{Z}_4} = 2^{2^7 + 2^2\left(2^{(2^7+2^8)}+2^{(2^5+2^6)}+2^{(2^3+2^4)}+2^{(2^1+2^2)}+1\right)} + 2^{2^5 + 2^2\left(2^{(2^7+2^6)}+2^{(2^5+2^8)}+2^{(2^3+2^2)}+2^{(2^1+2^4)}+1\right)}
$$
$$
+ 2^{2^3 + 2^2\left(2^{(2^7+2^4)}+2^{(2^5+2^2)}+2^{(2^3+2^6)}+2^{(2^1+2^8)}+1\right)} + 2^{2^1 + 2^2\left(2^{(2^7+2^2)}+2^{(2^5+2^4)}+2^{(2^3+2^8)}+2^{(2^1+2^6)}+1\right)}.
$$

We wish to compare the groups $K(4)$ and $\mathbb{Z}_4$ in terms of the order of natural numbers. The odd number of the terms do not determine the order because the even numbers, representing the operation functions, are much larger than the odd numbers. The group with the largest operation function, that is not in both groups, is the larger of the two. The group $K(4)$ has larger numeric representation than $\mathbb{Z}_4$ because $K(4)$ has the largest operation function that is not in both groups; $N_{\mathbb{Z}_4} < N_{K(4)}$. As we would expect, the cyclic group has the smallest representation, just as the one cycle permutation (a, b, c, d) has smaller representation than $(a, b)(c, d)$.

4.3 $|G| = 5$

If G is a group with five objects, we know that all non trivial objects satisfy $|g| \,\big|\, 7$. This implies $|g| = 7$, for all non trivial $g \in G$. Without loss of generality, choose any object g_1. Then, g_1^2 is a non trivial object, g_2. We find $g_1 * g_2 = g_1^3$ is a new non trivial object, g_3, etc.

$$
\begin{array}{l}
e\ \ g_1\ g_2\ g_3\ g_4 \\
g_1\ g_2 \\
g_2\ g_3 \\
g_3\ g_4 \\
g_4\ \ e
\end{array}
$$

Now, we have to use the associative property to find the operation function of g_2, and it will be placed in the second column. We know $g_2 = g_1 * g_1$, so that we must have $*g_2 = *g_1 \circ *g_1$. This means $*g_2(g_1)$ is found by $g_1 \to_{*g_1} g_2 \to_{*g_1} g_3$. We also have $*g_2(*g_2)$ because $g_2 \to_{*g_1} g_3 \to_{*g_1} g_4$, etc.

$$
\begin{array}{l}
e\ \ g_1\ g_2\ g_3\ g_4 \\
g_1\ g_2\ g_3 \\
g_2\ g_3\ g_4 \\
g_3\ g_4\ g_5 \\
g_4\ \ e\ \ g_1
\end{array}
$$

We do the same with the column of $g_3 = g_1 * g_2$ and $g_4 = g_1 * g_3$, so that $*g_3 = *g_1 \circ *g_2$ and $*g_4 = *g_1 \circ *g_3$. For example, $g_3 * g_1 = *g_3(g_1)$ is given by the arrows $g_1 \to_{*g_2} g_3 \to_{*g_1} g_4$, etc.

$$e \ g_1 \ g_2 \ g_3 \ g_4$$
$$g_1 \ g_2 \ g_3 \ g_4 \ e$$
$$g_2 \ g_3 \ g_4 \ e \ g_1$$
$$g_3 \ g_4 \ e \ g_1 \ g_2$$
$$g_4 \ e \ g_1 \ g_2 \ g_3$$

The group is defined by the number of objects, so that there exists only one group, $\mathbb{Z}_5$, of five objects. Let us find the canonical naming functions. We know that we must make $e = 4$ and $a = 3$ for some object $a \in \mathbb{Z}_5$ such that $|a| = 5$. However, all non trivial objects have order 5, so that a can be any non trivial object.

If we wish to maximize the representation, the object $b = a^2$ has to be assigned the numerical value 2.

$$4 \ 3 \ 2 \ 1 \ 0$$
$$3 \ 2$$
$$2$$
$$1$$
$$0$$

The new object $c = a * b = a^3$ is assigned the value 1, and $d = a^4$ is assigned the value 0.

$$4 \ 3 \ 2 \ 1 \ 0$$
$$3 \ 2$$
$$2 \ 1$$
$$1 \ 0$$
$$0 \ 4$$

Using the associative property, we find the rest of the table

$$4 \ 3 \ 2 \ 1 \ 0$$
$$3 \ 2 \ 1 \ 0 \ 4$$
$$2 \ 1 \ 0 \ 4 \ 3$$
$$1 \ 0 \ 4 \ 3 \ 2$$
$$0 \ 4 \ 3 \ 2 \ 1$$

This numerical table is given by four different naming functions. Consider the naming function that has $e = 4$ and $g_4 = 3$. Then $g_4^2 = g_3 = 2$, and $g_4^3 = g_2 = 1$, and $g_4^4 = g_1 = 0$. This naming functions is represented by the sequence (e, g_4, g_3, g_2, g_1). The four canonical naming functions are

$$(e, g_1, g_2, g_3, g_4)$$
$$(e, g_2, g_4, g_1, g_3)$$
$$(e, g_3, g_1, g_4, g_2)$$
$$(e, g_4, g_3, g_2, g_1)$$

These four canonical naming functions are actually the automorphisms of $\mathbb{Z}_5$, in disguise. Fix any one of these naming functions, say $A = (e, g_3, g_1, g_4, g_2)$. Let B any other canonical naming function, say $B = (e, g_2, g_4, g_1, g_3)$. The bijective function defined below is an automorphism.

$$e \mapsto e$$
$$g_1 \mapsto g_4$$
$$g_2 \mapsto g_3$$
$$g_3 \mapsto g_2$$
$$g_4 \mapsto g_1$$

Let B any other canonical naming functions, say $B = (e, g_4, g_3, g_2, g_1)$. We have determined a second automorphism

$$e \mapsto e$$
$$g_1 \mapsto g_3$$
$$g_2 \mapsto g_1$$
$$g_3 \mapsto g_4$$
$$g_4 \mapsto g_2$$

We find all four automorphisms of $\mathbb{Z}_5$ using the four canonical naming functions. The canonical representation is

$$N_{\mathbb{Z}_5} = 2^{2^9 + 2^2\left(2(2^9+2^{10}) + 2(2^7+2^8) + 2(2^5+2^6) + 2(2^3+2^4) + 2(2^1+2^2) + 1\right)} + 2^{2^7 + 2^2\left(2(2^9+2^8) + 2(2^7+2^6) + 2(2^5+2^4) + 2(2^3+2^2) + 2(2^1+2^{10}) + 1\right)}$$
$$+ 2^{2^5 + 2^2\left(2(2^9+2^6) + 2(2^7+2^4) + 2(2^5+2^2) + 2(2^3+2^{10}) + 2(2^1+2^8) + 1\right)} + 2^{2^3 + 2^2\left(2(2^9+2^4) + 2(2^7+2^2) + 2(2^5+2^{10}) + 2(2^3+2^8) + 2(2^1+2^6) + 1\right)}$$
$$+ 2^{2^1 + 2^2\left(2(2^9+2^2) + 2(2^7+2^{10}) + 2(2^5+2^8) + 2(2^3+2^6) + 2(2^1+2^4) + 1\right)}.$$

4.4 $|G| = 6$

Symmetry group Δ_3. We begin as usual with the list of objects.

	e	g_1	g_2	g_3	g_4	g_5
g_1						
g_2						
g_3						
g_4						
g_5						

We know we will have at least one element of order equal to the smallest prime divisor of 6. There is at least one object of order 2. Since 3 is a prime divisor of 6, we also know our group has at least one object of order 3. In fact, there has to be a multiple of $\phi(3) = 2$ many objects of order 3. Therefore, we can consider groups of six objects with two, or four, objects of order 3. First, consider the case with two objects of order 3, and three objects of order 2. We can suppose, without loss of generality, $g_1^2 = g_2$ and $g_1 * g_2 = e$.

	e	g_1	g_2	g_3	g_4	g_5
g_1	g_2	e				
g_2	e	g_1				
g_3			e			
g_4				e		
g_5					e	

Then $g_1 * g_3$ is a new object g_4, and the column of g_1 is determined. Then we find the column of g_2 by means of the composition $*g_1 \circ *g_1$.

	e	g_1	g_2	g_3	g_4	g_5
g_1	g_2	e				
g_2	e	g_1				
g_3	g_4	g_5	e			
g_4	g_5	g_3		e		
g_5	g_3	g_4			e	

Then, we use $|g_3| = 2$ to find

	e	g_1	g_2	g_3	g_4	g_5
g_1	g_2	e				
g_2	e	g_1				
g_3	g_4	g_5	e			
g_4	g_5	g_3	g_2			
g_5	g_3	g_4	g_1			

Again, we use $|g_3| = 2$, now to find

	e	g_1	g_2	g_3	g_4	g_5
g_1	g_2	e	g_5			
g_2	e	g_1	g_4			
g_3	g_4	g_5	e			
g_4	g_5	g_3	g_2			
g_5	g_3	g_4	g_1			

It is trivial to find the columns of g_4, g_5 in terms of the rest of the columns, using associativity as usual.

$$
\begin{array}{cccccc}
e & g_1 & g_2 & g_3 & g_4 & g_5 \\
g_1 & g_2 & e & g_5 & g_3 & g_4 \\
g_2 & e & g_1 & g_4 & g_5 & g_3 \\
g_3 & g_4 & g_5 & e & g_1 & g_2 \\
g_4 & g_5 & g_3 & g_2 & e & g_1 \\
g_5 & g_3 & g_4 & g_1 & g_2 & e
\end{array}
\tag{12}
$$

This is the symmetry group Δ_3. It is determined by the equations

$$
g_1^2 = g_2
$$
$$
g_1 * g_2 = g_3^2 = g_4^2 = g_5^2 = e.
$$

We will use letters $a, b, c, \ldots$ and $x_1, x_2, x_3, \ldots$ as auxiliary variables in finding our canonical naming. We know we have to start with $e = 5$. Recall we are trying to assign the larger numbers by giving priority to the left-most columns. Within a column we are giving priority to the objects of upper rows. Our first observation is that we have three objects of second order. One of these three objects, call it a, will be assigned the value 4. Then, whatever object we may choose for b, we have a fourth object $a * b = x_1$. And, since $|a| = 2$ we also have $a * x_1 = b$.

$$
\begin{array}{cccc}
e & a & b & x_1 \\
a & e & & \\
b & x_1 & & \\
x_1 & b & &
\end{array}
$$

In order to maximize our representation we name $b = 3$ and $a * b = x_1 = 2$. That way, we have the numeric table

$$
\begin{array}{cccc}
5 & 4 & 3 & 2 \\
4 & 5 & & \\
3 & 2 & & \\
2 & 3 & &
\end{array}
$$

So far, the only thing we know about the canonical naming functions, is that $a = 4$ is one of the second order objects. We know, from (12), that there is no x_1 that commutes with a. That is to say, the second order objects of Δ_3 do not commute with any non trivial object. Therefore, we need new objects $c = b * a$ and $x_2 = a * c$,

$$
\begin{array}{cccccc}
e & a & b & x_1 & c & x_2 \\
a & e & c & & & \\
b & x_1 & & & & \\
x_1 & b & & & & \\
c & x_2 & & & & \\
x_2 & c & & & &
\end{array}
$$

If we make $|b| = 2$, we maximize our representation. Now we know a canonical naming function must have $a = 4$ and $b = 3$ for two second order objects a, b. We also have to make $c = 1$ and $x_2 = 0$ if we wish to maximize the representation. Then we use the fact that $|b| = 2$ to find the rest of the column of b. The rest of the table is determined using associativity.

$$
\begin{array}{cccccc}
5 & 4 & 3 & 2 & 1 & 0 \\
4 & 5 & 1 & 0 & 3 & 2 \\
3 & 2 & 5 & 4 & 0 & 1 \\
2 & 3 & 0 & 1 & 5 & 4 \\
1 & 0 & 4 & 5 & 2 & 3 \\
0 & 1 & 2 & 3 & 4 & 5
\end{array}
$$

To obtain a canonical naming function make $a = 4$, $b = 3$ for two objects of order 2. Obviously, g_3, g_4, g_5 are equivalent objects; two of these have to be chosen to take the values of 4 and 3. This implies g_3, g_4, g_5 are equivalent. The object $a * b$ is assigned the value $x_1 = 2$. Then $b * a = c = 1$ and $a * c = x_2 = 0$. The objects g_2, g_3 are equivalent. We have a total of six possible canonical naming functions.

$$
\begin{array}{ccc}
(e, g_3, g_4, g_2, g_1, g_5) & (e, g_4, g_3, g_1, g_2, g_5) & (e, g_5, g_3, g_2, g_1, g_4) \\
(e, g_3, g_5, g_1, g_2, g_4) & (e, g_4, g_5, g_2, g_1, g_3) & (e, g_5, g_4, g_1, g_2, g_3)
\end{array}
$$

The group has a total of six automorphisms, given by the six canonical naming functions. We have block form, but the blocks are not cosets of a normal subgroup (even though Δ_6 has a normal subgroup). We have a table of four 3×3 blocks, and there are two types of blocks. The first type of block has objects in $A = \{1, 2, 3, 4, 5\}$ while the second type of block has objects in $B = \{0, 1, 2, 3, 4\}$. We have blocks A_1 and A_2 in the upper left corner and lower right corner, respectively. We have blocks B_1 and B_2 in the upper right hand and lower left hand, respectively. In this case, we have a normal subgroup, but it is not apparent in the canonical naming table. The normal subgroup is $N = \{e = 5, g_2 = 2, g_3 = 1\}$. We can write the canonical table in such a manner

that N will be trivially seen. The only thing that we have to do is change the rows and columns, appropriately. This group has canonical representation

$$
\begin{aligned}
N_{\Delta_3} = 2^{2^{11}+2^2\left(2^{(2^{11}+2^{12})}+2^{(2^9+2^{10})}+2^{(2^7+2^8)}+2^{(2^5+2^6)}+2^{(2^3+2^4)}+2^{(2^1+2^2)}+1\right)} &+ 2^{2^9+2^2\left(2^{(2^{11}+2^{10})}+2^{(2^9+2^{12})}+2^{(2^7+2^6)}+2^{(2^5+2^8)}+2^{(2^3+2^2)}+2^{(2^1+2^4)}+1\right)} \\
+ 2^{2^7+2^2\left(2^{(2^{11}+2^8)}+2^{(2^9+2^4)}+2^{(2^7+2^{12})}+2^{(2^5+2^2)}+2^{(2^3+2^{10})}+2^{(2^1+2^6)}+1\right)} &+ 2^{2^5+2^2\left(2^{(2^{11}+2^6)}+2^{(2^9+2^2)}+2^{(2^7+2^{10})}+2^{(2^5+2^4)}+2^{(2^3+2^{12})}+2^{(2^1+2^8)}+1\right)} \\
+ 2^{2^3+2^2\left(2^{(2^{11}+2^4)}+2^{(2^9+2^8)}+2^{(2^7+2^2)}+2^{(2^5+2^{12})}+2^{(2^3+2^6)}+2^{(2^1+2^{10})}+1\right)} &+ 2^{2^1+2^2\left(2^{(2^{11}+2^2)}+2^{(2^9+2^6)}+2^{(2^7+2^4)}+2^{(2^5+2^{10})}+2^{(2^3+2^8)}+2^{(2^1+2^{12})}+1\right)} .
\end{aligned}
$$

Cyclic Group $\mathbb{Z}_6$. Now we consider the case with four objects of order 4, and one object of order 2. We begin with

	e	g_1	g_2	g_3	g_4	g_5
g_1	e					
g_2		g_3	e			
g_3			e	g_2		
g_4						
g_5						

We make $g_1 * g_2 = g_4$, without loss of generality,

	e	g_1	g_2	g_3	g_4	g_5
g_1	e					
g_2	g_4	g_3	e			
g_3	g_5	e	g_2			
g_4						
g_5						

Using $|g_1| = 2$, we have

	e	g_1	g_2	g_3	g_4	g_5
g_1	e					
g_2	g_4	g_3	e			
g_3	g_5	e	g_2			
g_4	g_2					
g_5	g_3					

Now use $|g_2| = |g_3| = 3$ to find

	e	g_1	g_2	g_3	g_4	g_5
g_1	e					
g_2	g_4	g_3	e	g_5	g_1	
g_3	g_5	e	g_2	g_1	g_4	
g_4	g_2					
g_5	g_3					

We are considering $|g_4| = |g_5| \neq 2$, so that our only option is $g_4^2 = g_3$ and $g_5^2 = g_2$.

	e	g_1	g_2	g_3	g_4	g_5
g_1	e					
g_2	g_4	g_3	e	g_5	g_1	
g_3	g_5	e	g_2	g_1	g_4	
g_4	g_2				g_3	
g_5	g_3					g_2

However, it is easy to see that $|g_4| = |g_5| = 6$. We conclude there is no group $|G| = 4$ with four objects of order 2. The table is determined and we obtain the cyclic group.

	e	g_1	g_2	g_3	g_4	g_5
g_1	e	g_4	g_5	g_2	g_3	
g_2	g_4	g_3	e	g_5	g_1	
g_3	g_5	e	g_2	g_1	g_4	
g_4	g_2	g_5	g_1	g_3	e	
g_5	g_3	g_1	g_4	e	g_2	

(13)

The cyclic group $\mathbb{Z}_6$ is determined by $|G| = 6$ and

$$g_1^2 = e$$
$$g_2^2 = g_3^2 = g_4$$
$$g_1 * g_2 = g_3$$
$$g_4^2 = g_2.$$

Let us find the canonical naming functions; we use $a, b, c, \ldots$ and $x_1, x_2, x_3, \ldots$ as auxiliary variables. Start naming $e = 5$. There is only one second order object, so $g_1 = a = 4$. Add an object $b \neq g_1$. Whatever object we may choose for b, we have another object $a * b = x_1$. The group is commutative, so we also have $b * a = x_1$. Since $|a| = 2$, we have $a * x_1 = b$. Commutativity gives us $x_1 * a = b$.

$$
\begin{array}{cccc}
e & a & b & x_1 \\
a & e & x_1 & b \\
b & x_1 & & \\
x_1 & b & &
\end{array}
$$

In order to maximize our representation we name $b = 3$ and $a * b = x_1 = 2$. But, we still do not know what object of the group will be assigned to $b = 3$.

The possible naming functions we have are

$$
\begin{array}{llll}
(e, g_1, g_2, g_4, g_3, g_5) & (e, g_1, g_3, g_5, g_2, g_4) & (e, g_1, g_4, g_2, g_3, g_5) & (e, g_1, g_5, g_3, g_2, g_4) \\
(e, g_1, g_2, g_4, g_5, g_3) & (e, g_1, g_3, g_5, g_4, g_2) & (e, g_1, g_4, g_2, g_5, g_3) & (e, g_1, g_5, g_3, g_4, g_2)
\end{array}
$$

Whatever object b may be, we know b^2 is a new object c. Then, the operation $a * c$ is a new object x_2. Consequently, we find $b * x_1 = x_1 * b = x_2$ and $x_1^2 = c$. To maximize our representation we have to make $c = 1$ and $x_2 = 0$.

$$
\begin{array}{cccccc}
e & a & b & x_1 & c & x_2 \\
a & e & x_1 & b & x_2 & c \\
b & x_1 & c & x_2 & & \\
x_1 & b & x_2 & c & & \\
c & x_2 & & & & \\
x_2 & c & & & &
\end{array}
$$

We can eliminate some naming functions. We only keep those such that the square of the third component is equal to the fifth component ($b^2 = c$). Notice, only the objects g_2, g_3 are the square of some other object. The naming functions that satisfy these conditions are reduced to four.

$$
\begin{array}{l}
(e, g_1, g_2, g_4, g_3, g_5) \\
(e, g_1, g_3, g_5, g_2, g_4) \\
(e, g_1, g_4, g_2, g_3, g_5) \\
(e, g_1, g_5, g_3, g_2, g_4)
\end{array}
$$

Any of the naming functions above, gives the table below.

$$
\begin{array}{cccccc}
e & a & b & x_1 & c & x_2 \\
a & e & x_1 & b & x_2 & c \\
b & x_1 & c & x_2 & & \\
x_1 & b & x_2 & c & & \\
c & x_2 & & & & \\
x_2 & c & & & &
\end{array}
$$

We can not find more operations with the information we have. We have to choose choose b, c so that $b * c = e$ or $b * c = a$. Choosing them so $b * c = e$ maximizes our representation. The four candidate naming functions above satisfy this condition, so we have not reduced the candidate naming functions. However, we have the table

$$
\begin{array}{cccccc}
e & a & b & x_1 & c & x_2 \\
a & e & x_1 & b & x_2 & c \\
b & x_1 & c & x_2 & e & a \\
x_1 & b & x_2 & c & a & e \\
c & x_2 & e & a & & \\
x_2 & c & a & e & &
\end{array}
$$

Now, we have to focus on c^2. Notice that two of our four naming functions satisfy $c^2 = x_1$. The other two naming functions satisfy $c^2 = b$. The latter two maximize the representation. Our two canonical naming functions are $(e, g_1, g_2, g_4, g_3, g_5)$ and $(e, g_1, g_3, g_5, g_2, g_4)$. The cyclic group $\mathbb{Z}_6$ has a total of two automorphisms.

Take $A = (e, g_1, g_3, g_5, g_2, g_4)$. The non trivial automorphism is the function ϕ with components $e \mapsto e$, $g_1 \mapsto g_1$, $g_2 \mapsto g_3$, $g_3 \mapsto g_2$, $g_4 \mapsto g_5$, $g_5 \mapsto g_4$. If we take $A = (e, g_1, g_2, g_4, g_3, g_5)$ and $B = (e, g_1, g_3, g_5, g_2, g_4)$, we get the same non trivial automorphism ϕ. The numeric table obtained by these naming functions is

$$
\begin{array}{cccccc}
5 & 4 & 3 & 2 & 1 & 0 \\
4 & 5 & 2 & 3 & 0 & 1 \\
3 & 2 & 1 & 0 & 5 & 4 \\
2 & 3 & 0 & 1 & 4 & 5 \\
1 & 0 & 5 & 4 & 3 & 2 \\
0 & 1 & 4 & 5 & 2 & 3
\end{array}
$$

The 2×2 block on the upper left hand corner is the normal subgroup $N = \mathbb{Z}_2$. The table is made up of nine 2×2 blocks that are the cosets N, bN and b^2N, for $b \in \{g_2, g_3\}$. These coset blocks form the group $\mathbb{Z}_3$. The canonical table above is written as

$$
\begin{array}{ccc}
N & bN & b^2N \\
bN & b^2N & N \\
b^2N & N & bN
\end{array}
$$

The canonical naming table gives us the additional information that $\mathbb{Z}_6/\mathbb{Z}_2 = \mathbb{Z}_3$. These canonical representation of the cyclic group is

$$
\begin{aligned}
N_{\mathbb{Z}_6} = {} & 2^{2^{11}+2^2\left(2^{(2^{11}+2^{12})}+2^{(2^9+2^{10})}+2^{(2^7+2^8)}+2^{(2^5+2^6)}+2^{(2^3+2^4)}+2^{(2^1+2^2)}+1\right)} + 2^{2^9+2^2\left(2^{(2^{11}+2^{10})}+2^{(2^9+2^{12})}+2^{(2^7+2^6)}+2^{(2^5+2^8)}+2^{(2^3+2^2)}+2^{(2^1+2^4)}+1\right)} \\
& + 2^{2^7+2^2\left(2^{(2^{11}+2^8)}+2^{(2^9+2^6)}+2^{(2^7+2^4)}+2^{(2^5+2^2)}+2^{(2^3+2^{12})}+2^{(2^1+2^{10})}+1\right)} + 2^{2^5+2^2\left(2^{(2^{11}+2^6)}+2^{(2^9+2^8)}+2^{(2^7+2^2)}+2^{(2^5+2^4)}+2^{(2^3+2^{10})}+2^{(2^1+2^{12})}+1\right)} \\
& + 2^{2^3+2^2\left(2^{(2^{11}+2^4)}+2^{(2^9+2^2)}+2^{(2^7+2^{12})}+2^{(2^5+2^{10})}+2^{(2^3+2^8)}+2^{(2^1+2^6)}+1\right)} + 2^{2^1+2^2\left(2^{(2^{11}+2^2)}+2^{(2^9+2^4)}+2^{(2^7+2^{10})}+2^{(2^5+2^{12})}+2^{(2^3+2^6)}+2^{(2^1+2^8)}+1\right)} .
\end{aligned}
$$

Up to this point, we have not had any difficulty in finding the canonical naming and representation of the smaller groups. So far we know that the first groups are ordered

$$
\begin{aligned}
G_0 &= \mathbb{Z}_1 \\
G_1 &= \mathbb{Z}_2 \\
G_2 &= \mathbb{Z}_3 \\
G_3 &= \mathbb{Z}_4 \\
G_4 &= K(4) \\
G_5 &= \mathbb{Z}_5 \\
G_6 &= \mathbb{Z}_6 \\
G_7 &= \Delta_3
\end{aligned}
$$

The first step in finding the canonical naming function is to identify the objects of smallest order. By now we know how to find the canonical table and representation of $\mathbb{Z}_7$ (see $\mathbb{Z}_5$). This is the next group in order, $G_8 = \mathbb{Z}_7$.

4.5 $|G| = 8$

Let us find groups of eight objects. We know The possible orders of the objects are the divisors of 8. Particularly, we have at least one object of order 2, we can have $2i$ objects of order 4 and we can have $4j$ objects of order 8. We will find all groups of eight objects. We will provide each group found with a canonical naming function given in the numeric table, the minimal independent set of equations that defines the group, and the canonical representation. Then, we will compare the canonical representations of these groups to find $G_9 < G_{10} < G_{11} < G_{12} < G_{13}$.

Direct Product $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Let us take the simplest case first, and then it will be clear how we can complicate things little by little, so that we find all possible groups of order 8. The simplest case is to consider all objects of order 2 (we make $i = j = 0$). Additionally, we will suppose they all commute.

$$
\begin{array}{cccccccc}
e & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 \\
g_1 & e & g_3 & g_2 & g_5 & g_4 & g_7 & g_6 \\
g_2 & g_3 & e & & & & & \\
g_3 & g_2 & & e & & & & \\
g_4 & g_5 & & & e & & & \\
g_5 & g_4 & & & & e & & \\
g_6 & g_7 & & & & & e & \\
g_7 & g_6 & & & & & & e
\end{array}
$$

We can easily find

$$
\begin{array}{cccccccc}
e & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 \\
g_1 & e & g_3 & g_2 & g_5 & g_4 & g_7 & g_6 \\
g_2 & g_3 & e & g_1 & & & & \\
g_3 & g_2 & g_1 & e & & & & \\
g_4 & g_5 & & & e & g_1 & & \\
g_5 & g_4 & & & g_1 & e & & \\
g_6 & g_7 & & & & & e & g_1 \\
g_7 & g_6 & & & & & g_1 & e
\end{array}
$$

We know $g_2 * g_4 \notin \{e, g_1, g_2, g_3, g_4, g_5\}$. Suppose without loss of generality, $g_2 * g_4 = g_6$. This determines the rest of the column of g_2. Then we use $g_2 * g_4 = g_4 * g_2$ and $g_2 * g_6 = g_6 * g_2$ to find the third row. Now we can find the fourth column and fourth row using the associative property. For example, we use $g_6 * g_2 = g_4$ to find $g_4 * g_3 = g_6 * (g_2 * g_3) = g_6 * g_1 = g_7$. Finally, we use $g_3 * g_5 = g_6$ to find $g_6 * g_4 = g_3 * (g_5 * g_4) = g_3 * g_1 = g_2$.

$$
\begin{array}{cccccccc}
e & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 \\
g_1 & e & g_3 & g_2 & g_5 & g_4 & g_7 & g_6 \\
g_2 & g_3 & e & g_1 & g_6 & g_7 & g_4 & g_5 \\
g_3 & g_2 & g_1 & e & g_7 & g_6 & g_5 & g_4 \\
g_4 & g_5 & g_6 & g_7 & e & g_1 & g_2 & g_3 \\
g_5 & g_4 & g_7 & g_6 & g_1 & e & g_3 & g_2 \\
g_6 & g_7 & g_4 & g_5 & g_2 & g_3 & e & g_1 \\
g_7 & g_6 & g_5 & g_4 & g_3 & g_2 & g_1 & e
\end{array}
\tag{14}
$$

This determines the group $\mathbb{Z}_2^3 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Again, we have the special block form of cosets of $N = \mathbb{Z}_2$. The expression $\mathbb{Z}_8 / N = \mathbb{Z}_4$ is given in the table, because we have sixteen 2×2 blocks, $N, g_2 N, g_4 N, g_6 N$, forming $\mathbb{Z}_4$.

$$
\begin{array}{cccc}
N & g_2 N & g_4 N & g_6 N \\
g_2 N & N & g_6 N & g_4 N \\
g_4 N & g_6 N & N & g_2 N \\
g_6 N & g_4 N & g_2 N & N
\end{array}
$$

This coset table, is itself an expression of quotient groups. It expresses $\mathbb{Z}_4 / \mathbb{Z}_2 = \mathbb{Z}_2$. We have a third expression of group quotients, going back to table (14). It simultaneously shows $\mathbb{Z}_8 / \mathbb{Z}_4 = \mathbb{Z}_2$ because we have four 4×4 blocks forming $\mathbb{Z}_2$; these blocks are the cosets of $N_3 = \mathbb{Z}_4$,

$$
\begin{array}{cc}
N_3 & c N_3 \\
c N_3 & N_3
\end{array}
$$

To define this group we need seven objects of order 2. We also need an object g_1 that commute with the rest of the objects.

$$
e = g_1^2 = g_2^2 = g_3^2 = g_4^2 = g_5^2 = g_6^2 = g_7^2
$$
$$
g_1 * g = g * g_1, \qquad\qquad\qquad\qquad g \in \mathbb{Z}_2^3.
$$

Let us find the one hundred and sixty eight distinct automorphisms of $\mathbb{Z}_2^3$. We must find the canonical naming functions. Given that all of the objects commute, and they are all second order objects, we know they are all equivalent. This means we make $e = 7$, and $a = 6$ for an arbitrary object of the group. Then, we assign value to another arbitrary object $b = 5$, and $x_1 = 4$.

$$
\begin{array}{cccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b & x_2 & c & x_3 & d \\
b & x_1 & e & a & & & & \\
x_1 & b & a & e & & & & \\
c & x_2 & & & e & a & & \\
x_2 & c & & & a & e & & \\
d & x_3 & & & & & e & a \\
x_3 & d & & & & & a & e
\end{array}
$$

Now we choose a third object to assign to $c = 3$, and $a * c = x_2 = 2$. Finally, we make $b * c = d = 1$ and $a * d = x_3 = 0$. This determines the rest of the table. The first object, a, is chosen from seven different possible choices. The object b is chosen from a total of six options. Finally, we choose c from a total of four different options. The numeric table, given by these canonical naming functions is

$$
\begin{array}{cccccccc}
7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\
6 & 7 & 4 & 5 & 2 & 3 & 0 & 1 \\
5 & 4 & 7 & 6 & 1 & 0 & 3 & 2 \\
4 & 5 & 6 & 7 & 0 & 1 & 2 & 3 \\
3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 \\
2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 \\
1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7
\end{array}
$$

and the canonical representation is

$$N_{\mathbb{Z}_2^3} = 2^{2^{15}+2^2\left(2^{(2^{15}+2^{16})}+2^{(2^{13}+2^{14})}+2^{(2^{11}+2^{12})}+2^{(2^9+2^{10})}+2^{(2^7+2^8)}+2^{(2^5+2^6)}+2^{(2^3+2^4)}+2^{(2^1+2^2)}+1\right)}$$

$$+ 2^{2^{13}+2^2\left(2^{(2^{15}+2^{14})}+2^{(2^{13}+2^{16})}+2^{(2^{11}+2^{10})}+2^{(2^9+2^{12})}+2^{(2^7+2^6)}+2^{(2^5+2^8)}+2^{(2^3+2^2)}+2^{(2^1+2^4)}+1\right)}$$

$$+ 2^{2^{11}+2^2\left(2^{(2^{15}+2^{12})}+2^{(2^{13}+2^{10})}+2^{(2^{11}+2^{16})}+2^{(2^9+2^{14})}+2^{(2^7+2^4)}+2^{(2^5+2^2)}+2^{(2^3+2^8)}+2^{(2^1+2^6)}+1\right)}$$

$$+ 2^{2^9+2^2\left(2^{(2^{15}+2^{10})}+2^{(2^{13}+2^{12})}+2^{(2^{11}+2^{14})}+2^{(2^9+2^{16})}+2^{(2^7+2^2)}+2^{(2^5+2^4)}+2^{(2^3+2^6)}+2^{(2^1+2^8)}+1\right)}$$

$$+ 2^{2^7+2^2\left(2^{(2^{15}+2^8)}+2^{(2^{13}+2^6)}+2^{(2^{11}+2^4)}+2^{(2^9+2^2)}+2^{(2^7+2^{16})}+2^{(2^5+2^{14})}+2^{(2^3+2^{12})}+2^{(2^1+2^{10})}+1\right)}$$

$$+ 2^{2^5+2^2\left(2^{(2^{15}+2^6)}+2^{(2^{13}+2^8)}+2^{(2^{11}+2^2)}+2^{(2^9+2^4)}+2^{(2^7+2^{14})}+2^{(2^5+2^{16})}+2^{(2^3+2^{10})}+2^{(2^1+2^{12})}+1\right)}$$

$$+ 2^{2^3+2^2\left(2^{(2^{15}+2^4)}+2^{(2^{13}+2^2)}+2^{(2^{11}+2^8)}+2^{(2^9+2^6)}+2^{(2^7+2^{12})}+2^{(2^5+2^{10})}+2^{(2^3+2^{16})}+2^{(2^1+2^{14})}+1\right)}$$

$$+ 2^{2^1+2^2\left(2^{(2^{15}+2^2)}+2^{(2^{13}+2^4)}+2^{(2^{11}+2^6)}+2^{(2^9+2^8)}+2^{(2^7+2^{10})}+2^{(2^5+2^{12})}+2^{(2^3+2^{14})}+2^{(2^1+2^{16})}+1\right)}$$

Now we will look for groups with all objects of order 2, and $a*c \neq c*a$. We can take $c*a = d$. This implies $d*a = c$ because $|a| = 2$. Since $|d| = 2$ we also have $d*c = a$. Also, $a*c = x_2$ and $|c| = 2$ imply $x_2*c = a$. This is a contradiction.

$$
\begin{array}{cccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b & d & x_3 & c & x_2 \\
b & x_1 & e & a & & & & \\
x_1 & b & a & e & & & & \\
c & x_2 & & & e & a & a & \\
x_2 & c & & & & e & & \\
d & x_3 & & & & & e & \\
x_3 & d & & & & & & e \\
\end{array}
$$

The contradiction does not depend on the first four objects e, a, b, x_1. This means that any non abelian group of eight objects, must also have objects of order 4 or 8. In particular, the group $\mathbb{Z}_2^3$, above, is the only group of eight objects with all non trivial elements of order 2.

Dihedral Group D_8. Now we seek for G with objects of order 4. We must have a multiple of $2 = \phi(4)$, many objects of order 4. We first consider the case with two objects of order 4, and five objects of second order. Let a, b, x_1, c, x_2 be the objects of order 2, and let d, x_3 our objects of order 4. We have the form

$$
\begin{array}{cccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & & & & & & \\
b & x_1 & e & & & & & \\
x_1 & b & & e & & & & \\
c & x_2 & & & e & & & \\
x_2 & c & & & & e & & \\
d & x_3 & & & & & a & e \\
x_3 & d & & & & & e & a \\
\end{array}
$$

Since $|b| = |x_1| = |c| = |x_2| = 2$, we have $x_1*b = b*x_1 = x_2*c = c*x_2 = a$, respectively.

$$
\begin{array}{cccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & & & & & & \\
b & x_1 & e & a & & & & \\
x_1 & b & a & e & & & & \\
c & x_2 & & & e & a & & \\
x_2 & c & & & a & e & & \\
d & x_3 & & & & & a & e \\
x_3 & d & & & & & e & a \\
\end{array}
$$

Now, $|b| = |x_1| = |c| = |x_2| = 2$ implies $b*a = x_1$, $x_1*a = b$, $c*a = x_2$, $x_2*a = c$, respectively. Then, $d*a = x_3$ and $x_3*a = d$. Notice we are starting to see a block form of the table for $K(4)$. We have 2×2 blocks forming the Klein group. The blocks of d, x_3 have not yet interfered with the rest of the blocks. We can suppose $b*c = d$, without loss of generality,

$$
\begin{array}{cccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b & x_2 & c & x_3 & d \\
b & x_1 & e & a \\
x_1 & b & a & e \\
c & x_2 & d & x_3 & e & a \\
x_2 & c & x_3 & d & a & e \\
d & x_3 & & & a & e \\
x_3 & d & & & e & a
\end{array}
$$

The rest of the table is determined. Find $b*d = c$, and $d*c = b$.

$$
\begin{array}{cccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b & x_2 & c & x_3 & d \\
b & x_1 & e & a \\
x_1 & b & a & e \\
c & x_2 & d & x_3 & e & a & b & x_1 \\
x_2 & c & x_3 & d & a & e & x_1 & b \\
d & x_3 & c & x_2 & & & a & e \\
x_3 & d & x_2 & c & & & e & a
\end{array}
$$

Now we can use $c = b*d$ to find $c*d = b*(d*d) = b*a = x_1$.

$$
\begin{array}{cccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b & x_2 & c & x_3 & d \\
b & x_1 & e & a \\
x_1 & b & a & e \\
c & x_2 & d & x_3 & e & a & b & x_1 \\
x_2 & c & x_3 & d & a & e & x_1 & b \\
d & x_3 & c & x_2 & x_1 & b & a & e \\
x_3 & d & x_2 & c & b & x_1 & e & a
\end{array}
$$

The rest of the table is determined similarly. For example, $|c| = 2$ implies $c*b = x_3$.

$$
\begin{array}{cccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b & x_2 & c & x_3 & d \\
b & x_1 & e & a & x_3 & d & c & x_2 \\
x_1 & b & a & e & d & x_3 & x_2 & c \\
c & x_2 & d & x_3 & e & a & b & x_1 \\
x_2 & c & x_3 & d & a & e & x_1 & b \\
d & x_3 & c & x_2 & x_1 & b & a & e \\
x_3 & d & x_2 & c & b & x_1 & e & a
\end{array}
$$

This is the Dihedral group, D_8, defined by $|G| = 8$ and the set of equations

$$
e = a^2 = b^2 = x_1^2 = c^2 = x_2^2
$$
$$
(b*c)^2 = a.
$$

It is the only group $|G| = 8$, with exactly two objects of order 4, and five objects of order 2. Notice that the set of equations only mentions seven different objects. The eighth object is $a*(b*c)$, and it is also of order 4, just as $b*c$. Now we will find the canonical naming function of this group. We write the group with generic symbols.

$$
\begin{array}{cccccccc}
e & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 \\
g_1 & e & g_3 & g_2 & g_5 & g_4 & g_7 & g_6 \\
g_2 & g_3 & g_1 & e & g_7 & g_6 & g_4 & g_5 \\
g_3 & g_2 & e & g_1 & g_6 & g_7 & g_5 & g_4 \\
g_4 & g_5 & g_6 & g_7 & e & g_1 & g_2 & g_3 \\
g_5 & g_4 & g_7 & g_6 & g_1 & e & g_3 & g_2 \\
g_6 & g_7 & g_5 & g_4 & g_3 & g_2 & e & g_1 \\
g_7 & g_6 & g_4 & g_5 & g_2 & g_3 & g_1 & e
\end{array}
\tag{15}
$$

Now we will use the letters $a, b, \ldots, x_1, x_2, \ldots$ as auxiliary variables to find the canonical naming. We want to avoid confusion with the fact that we just used the same symbols $a, b, \ldots, x_1, x_2, \ldots$ as auxiliary variables to find the group. Table (15) will be the reference for D_8. We start with $e = 7$, and an arbitrary object, $a = 6$, of order 2. We add an object $b = 5$, and if we want to maximize we have to make $x_1 = a*b = 4$.

$$
\begin{array}{llll}
e & a & b & x_1 \\
a & e & & \\
b & x_1 & & \\
x_1 & b & &
\end{array}
$$

We simply need two objects a, b that satisfy $e = a^2$ and $a * b = b * a$. There are many options of ordered pairs of D_8 that satisfy this. For example, g_7 is a second order object and it commutes with g_6. Also, g_1 is a second order object and it commutes with g_2. We have a total of ten options to do this.

$$
\begin{array}{llll}
e & a & b & x_1 \\
a & e & x_1 & b \\
b & x_1 & & \\
x_1 & b & &
\end{array}
$$

We can find b such that $|b| = 2$, maximizing the representation. Finding two objects of order 2 that commute, gives us the partial table below.

$$
\begin{array}{llll}
e & a & b & x_1 \\
a & e & x_1 & b \\
b & x_1 & e & a \\
x_1 & b & a & e
\end{array}
$$

We have six options to do this. The objects g_4, g_5 commute, as do g_6, g_7 and they are all second order objects. Also, g_1 commutes with each of them. Therefore, any of these objects can take the place of a, for now. Add another object to the table, say $c = 3$, and consequently $x_2 = a * c = 2$. Then, we need to add another object $d = 1$, for the product $b * c = d$. Finally we have $x_3 = a * d = 0$.

$$
\begin{array}{lllllll}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b & & & & \\
b & x_1 & e & a & & & & \\
x_1 & b & a & e & & & & \\
c & x_2 & d & x_3 & & & & \\
x_2 & c & x_3 & d & & & & \\
d & x_3 & c & x_2 & & & & \\
x_3 & d & x_2 & c & & & &
\end{array}
$$

If we wish to maximize the representation, we will have to find c that commutes with a. This implies a also commutes with $a * c$. The only object that commutes with four objects, of order 2, is g_1. This means $a = g_1$. We have reduced the possible canonical naming functions, that give the table below, to a total of sixteen possible naming functions. We choose b from four different objects and c can also be chosen from four different objects.

$$
\begin{array}{llllllll}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b & x_2 & c & x_3 & d \\
b & x_1 & e & a & & & & \\
x_1 & b & a & e & & & & \\
c & x_2 & d & x_3 & & & & \\
x_2 & c & x_3 & d & & & & \\
d & x_3 & c & x_2 & & & & \\
x_3 & d & x_2 & c & & & &
\end{array}
$$

None of our choices of naming functions will have $b * c = c * b$. This is because our four options of b are g_4, g_5, g_6, g_7. Each of these objects only commutes with g_1 and $a * b = x_1$. For example, g_4 commutes with $g_5 = g_1 * g_4$, etc. We have the table

$$
\begin{array}{llllllll}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b & x_2 & c & x_3 & d \\
b & x_1 & e & a & x_3 & d & & \\
x_1 & b & a & e & d & x_3 & & \\
c & x_2 & d & x_3 & & & & \\
x_2 & c & x_3 & d & & & & \\
d & x_3 & c & x_2 & & & & \\
x_3 & d & x_2 & c & & & &
\end{array}
$$

Notice that in eight of the sixteen possible naming functions, we have $c^2 = e$. The other eight functions are the ones that have c equal to g_2 or g_3. We wish to maximize the representation so we choose the first eight naming functions; assign c to a second order object.

$$
\begin{array}{cccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b & x_2 & c & x_3 & d \\
b & x_1 & e & a & x_3 & d & & \\
x_1 & b & a & e & d & x_3 & & \\
c & x_2 & d & x_3 & e & a & & \\
x_2 & c & x_3 & d & a & e & & \\
d & x_3 & & & & & & \\
x_3 & d & & & & & &
\end{array}
$$

The rest of the table is determined. We have a total of eight canonical naming functions. We can choose b from four different objects g_4, g_5, g_6, g_7, and make $x_1 = g_1 * b$. Then we can choose c from the remaining two objects of that list. The objects g_4, g_5 are equivalent, and g_6, g_7 are equivalent. The order 4 objects g_2, g_3 are equivalent. The canonical naming functions are

$$
\begin{array}{llll}
(e, g_1, g_4, g_5, g_6, g_7, g_3, g_2) & (e, g_1, g_5, g_4, g_6, g_7, g_2, g_3) & (e, g_1, g_6, g_7, g_4, g_5, g_2, g_3) & (e, g_1, g_7, g_6, g_4, g_5, g_3, g_2) \\
(e, g_1, g_4, g_5, g_7, g_6, g_2, g_3) & (e, g_1, g_5, g_4, g_7, g_6, g_3, g_2) & (e, g_1, g_6, g_7, g_5, g_4, g_3, g_2) & (e, g_1, g_7, g_6, g_5, g_4, g_2, g_3)
\end{array}
$$

The numeric table is

$$
\begin{array}{cccccccc}
7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\
6 & 7 & 4 & 5 & 2 & 3 & 0 & 1 \\
5 & 4 & 7 & 6 & 0 & 1 & 2 & 3 \\
4 & 5 & 6 & 7 & 1 & 0 & 3 & 2 \\
3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 \\
2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 \\
1 & 0 & 3 & 2 & 4 & 5 & 6 & 7 \\
0 & 1 & 2 & 3 & 5 & 4 & 7 & 6
\end{array}
$$

and the canonical representation is

$$
\begin{aligned}
N_{D_8} = {} & 2^{2^{15}+2^2\left(2^{(2^{15}+2^{16})}+2^{(2^{13}+2^{14})}+2^{(2^{11}+2^{12})}+2^{(2^9+2^{10})}+2^{(2^7+2^8)}+2^{(2^5+2^6)}+2^{(2^3+2^4)}+2^{(2^1+2^2)}+1\right)} \\
& + 2^{2^{13}+2^2\left(2^{(2^{15}+2^{14})}+2^{(2^{13}+2^{16})}+2^{(2^{11}+2^{10})}+2^{(2^9+2^{12})}+2^{(2^7+2^6)}+2^{(2^5+2^8)}+2^{(2^3+2^2)}+2^{(2^1+2^4)}+1\right)} \\
& + 2^{2^{11}+2^2\left(2^{(2^{15}+2^{12})}+2^{(2^{13}+2^{10})}+2^{(2^{11}+2^{16})}+2^{(2^9+2^{14})}+2^{(2^7+2^4)}+2^{(2^5+2^2)}+2^{(2^3+2^8)}+2^{(2^1+2^6)}+1\right)} \\
& + 2^{2^9+2^2\left(2^{(2^{15}+2^{10})}+2^{(2^{13}+2^{12})}+2^{(2^{11}+2^{14})}+2^{(2^9+2^{16})}+2^{(2^7+2^2)}+2^{(2^5+2^4)}+2^{(2^3+2^6)}+2^{(2^1+2^8)}+1\right)} \\
& + 2^{2^7+2^2\left(2^{(2^{15}+2^8)}+2^{(2^{13}+2^6)}+2^{(2^{11}+2^2)}+2^{(2^9+2^4)}+2^{(2^7+2^{16})}+2^{(2^5+2^{14})}+2^{(2^3+2^{10})}+2^{(2^1+2^{12})}+1\right)} \\
& + 2^{2^5+2^2\left(2^{(2^{15}+2^6)}+2^{(2^{13}+2^8)}+2^{(2^{11}+2^4)}+2^{(2^9+2^2)}+2^{(2^7+2^{14})}+2^{(2^5+2^{16})}+2^{(2^3+2^{12})}+2^{(2^1+2^{10})}+1\right)} \\
& + 2^{2^3+2^2\left(2^{(2^{15}+2^4)}+2^{(2^{13}+2^2)}+2^{(2^{11}+2^6)}+2^{(2^9+2^8)}+2^{(2^7+2^{12})}+2^{(2^5+2^{10})}+2^{(2^3+2^{14})}+2^{(2^1+2^{16})}+1\right)} \\
& + 2^{2^1+2^2\left(2^{(2^{15}+2^2)}+2^{(2^{13}+2^4)}+2^{(2^{11}+2^8)}+2^{(2^9+2^6)}+2^{(2^7+2^{10})}+2^{(2^5+2^{12})}+2^{(2^3+2^{16})}+2^{(2^1+2^{14})}+1\right)}
\end{aligned}
$$

Direct Product $\mathbb{Z}_2 \oplus \mathbb{Z}_4$**.** Now we will consider groups with four objects of order 4, and three objects of order 2. Let a any object of order 4. We know $a^2 = b$ is a new object, as is $a^3 = c$.

$$
\begin{array}{cccccccc}
e & a & x_1 & x_2 & b & x_3 & x_4 & x_5 \\
a & x_1 & & & & & & \\
x_1 & x_2 & & & & & & \\
x_2 & e & & & & & & \\
b & & & & & & & \\
x_3 & & & & & & & \\
x_4 & & & & & & & \\
x_5 & & & & & & &
\end{array}
$$

We can easily find operations for x_1 and then for x_2.

$$
\begin{array}{llllllll}
e & a & x_1 & x_2 & b & x_3 & x_4 & x_5 \\
a & x_1 & x_2 & e & & & & \\
x_1 & x_2 & e & a & & & & \\
x_2 & e & a & x_1 & & & & \\
b & & & & & & & \\
x_3 & & & & & & & \\
x_4 & & & & & & & \\
x_5 & & & & & & & \\
\end{array}
$$

The column of a can be completed defining $a*b = x_3$. Then we can complete the column of x_1 and x_2.

$$
\begin{array}{llllllll}
e & a & x_1 & x_2 & b & x_3 & x_4 & x_5 \\
a & x_1 & x_2 & e & & & & \\
x_1 & x_2 & e & a & & & & \\
x_2 & e & a & x_1 & & & & \\
b & x_3 & x_4 & x_5 & & & & \\
x_3 & x_4 & x_5 & b & & & & \\
x_4 & x_5 & b & x_3 & & & & \\
x_5 & b & x_3 & x_4 & & & & \\
\end{array}
$$

We can suppose $|b| = 2$, without loss of generality. This implies $x_3 * b = a$, $x_4 * b = x_1$ and $x_5 * b = x_2$.

$$
\begin{array}{llllllll}
e & a & x_1 & x_2 & b & x_3 & x_4 & x_5 \\
a & x_1 & x_2 & e & & & & \\
x_1 & x_2 & e & a & & & & \\
x_2 & e & a & x_1 & & & & \\
b & x_3 & x_4 & x_5 & e & a & x_1 & x_2 \\
x_3 & x_4 & x_5 & b & & & & \\
x_4 & x_5 & b & x_3 & & & & \\
x_5 & b & x_3 & x_4 & & & & \\
\end{array}
$$

Consider two different cases; b, x_3 commute or not. If we suppose they do not commute we come to a contradiction. It is a good exercise to see how we come to a contradiction in the least number of steps. Let us consider the commutative case. Then the table is determined.

$$
\begin{array}{llllllll}
e & a & x_1 & x_2 & b & x_3 & x_4 & x_5 \\
a & x_1 & x_2 & e & x_3 & x_4 & x_5 & b \\
x_1 & x_2 & e & a & x_4 & x_5 & b & x_3 \\
x_2 & e & a & x_1 & x_5 & b & x_3 & x_4 \\
b & x_3 & x_4 & x_5 & e & a & x_1 & x_2 \\
x_3 & x_4 & x_5 & b & a & x_1 & x_2 & e \\
x_4 & x_5 & b & x_3 & x_1 & x_2 & e & a \\
x_5 & b & x_3 & x_4 & x_2 & e & a & x_1 \\
\end{array}
$$

This is the direct product group $\mathbb{Z}_2 \oplus \mathbb{Z}_4$. To define our group, we need an object of order 4, given by the equations $a^2 = x_1$, $a*x_1 = x_2$, $a*x_2 = e$. Then we need a second order object, b, that commutes with $x_3 = a*b$. This is the system of equations

$$
\begin{aligned}
a^2 &= x_1 \\
a^3 &= x_2 \\
a*x_2 = b^2 &= e \\
a*b &= x_3 \\
b*x_3 &= x_3*b
\end{aligned}
$$

To find the canonical naming functions, we write the table in terms of g_i.

$$
\begin{array}{llllllll}
e & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 \\
g_1 & g_2 & g_3 & e & g_5 & g_6 & g_7 & g_4 \\
g_2 & g_3 & e & g_1 & g_6 & g_7 & g_4 & g_5 \\
g_3 & e & g_1 & g_2 & g_7 & g_4 & g_5 & g_6 \\
g_4 & g_5 & g_6 & g_7 & e & g_1 & g_2 & g_3 \\
g_5 & g_6 & g_7 & g_4 & g_1 & g_2 & g_3 & e \\
g_6 & g_7 & g_4 & g_5 & g_2 & g_3 & e & g_1 \\
g_7 & g_4 & g_5 & g_6 & g_3 & e & g_1 & g_2 \\
\end{array}
\tag{16}
$$

We begin by assigning $e = 7$, and $a = 6$ for some second order object a. Choose an arbitrary object $b = 5$, and make $a * b = x_1 = 4$. The group is commutative so $b * a = x_1$.

$$
\begin{array}{cccc}
e & a & b & x_1 \\
a & e & x_1 & b \\
b & x_1 & & \\
x_1 & b & &
\end{array}
$$

We choose b of second order. This gives us the table of $K(4)$. Add another arbitrary object $c = 3$, and $a * c = x_2 = 2$.

$$
\begin{array}{cccccc}
e & a & b & x_1 & c & x_2 \\
a & e & x_1 & b & x_2 & c \\
b & x_1 & e & a & & \\
x_1 & b & a & e & & \\
c & x_2 & & & & \\
x_2 & c & & & &
\end{array}
$$

We need to add another new object $b * c = c * b = d = 1$, and $x_3 = a * d = 0$.

$$
\begin{array}{cccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b & x_2 & c & x_3 & d \\
b & x_1 & e & a & d & x_3 & c & x_2 \\
x_1 & b & a & e & x_3 & d & x_2 & c \\
c & x_2 & d & x_3 & & & & \\
x_2 & c & x_3 & d & & & & \\
d & x_3 & c & x_2 & & & & \\
x_3 & d & x_2 & c & & & &
\end{array}
$$

If we wish to maximize the representation, we must choose a so that it is the square of some object; $c^2 = a$. Therefore, $g_2 = a = 7$. This determines the table. To find a canonical naming function we can choose b from two possible choices, g_4, g_6. Then we choose c from four possible choices, g_1, g_3, g_5, g_7. There is a total of eight canonical naming functions defining eight automorphisms of $\mathbb{Z}_2 \oplus \mathbb{Z}_4$.

$$
\begin{array}{llll}
(e, g_2, g_4, g_6, g_1, g_3, g_5, g_7) & (e, g_2, g_4, g_6, g_3, g_1, g_7, g_5) & (e, g_2, g_4, g_6, g_5, g_7, g_1, g_3) & (e, g_2, g_4, g_6, g_7, g_5, g_3, g_1) \\
(e, g_2, g_6, g_4, g_1, g_3, g_7, g_5) & (e, g_2, g_6, g_4, g_3, g_1, g_5, g_7) & (e, g_2, g_6, g_4, g_5, g_7, g_3, g_1) & (e, g_2, g_6, g_4, g_7, g_5, g_1, g_3)
\end{array}
$$

These naming functions give the numeric table

$$
\begin{array}{cccccccc}
7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\
6 & 7 & 4 & 5 & 2 & 3 & 0 & 1 \\
5 & 4 & 7 & 6 & 1 & 0 & 3 & 2 \\
4 & 5 & 6 & 7 & 0 & 1 & 2 & 3 \\
3 & 2 & 1 & 0 & 6 & 7 & 4 & 5 \\
2 & 3 & 0 & 1 & 7 & 6 & 5 & 4 \\
1 & 0 & 3 & 2 & 4 & 5 & 6 & 7 \\
0 & 1 & 2 & 3 & 5 & 4 & 7 & 6
\end{array}
$$

with canonical representation

$$
\begin{aligned}
N_{\mathbb{Z}_2 \oplus \mathbb{Z}_4} = \; & 2^{2^{15}+2^{2\left(2^{(2^{15}+2^{16})}+2^{(2^{13}+2^{14})}+2^{(2^{11}+2^{12})}+2^{(2^9+2^{10})}+2^{(2^7+2^8)}+2^{(2^5+2^6)}+2^{(2^3+2^4)}+2^{(2^1+2^2)}+1\right)}} \\
& + 2^{2^{13}+2^{2\left(2^{(2^{15}+2^{14})}+2^{(2^{13}+2^{16})}+2^{(2^{11}+2^{10})}+2^{(2^9+2^{12})}+2^{(2^7+2^6)}+2^{(2^5+2^8)}+2^{(2^3+2^2)}+2^{(2^1+2^4)}+1\right)}} \\
& + 2^{2^{11}+2^{2\left(2^{(2^{15}+2^{12})}+2^{(2^{13}+2^{10})}+2^{(2^{11}+2^{16})}+2^{(2^9+2^{14})}+2^{(2^7+2^4)}+2^{(2^5+2^2)}+2^{(2^3+2^8)}+2^{(2^1+2^6)}+1\right)}} \\
& + 2^{2^9+2^{2\left(2^{(2^{15}+2^{10})}+2^{(2^{13}+2^{12})}+2^{(2^{11}+2^{14})}+2^{(2^9+2^{16})}+2^{(2^7+2^2)}+2^{(2^5+2^4)}+2^{(2^3+2^6)}+2^{(2^1+2^8)}+1\right)}} \\
& + 2^{2^7+2^{2\left(2^{(2^{15}+2^8)}+2^{(2^{13}+2^6)}+2^{(2^{11}+2^4)}+2^{(2^9+2^2)}+2^{(2^7+2^{14})}+2^{(2^5+2^{16})}+2^{(2^3+2^{10})}+2^{(2^1+2^{12})}+1\right)}} \\
& + 2^{2^5+2^{2\left(2^{(2^{15}+2^6)}+2^{(2^{13}+2^8)}+2^{(2^{11}+2^2)}+2^{(2^9+2^4)}+2^{(2^7+2^{16})}+2^{(2^5+2^{14})}+2^{(2^3+2^{12})}+2^{(2^1+2^{10})}+1\right)}} \\
& + 2^{2^3+2^{2\left(2^{(2^{15}+2^4)}+2^{(2^{13}+2^2)}+2^{(2^{11}+2^8)}+2^{(2^9+2^6)}+2^{(2^7+2^{10})}+2^{(2^5+2^{12})}+2^{(2^3+2^{14})}+2^{(2^1+2^{16})}+1\right)}} \\
& + 2^{2^1+2^{2\left(2^{(2^{15}+2^2)}+2^{(2^{13}+2^4)}+2^{(2^{11}+2^6)}+2^{(2^9+2^8)}+2^{(2^7+2^{12})}+2^{(2^5+2^{10})}+2^{(2^3+2^{16})}+2^{(2^1+2^{14})}+1\right)}}
\end{aligned}
$$

Quaternion Group Q_8**.** Consider G with six objects of order 4. Let a be our only object of second order.

$$
\begin{array}{ccccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e \\
b & x_1 & a \\
x_1 & b & & a \\
c & x_2 & & & a \\
x_2 & c & & & & a \\
d & x_3 & & & & & a \\
x_3 & d & & & & & & a
\end{array}
$$

We find $x_1 * b = e$ and $b * x_1 = e$.

$$
\begin{array}{ccccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e \\
b & x_1 & a & e \\
x_1 & b & e & a \\
c & x_2 & & & a \\
x_2 & c & & & & a \\
d & x_3 & & & & & a \\
x_3 & d & & & & & & a
\end{array}
$$

Use $|b| = 4$ to find $b * a = x_1$.

$$
\begin{array}{ccccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b \\
b & x_1 & a & e \\
x_1 & b & e & a \\
c & x_2 & & & a \\
x_2 & c & & & & a \\
d & x_3 & & & & & a \\
x_3 & d & & & & & & a
\end{array}
$$

We have, without loss of generality, $b * c = d$,

$$
\begin{array}{ccccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b \\
b & x_1 & a & e \\
x_1 & b & e & a \\
c & x_2 & d & x_3 & a \\
x_2 & c & x_3 & d & & a \\
d & x_3 & x_2 & c & & & a \\
x_3 & d & c & x_2 & & & & a
\end{array}
$$

We use associativity as usual, to find

$$
\begin{array}{ccccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b \\
b & x_1 & a & e \\
x_1 & b & e & a \\
c & x_2 & d & x_3 & a & e \\
x_2 & c & x_3 & d & e & a \\
d & x_3 & x_2 & c & & & a & e \\
x_3 & d & c & x_2 & & & e & a
\end{array}
$$

Again we use $|c| = 4$ to find $c * a = x_2$. In the same way we use $|d| = 4$ to find $d * a = x_3$.

$$
\begin{array}{ccccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b & x_2 & c & x_3 & d \\
b & x_1 & a & e \\
x_1 & b & e & a \\
c & x_2 & d & x_3 & a & e \\
x_2 & c & x_3 & d & e & a \\
d & x_3 & x_2 & c & & & a & e \\
x_3 & d & c & x_2 & & & e & a
\end{array}
$$

Now we can use $c = x_1 * d$ to find $c * d = x_1 * (d * d) = x_1 * a = b$.

$$
\begin{array}{cccccccc}
e & a & b & x_1 & c & x_2 & d & x_3 \\
a & e & x_1 & b & x_2 & c & x_3 & d \\
b & x_1 & a & e \\
x_1 & b & e & a \\
c & x_2 & d & x_3 & a & e \\
x_2 & c & x_3 & d & e & a \\
d & x_3 & x_2 & c & b & x_1 & a & e \\
x_3 & d & c & x_2 & x_1 & b & e & a
\end{array}
$$

The rest of the table is determined as usual, with generic variables $g_1, g_2, g_3, g_4, g_5, g_6, g_7$.

$$
\begin{array}{cccccccc}
e & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 \\
g_1 & e & g_3 & g_2 & g_5 & g_4 & g_7 & g_6 \\
g_2 & g_3 & g_1 & e & g_7 & g_6 & g_4 & g_5 \\
g_3 & g_2 & e & g_1 & g_6 & g_7 & g_5 & g_4 \\
g_4 & g_5 & g_6 & g_7 & g_1 & e & g_3 & g_2 \\
g_5 & g_4 & g_7 & g_6 & e & g_1 & g_2 & g_3 \\
g_6 & g_7 & g_5 & g_4 & g_2 & g_3 & g_1 & e \\
g_7 & g_6 & g_4 & g_5 & g_3 & g_2 & e & g_1
\end{array}
$$

This group was determined by the conditions of having one second order object, g_1, and $g_1 = g_2^2 = g_3^2 = g_4^2 = g_5^2 = g_6^2$, where $g_6 = g_2 * g_4$. Thus, the system of equations

$$
g_1^2 = e
$$
$$
g_2^2 = g_4^2 = (g_1 * g_2)^2 = (g_1 * g_4)^2 = (g_2 * g_4)^2 = g_1.
$$

determines the quaternion group Q_8. Notice we did not include $g_1 = (g_4 * g_2)^2$, because it is implied by the others. We would like to find the canonical naming functions. we start with $e = 7$ and $g_1 = a = 6$ because g_1 is the only second order object. Then, we must choose a fourth order object to take the numerical value $b = 5$, and $x_1 = a * b = 4$. This object, b, is chosen from six possible objects of fourth order. Then we have to choose another object $c = 3$, and $a * c = x_2 = 2$, $b * c = d = 1$, $a * d = x_3 = 0$. The object c is chosen from four remaining objects. All the fourth order objects are equivalent and we have a total of twenty four canonical naming functions and automorphisms.

The numeric table given by the canonical naming funcitons is

$$
\begin{array}{cccccccc}
7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\
6 & 7 & 4 & 5 & 2 & 3 & 0 & 1 \\
5 & 4 & 6 & 7 & 0 & 1 & 3 & 2 \\
4 & 5 & 7 & 6 & 1 & 0 & 2 & 3 \\
3 & 2 & 1 & 0 & 6 & 7 & 4 & 5 \\
2 & 3 & 0 & 1 & 7 & 6 & 5 & 4 \\
1 & 0 & 2 & 3 & 5 & 4 & 6 & 7 \\
0 & 1 & 3 & 2 & 4 & 5 & 7 & 6
\end{array}
$$

The canonical representation is

$$
\begin{aligned}
N_{Q_8} = \; & 2^{2^{15}+2^2\left(2^{(2^{15}+2^{16})}+2^{(2^{13}+2^{14})}+2^{(2^{11}+2^{12})}+2^{(2^9+2^{10})}+2^{(2^7+2^8)}+2^{(2^5+2^6)}+2^{(2^3+2^4)}+2^{(2^1+2^2)}+1\right)} \\
+ \; & 2^{2^{13}+2^2\left(2^{(2^{15}+2^{14})}+2^{(2^{13}+2^{16})}+2^{(2^{11}+2^{10})}+2^{(2^9+2^{12})}+2^{(2^7+2^6)}+2^{(2^5+2^8)}+2^{(2^3+2^2)}+2^{(2^1+2^4)}+1\right)} \\
+ \; & 2^{2^{11}+2^2\left(2^{(2^{15}+2^{12})}+2^{(2^{13}+2^{10})}+2^{(2^{11}+2^{14})}+2^{(2^9+2^{16})}+2^{(2^7+2^4)}+2^{(2^5+2^2)}+2^{(2^3+2^6)}+2^{(2^1+2^8)}+1\right)} \\
+ \; & 2^{2^9+2^2\left(2^{(2^{15}+2^{10})}+2^{(2^{13}+2^{12})}+2^{(2^{11}+2^{16})}+2^{(2^9+2^{14})}+2^{(2^7+2^2)}+2^{(2^5+2^4)}+2^{(2^3+2^8)}+2^{(2^1+2^6)}+1\right)} \\
+ \; & 2^{2^7+2^2\left(2^{(2^{15}+2^8)}+2^{(2^{13}+2^6)}+2^{(2^{11}+2^2)}+2^{(2^9+2^4)}+2^{(2^7+2^{14})}+2^{(2^5+2^{16})}+2^{(2^3+2^{12})}+2^{(2^1+2^{10})}+1\right)} \\
+ \; & 2^{2^5+2^2\left(2^{(2^{15}+2^6)}+2^{(2^{13}+2^8)}+2^{(2^{11}+2^4)}+2^{(2^9+2^2)}+2^{(2^7+2^{16})}+2^{(2^5+2^{14})}+2^{(2^3+2^{10})}+2^{(2^1+2^{12})}+1\right)} \\
+ \; & 2^{2^3+2^2\left(2^{(2^{15}+2^4)}+2^{(2^{13}+2^2)}+2^{(2^{11}+2^8)}+2^{(2^9+2^6)}+2^{(2^7+2^{10})}+2^{(2^5+2^{12})}+2^{(2^3+2^{14})}+2^{(2^1+2^{16})}+1\right)} \\
+ \; & 2^{2^1+2^2\left(2^{(2^{15}+2^2)}+2^{(2^{13}+2^4)}+2^{(2^{11}+2^6)}+2^{(2^9+2^8)}+2^{(2^7+2^{12})}+2^{(2^5+2^{10})}+2^{(2^3+2^{16})}+2^{(2^1+2^{14})}+1\right)} .
\end{aligned}
$$

Cyclic Group $\mathbb{Z}_8$. Finding the cyclic group is trivial, and it is defined by the equations $a^2 = b$, $b^2 = c$, $c^2 = e$. It has numeric table

$$
\begin{array}{cccccccc}
7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\
6 & 5 & 4 & 3 & 2 & 1 & 0 & 7 \\
5 & 4 & 3 & 2 & 1 & 0 & 7 & 6 \\
4 & 3 & 2 & 1 & 0 & 7 & 6 & 5 \\
3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 \\
2 & 1 & 0 & 7 & 6 & 5 & 4 & 3 \\
1 & 0 & 7 & 6 & 5 & 4 & 3 & 2 \\
0 & 7 & 6 & 5 & 4 & 3 & 2 & 1
\end{array}
$$

The canonical representation of this group being

$$
\begin{aligned}
N_{\mathbb{Z}_8} = \; & 2^{2^{15}+2^2\left(2^{(2^{15}+2^{16})}+2^{(2^{13}+2^{14})}+2^{(2^{11}+2^{12})}+2^{(2^9+2^{10})}+2^{(2^7+2^8)}+2^{(2^5+2^6)}+2^{(2^3+2^4)}+2^{(2^1+2^2)}+1\right)} \\
+ \; & 2^{2^{13}+2^2\left(2^{(2^{15}+2^{14})}+2^{(2^{13}+2^{12})}+2^{(2^{11}+2^{10})}+2^{(2^9+2^8)}+2^{(2^7+2^6)}+2^{(2^5+2^4)}+2^{(2^3+2^2)}+2^{(2^1+2^{16})}+1\right)} \\
+ \; & 2^{2^{11}+2^2\left(2^{(2^{15}+2^{12})}+2^{(2^{13}+2^{10})}+2^{(2^{11}+2^8)}+2^{(2^9+2^6)}+2^{(2^7+2^4)}+2^{(2^5+2^2)}+2^{(2^3+2^{16})}+2^{(2^1+2^{14})}+1\right)} \\
+ \; & 2^{2^9+2^2\left(2^{(2^{15}+2^{10})}+2^{(2^{13}+2^8)}+2^{(2^{11}+2^6)}+2^{(2^9+2^4)}+2^{(2^7+2^2)}+2^{(2^5+2^{16})}+2^{(2^3+2^{14})}+2^{(2^1+2^{12})}+1\right)} \\
+ \; & 2^{2^7+2^2\left(2^{(2^{15}+2^8)}+2^{(2^{13}+2^6)}+2^{(2^{11}+2^4)}+2^{(2^9+2^2)}+2^{(2^7+2^{16})}+2^{(2^5+2^{14})}+2^{(2^3+2^{12})}+2^{(2^1+2^{10})}+1\right)} \\
+ \; & 2^{2^5+2^2\left(2^{(2^{15}+2^6)}+2^{(2^{13}+2^4)}+2^{(2^{11}+2^2)}+2^{(2^9+2^{16})}+2^{(2^7+2^{14})}+2^{(2^5+2^{12})}+2^{(2^3+2^{10})}+2^{(2^1+2^8)}+1\right)} \\
+ \; & 2^{2^3+2^2\left(2^{(2^{15}+2^4)}+2^{(2^{13}+2^2)}+2^{(2^{11}+2^{16})}+2^{(2^9+2^{14})}+2^{(2^7+2^{12})}+2^{(2^5+2^{10})}+2^{(2^3+2^8)}+2^{(2^1+2^6)}+1\right)} \\
+ \; & 2^{2^1+2^2\left(2^{(2^{15}+2^2)}+2^{(2^{13}+2^{16})}+2^{(2^{11}+2^{14})}+2^{(2^9+2^{12})}+2^{(2^7+2^{10})}+2^{(2^5+2^8)}+2^{(2^3+2^6)}+2^{(2^1+2^4)}+1\right)}
\end{aligned}
$$

We have ordered groups of eight objects. The order is $\mathbb{Z}_8 < Q_8 < D_8 < \mathbb{Z}_2 \oplus \mathbb{Z}_4 < \mathbb{Z}_2^3$.

4.6 $|G| = 9$

Direct Product $\mathbb{Z}_3 \oplus \mathbb{Z}_3$. We know that if $|G| = 9$ then $|g| = 3$ or $|g| = 9$ for any $g \in G$, so we start looking for groups with all objects of order 3.

$$
\begin{array}{ccccccccc}
e & a & x_1 & b & x_2 & x_3 & c & x_4 & x_5 \\
a & x_1 \\
x_1 & e \\
b & x_2 \\
x_2 & x_3 \\
x_3 & b \\
c & x_4 \\
x_4 & x_5 \\
x_5 & c
\end{array}
$$

We know the function $*x_1$ is equal to the composition $*a \circ *a$ so that

$$
\begin{array}{ccccccccc}
e & a & x_1 & b & x_2 & x_3 & c & x_4 & x_5 \\
a & x_1 & e \\
x_1 & e & a \\
b & x_2 & x_3 \\
x_2 & x_3 & b \\
x_3 & b & x_2 \\
c & x_4 & x_5 \\
x_4 & x_5 & c \\
x_5 & c & x_4
\end{array}
$$

Since $|b| = 3$, we know $b^2 \neq a$. If $b^2 = a$, then we would have $b*a = e$ which is a contradiction. We suppose $b^2 = c$, without loss of generality.

$$
\begin{array}{llllllllll}
e & a & x_1 & b & x_2 & x_3 & c & x_4 & x_5 \\
a & x_1 & e \\
x_1 & e & a \\
b & x_2 & x_3 & c \\
x_2 & x_3 & b \\
x_3 & b & x_2 \\
c & x_4 & x_5 & e \\
x_4 & x_5 & c \\
x_5 & c & x_4
\end{array}
$$

We easily find the rest of the rows of b and c.

$$
\begin{array}{llllllllll}
e & a & x_1 & b & x_2 & x_3 & c & x_4 & x_5 \\
a & x_1 & e \\
x_1 & e & a \\
b & x_2 & x_3 & c & x_4 & x_5 & e & a & x_1 \\
x_2 & x_3 & b \\
x_3 & b & x_2 \\
c & x_4 & x_5 & e & a & x_1 & b & x_2 & x_3 \\
x_4 & x_5 & c \\
x_5 & c & x_4
\end{array}
$$

Let us see if we can have a non abelian group. The first option for this is $b * a = x_3$, which implies $x_2 * a = b$.

$$
\begin{array}{llllllllll}
e & a & x_1 & b & x_2 & x_3 & c & x_4 & x_5 \\
a & x_1 & e & x_3 & b \\
x_1 & e & a \\
b & x_2 & x_3 & c & x_4 & x_5 & e & a & x_1 \\
x_2 & x_3 & b \\
x_3 & b & x_2 \\
c & x_4 & x_5 & e & a & x_1 & b & x_2 & x_3 \\
x_4 & x_5 & c \\
x_5 & c & x_4
\end{array}
$$

We have a contradiction because $|x_2| = 3$ implies $x_2 * x_4 = a$. We also get a contradiction if $b * a = x_4$.

$$
\begin{array}{llllllllll}
e & a & x_1 & b & x_2 & x_3 & c & x_4 & x_5 \\
a & x_1 & e & x_4 & x_5 & c \\
x_1 & e & a \\
b & x_2 & x_3 & c & x_4 & x_5 & e & a & x_1 \\
x_2 & x_3 & b \\
x_3 & b & x_2 \\
c & x_4 & x_5 & e & a & x_1 & b & x_2 & x_3 \\
x_4 & x_5 & c \\
x_5 & c & x_4
\end{array}
$$

This table leads to contradiction because $|x_3| = 3$ implies $x_3 * x_1 = a$. The supposition $b * a = x_5$ leads to contradiction also.

$$
\begin{array}{llllllllll}
e & a & x_1 & b & x_2 & x_3 & c & x_4 & x_5 \\
a & x_1 & e & x_5 & c \\
x_1 & e & a \\
b & x_2 & x_3 & c & x_4 & x_5 & e & a & x_1 \\
x_2 & x_3 & b \\
x_3 & b & x_2 \\
c & x_4 & x_5 & e & a & x_1 & b & x_2 & x_3 \\
x_4 & x_5 & c \\
x_5 & c & x_4
\end{array}
$$

The table shows $x_2 * a = c$ and $x_2 * c = a$, which is a contradiction with the fact that $|x_2| = 3$. We conclude $b * a = x_2$. From this we can trivially find $x_2 * a = x_3$ and $x_3 * a = b$. We use this last expression to find $b * x_1 = x_3$.

$$
\begin{array}{lllllllll}
e & a & x_1 & b & x_2 & x_3 & c & x_4 & x_5 \\
a & x_1 & e & x_2 & x_3 & b \\
x_1 & e & a & x_3 & b & x_2 \\
b & x_2 & x_3 & c & x_4 & x_5 & e & a & x_1 \\
x_2 & x_3 & b \\
x_3 & b & x_2 \\
c & x_4 & x_5 & e & a & x_1 & b & x_2 & x_3 \\
x_4 & x_5 & c \\
x_5 & c & x_4
\end{array}
$$

Use the expression $b = x_2 * x_1$ to find $b * x_2 = x_4$.

$$
\begin{array}{lllllllll}
e & a & x_1 & b & x_2 & x_3 & c & x_4 & x_5 \\
a & x_1 & e & x_2 & x_3 & b \\
x_1 & e & a & x_3 & b & x_2 \\
b & x_2 & x_3 & c & x_4 & x_5 & e & a & x_1 \\
x_2 & x_3 & b & x_4 & x_5 & c \\
x_3 & b & x_2 & x_5 & c & x_4 \\
c & x_4 & x_5 & e & a & x_1 & b & x_2 & x_3 \\
x_4 & x_5 & c \\
x_5 & c & x_4
\end{array}
$$

Now use $b = x_2 * x_1$ to find $b * x_4 = a$.

$$
\begin{array}{lllllllll}
e & a & x_1 & b & x_2 & x_3 & c & x_4 & x_5 \\
a & x_1 & e & x_2 & x_3 & b \\
x_1 & e & a & x_3 & b & x_2 \\
b & x_2 & x_3 & c & x_4 & x_5 & e & a & x_1 \\
x_2 & x_3 & b & x_4 & x_5 & c \\
x_3 & b & x_2 & x_5 & c & x_4 \\
c & x_4 & x_5 & e & a & x_1 & b & x_2 & x_3 \\
x_4 & x_5 & c & a & x_1 & e \\
x_5 & c & x_4 & x_1 & e & a
\end{array}
$$

Finding the rest of the table is trivial. We have the direct product group $\mathbb{Z}_3 \oplus \mathbb{Z}_3$. The system of equations that defines this group is given by the relations

$$
\begin{aligned}
a^2 &= x_1 \\
b^2 &= c \\
a^3 = b^3 &= e \\
a * b &= b * a.
\end{aligned}
$$

Simply put, this group is determined by two commuting objects such that $|a| = |b| = 3$. Now let us find the canonical naming function of this group. We begin by expressing the table in generic variables g_i.

$$
\begin{array}{lllllllll}
e & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 \\
g_1 & g_2 & e & g_4 & g_5 & g_3 & g_7 & g_8 & g_6 \\
g_2 & e & g_1 & g_5 & g_3 & g_4 & g_8 & g_6 & g_7 \\
g_3 & g_4 & g_5 & g_6 & g_7 & g_8 & e & g_1 & g_2 \\
g_4 & g_5 & g_3 & g_7 & g_8 & g_6 & g_1 & g_2 & e \\
g_5 & g_3 & g_4 & g_8 & g_6 & g_7 & g_2 & e & g_1 \\
g_6 & g_7 & g_8 & e & g_1 & g_2 & g_3 & g_4 & g_5 \\
g_7 & g_8 & g_6 & g_1 & g_2 & e & g_4 & g_5 & g_3 \\
g_8 & g_6 & g_7 & g_2 & e & g_1 & g_5 & g_3 & g_4
\end{array}
$$

To find the canonical naming, observe that the group is commutative. Our group naming will be defined if we choose any two objects a, b such that $a^2 \neq b$. Let $e = 8$ and choose an arbitrary $a = 7$. Then $a^2 = 6$ maximizes our representation. The object a is chosen from eight possible choices. Next we need to choose a second object $b = 5$, and then we have to name $a * b = x_2 = 4$ and $a * x_2 = 3$. This object b can be chosen from six remaining objects. Finally, we assign the values $b^2 = c = 2$, $a * c = x_4 = 1$, $a * x_4 = x_5 = 0$. This has determined a total of forty eight canonical naming functions and automorphisms of $\mathbb{Z}_3^2$. Choose two objects a, b such that $a^2 \neq b$ and the rest of the naming values are determined. This gives us the numeric table

```
8 7 6 5 4 3 2 1 0
7 6 8 4 3 5 1 0 2
6 8 7 3 5 4 0 2 1
5 4 3 2 1 0 8 7 6
4 3 5 1 0 2 7 6 8
3 5 4 0 2 1 6 8 7
2 1 0 8 7 6 5 4 3
1 0 2 7 6 8 4 3 5
0 2 1 6 8 7 3 5 4
```

The canonical representation of this group is the number

$$N_{\mathbb{Z}_3^2} = 2^{2^{17}} + 2^{2\left(2^{(2^{17}+2^{18})}+2^{(2^{15}+2^{16})}+2^{(2^{13}+2^{14})}+2^{(2^{11}+2^{12})}+2^{(2^9+2^{10})}+2^{(2^7+2^8)}+2^{(2^5+2^6)}+2^{(2^3+2^4)}+2^{(2^1+2^2)}+1\right)}$$

$$+ 2^{2^{15}} + 2^{2\left(2^{(2^{17}+2^{16})}+2^{(2^{15}+2^{14})}+2^{(2^{13}+2^{18})}+2^{(2^{11}+2^{10})}+2^{(2^9+2^8)}+2^{(2^7+2^{12})}+2^{(2^5+2^4)}+2^{(2^3+2^2)}+2^{(2^1+2^6)}+1\right)}$$

$$+ 2^{2^{13}} + 2^{2\left(2^{(2^{17}+2^{14})}+2^{(2^{15}+2^{18})}+2^{(2^{13}+2^{16})}+2^{(2^{11}+2^8)}+2^{(2^9+2^{12})}+2^{(2^7+2^{10})}+2^{(2^5+2^2)}+2^{(2^3+2^6)}+2^{(2^1+2^4)}+1\right)}$$

$$+ 2^{2^{11}} + 2^{2\left(2^{(2^{17}+2^{12})}+2^{(2^{15}+2^{10})}+2^{(2^{13}+2^8)}+2^{(2^{11}+2^6)}+2^{(2^9+2^4)}+2^{(2^7+2^2)}+2^{(2^5+2^{18})}+2^{(2^3+2^{16})}+2^{(2^1+2^{14})}+1\right)}$$

$$+ 2^{2^9} + 2^{2\left(2^{(2^{17}+2^{10})}+2^{(2^{15}+2^8)}+2^{(2^{13}+2^{12})}+2^{(2^{11}+2^4)}+2^{(2^9+2^2)}+2^{(2^7+2^6)}+2^{(2^5+2^{16})}+2^{(2^3+2^{14})}+2^{(2^1+2^{18})}+1\right)}$$

$$+ 2^{2^7} + 2^{2\left(2^{2^{(2^{17}+2^8)}}+(2^{15}+2^{12})+2^{(2^{13}+2^{10})}+2^{(2^{11}+2^2)}+2^{(2^9+2^6)}+2^{(2^7+2^4)}+2^{(2^5+2^{14})}+2^{(2^3+2^{18})}+2^{(2^1+2^{16})}+1\right)}$$

$$+ 2^{2^5} + 2^{2\left(2^{(2^{17}+2^6)}+2^{(2^{15}+2^4)}+2^{(2^{13}+2^2)}+2^{(2^{11}+2^{18})}+2^{(2^9+2^{16})}+2^{(2^7+2^{14})}+2^{(2^5+2^{12})}+2^{(2^3+2^{10})}+2^{(2^1+2^8)}+1\right)}$$

$$+ 2^{2^3} + 2^{2\left(2^{(2^{17}+2^4)}+2^{(2^{15}+2^2)}+2^{(2^{13}+2^6)}+2^{(2^{11}+2^{16})}+2^{(2^9+2^{14})}+2^{(2^7+2^{18})}+2^{(2^5+2^{10})}+2^{(2^3+2^8)}+2^{(2^1+2^{12})}+1\right)}$$

$$+ 2^{2^1} + 2^{2\left(2^{(2^{17}+2^2)}+2^{(2^{15}+2^6)}+2^{(2^{13}+2^4)}+2^{(2^{11}+2^{14})}+2^{(2^9+2^{18})}+2^{(2^7+2^{16})}+2^{(2^5+2^8)}+2^{(2^3+2^{12})}+2^{(2^1+2^{10})}+1\right)}$$

Cyclic Group $\mathbb{Z}_9$**.** If $|G| = 9$, we know the objects of G have order 3 or 9. We found the only group with all the objects of order three. Now we consider the case where we have at least one object of order 9. But, since our group has nine objects, this must be the cyclic group, $\mathbb{Z}_9$. The cyclic group of nine objects is trivially given by the numeric table

```
8 7 6 5 4 3 2 1 0
7 6 5 4 3 2 1 0 8
6 5 4 3 2 1 0 8 7
5 4 3 2 1 0 8 7 6
4 3 2 1 0 8 7 6 5
3 2 1 0 8 7 6 5 4
2 1 0 8 7 6 5 4 3
1 0 8 7 6 5 4 3 2
0 8 7 6 5 4 3 2 1
```

The canonical representation is

$$N_{\mathbb{Z}_9} = 2^{2^{17}+2^{2\left(2^{(2^{17}+2^{18})}+2^{(2^{15}+2^{16})}+2^{(2^{13}+2^{14})}+2^{(2^{11}+2^{12})}+2^{(2^9+2^{10})}+2^{(2^7+2^8)}+2^{(2^5+2^6)}+2^{(2^3+2^4)}+2^{(2^1+2^2)}+1\right)}}$$

$$+ 2^{2^{15}+2^{2\left(2^{(2^{17}+2^{16})}+2^{(2^{15}+2^{14})}+2^{(2^{13}+2^{12})}+2^{(2^{11}+2^{10})}+2^{(2^9+2^8)}+2^{(2^7+2^6)}+2^{(2^5+2^4)}+2^{(2^3+2^2)}+2^{(2^1+2^{18})}+1\right)}}$$

$$+ 2^{2^{13}+2^{2\left(2^{(2^{17}+2^{14})}+2^{(2^{15}+2^{12})}+2^{(2^{13}+2^{10})}+2^{(2^{11}+2^8)}+2^{(2^9+2^6)}+2^{(2^7+2^4)}+2^{(2^5+2^2)}+2^{(2^3+2^{18})}+2^{(2^1+2^{16})}+1\right)}}$$

$$+ 2^{2^{11}+2^{2\left(2^{(2^{17}+2^{12})}+2^{(2^{15}+2^{10})}+2^{(2^{13}+2^8)}+2^{(2^{11}+2^6)}+2^{(2^9+2^4)}+2^{(2^7+2^2)}+2^{(2^5+2^{18})}+2^{(2^3+2^{16})}+2^{(2^1+2^{14})}+1\right)}}$$

$$+ 2^{2^9+2^{2\left(2^{(2^{17}+2^{10})}+2^{(2^{15}+2^8)}+2^{(2^{13}+2^6)}+2^{(2^{11}+2^4)}+2^{(2^9+2^2)}+2^{(2^7+2^{18})}+2^{(2^5+2^{16})}+2^{(2^3+2^{14})}+2^{(2^1+2^{12})}+1\right)}}$$

$$+ 2^{2^7+2^{2\left(2^{2^{(2^{17}+2^8)}}+(2^{15}+2^6)+2^{(2^{13}+2^4)}+2^{(2^{11}+2^2)}+2^{(2^9+2^{18})}+2^{(2^7+2^{16})}+2^{(2^5+2^{14})}+2^{(2^3+2^{12})}+2^{(2^1+2^{10})}+1\right)}}$$

$$+ 2^{2^5+2^{2\left(2^{(2^{17}+2^6)}+2^{(2^{15}+2^4)}+2^{(2^{13}+2^2)}+2^{(2^{11}+2^{18})}+2^{(2^9+2^{16})}+2^{(2^7+2^{14})}+2^{(2^5+2^{12})}+2^{(2^3+2^{10})}+2^{(2^1+2^8)}+1\right)}}$$

$$+ 2^{2^3+2^{2\left(2^{(2^{17}+2^4)}+2^{(2^{15}+2^2)}+2^{(2^{13}+2^{18})}+2^{(2^{11}+2^{16})}+2^{(2^9+2^{14})}+2^{(2^7+2^{12})}+2^{(2^5+2^{10})}+2^{(2^3+2^8)}+2^{(2^1+2^6)}+1\right)}}$$

$$+ 2^{2^1+2^{2\left(2^{(2^{17}+2^2)}+2^{(2^{15}+2^{18})}+2^{(2^{13}+2^{16})}+2^{(2^{11}+2^{14})}+2^{(2^9+2^{12})}+2^{(2^7+2^{10})}+2^{(2^5+2^8)}+2^{(2^3+2^6)}+2^{(2^1+2^4)}+1\right)}}$$

Comparing the two numbers, we verify $\mathbb{Z}_9 < \mathbb{Z}_3^2$. It is becoming more clear how to find the canonical representation, without having to calculate all the representations. But we still have several steps before considering the general case.

4.7 Δ_4

We exhibit, for reference, the multiplication table of Δ_4. The symbols g_i are used for the elements of order 2. We use h_i for the rest of the objects.

$$
\begin{array}{ccccccccccccccccccccccccc}
e & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 & g_9 & h_1 & h_2 & h_3 & h_4 & h_5 & h_6 & h_7 & h_8 & h_9 & h_{10} & h_{11} & h_{12} & h_{13} & h_{14} \\
g_1 & e & g_4 & g_5 & g_2 & g_3 & h_2 & h_1 & h_4 & h_3 & g_7 & g_6 & g_9 & g_8 & h_6 & h_5 & h_{12} & h_{11} & h_{14} & h_{13} & h_8 & h_7 & h_{10} & h_9 \\
g_2 & g_4 & e & h_6 & g_1 & h_5 & h_1 & h_2 & g_9 & g_8 & g_6 & g_7 & h_4 & h_3 & g_5 & g_3 & h_{11} & h_{12} & h_{10} & h_9 & h_7 & h_8 & h_{14} & h_{13} \\
g_3 & g_5 & h_5 & e & h_6 & g_1 & h_{10} & h_9 & h_8 & h_7 & h_{14} & h_{13} & h_{12} & h_{11} & g_2 & g_4 & g_9 & g_8 & g_7 & g_6 & h_4 & h_3 & h_2 & h_1 \\
g_4 & g_2 & g_1 & h_5 & e & h_6 & g_7 & g_6 & h_3 & h_4 & h_2 & h_1 & g_8 & g_9 & g_3 & g_5 & h_8 & h_7 & h_{13} & h_{14} & h_{12} & h_{11} & h_9 & h_{10} \\
g_5 & g_3 & h_6 & g_1 & h_5 & e & h_{13} & h_{14} & h_{11} & h_{12} & h_9 & h_{10} & h_7 & h_8 & g_4 & g_2 & h_3 & h_4 & h_1 & h_2 & g_8 & g_9 & g_6 & g_7 \\
g_6 & h_1 & h_2 & h_7 & g_7 & h_{11} & e & g_4 & h_{13} & h_{10} & g_1 & g_2 & h_9 & h_{14} & h_8 & h_{12} & g_3 & h_5 & h_3 & g_9 & g_5 & h_6 & g_8 & h_4 \\
g_7 & h_2 & h_1 & h_8 & g_6 & h_{12} & g_4 & e & h_9 & h_{14} & g_2 & g_1 & h_{13} & h_{10} & h_7 & h_{11} & h_5 & g_3 & g_8 & h_4 & h_6 & g_5 & h_3 & g_9 \\
g_8 & h_3 & g_9 & h_9 & h_4 & h_{13} & h_{11} & h_8 & e & g_2 & h_7 & h_{12} & g_1 & g_4 & h_{14} & h_{10} & h_1 & g_7 & g_3 & h_6 & g_6 & h_2 & g_5 & h_5 \\
g_9 & h_4 & g_8 & h_{10} & h_3 & h_{14} & h_7 & h_{12} & g_2 & e & h_{11} & h_8 & g_4 & g_1 & h_{13} & h_9 & g_6 & h_2 & h_6 & g_3 & h_1 & g_7 & h_5 & g_5 \\
h_1 & g_6 & g_7 & h_{11} & h_2 & h_7 & g_2 & g_1 & h_{14} & h_9 & g_4 & e & h_{10} & h_{13} & h_{12} & h_8 & h_6 & g_5 & h_4 & g_8 & h_5 & g_3 & g_9 & h_3 \\
h_2 & g_7 & g_6 & h_{12} & h_1 & h_8 & g_1 & g_2 & h_{10} & h_{13} & e & g_4 & h_{14} & h_9 & h_{11} & h_7 & g_5 & h_6 & g_9 & h_3 & g_3 & h_5 & h_4 & g_8 \\
h_3 & g_8 & h_4 & h_{13} & g_9 & h_9 & h_{12} & h_7 & g_4 & g_1 & h_8 & h_{11} & g_2 & e & h_{10} & h_{14} & h_2 & g_6 & h_5 & g_5 & g_7 & h_1 & h_6 & g_3 \\
h_4 & g_9 & h_3 & h_{14} & g_8 & h_{10} & h_8 & h_{11} & g_1 & g_4 & h_{12} & h_7 & e & g_2 & h_9 & h_{13} & g_7 & h_1 & g_5 & h_5 & h_2 & g_6 & g_3 & h_6 \\
h_5 & h_6 & g_3 & g_4 & g_5 & g_2 & h_{14} & h_{13} & h_7 & h_8 & h_{10} & h_9 & h_{11} & h_{12} & g_1 & e & h_4 & h_3 & g_6 & g_7 & g_9 & g_8 & h_1 & h_2 \\
h_6 & h_5 & g_5 & g_2 & g_3 & g_4 & h_9 & h_{10} & h_{12} & h_{11} & h_{13} & h_{14} & h_8 & h_7 & e & g_1 & g_8 & g_9 & h_2 & h_1 & h_3 & h_4 & g_7 & g_6 \\
h_7 & h_{11} & h_8 & g_6 & h_{12} & h_1 & g_9 & h_3 & h_5 & g_3 & h_4 & g_8 & h_6 & g_5 & h_2 & g_7 & h_{10} & h_{13} & g_4 & e & h_{14} & h_9 & g_2 & g_1 \\
h_8 & h_{12} & h_7 & g_7 & h_{11} & h_2 & h_4 & g_8 & g_3 & h_5 & g_9 & h_3 & g_5 & h_6 & h_1 & g_6 & h_{14} & h_9 & e & g_4 & h_{10} & h_{13} & g_1 & g_2 \\
h_9 & h_{13} & h_{14} & g_8 & h_{10} & h_3 & h_6 & g_3 & g_7 & h_1 & h_5 & g_5 & h_2 & g_6 & g_9 & h_4 & g_2 & e & h_8 & h_{11} & g_4 & g_1 & h_{12} & h_7 \\
h_{10} & h_{14} & h_{13} & g_9 & h_9 & h_4 & g_3 & h_6 & h_2 & g_6 & g_5 & h_5 & g_7 & h_1 & g_8 & h_3 & e & g_2 & h_{12} & h_7 & g_1 & g_4 & h_8 & h_{11} \\
h_{11} & h_7 & h_{12} & h_1 & h_8 & g_6 & g_8 & h_4 & g_5 & h_6 & h_3 & g_9 & g_3 & h_5 & g_7 & h_2 & h_9 & h_{14} & g_1 & g_2 & h_{13} & h_{10} & e & g_4 \\
h_{12} & h_8 & h_{11} & h_2 & h_7 & g_7 & h_3 & g_9 & h_6 & g_5 & g_8 & h_4 & h_5 & g_3 & g_6 & h_1 & h_{13} & h_{10} & g_2 & g_1 & h_9 & h_{14} & g_4 & e \\
h_{13} & h_9 & h_{10} & h_3 & h_{14} & g_8 & g_5 & h_5 & g_6 & h_2 & g_3 & h_6 & h_1 & g_7 & h_4 & g_9 & g_1 & g_4 & h_7 & h_{12} & e & g_2 & h_{11} & h_8 \\
h_{14} & h_{10} & h_9 & h_4 & h_{13} & g_9 & h_5 & g_5 & h_1 & g_7 & h_6 & g_3 & g_6 & h_2 & h_3 & g_8 & g_4 & g_1 & h_{11} & h_8 & g_2 & e & h_7 & h_{12}
\end{array}
$$

(17)

We do mention, ahead of time, the canonical naming function does not assign the highest ten values to the set $\{e, g_1, g_2, \ldots, g_9\}$. Some h_i objects will have a higher numeric value than some g_i. The smallest order of any non trivial object is 2. It is obvious we must make $e = 23$, $23 = a$, $22 = b$ for two second order objects, a, b, that commute. We have the following possible pairs:

$$\begin{array}{cc}
\{g_1,g_2\} & \{g_4,g_6\} \\
\{g_1,g_4\} & \{g_4,g_7\} \\
\{g_2,g_4\} & \{g_6,g_7\} \\
\{g_1,g_3\} & \{g_2,g_8\} \\
\{g_1,g_5\} & \{g_2,g_9\} \\
\{g_3,g_5\} & \{g_8,g_9\}
\end{array} \tag{18}$$

Let a,b any of these pairs; we can use the pairs in either order because they are not ordered pairs. For example, we can have $a = g_1$, $b = g_2$, or we can also assign $a = g_2$, $b = g_1$. We can use any of the pairs above, and the naming function $e = 23$, $a = 22$, $b = 21$, $x_1 = 20$ gives the table

$$\begin{array}{cccc}
e & a & b & x_1 \\
a & e & x_1 & b \\
b & x_1 & e & a \\
x_1 & b & a & e
\end{array}$$

If we wish to maximize our representation, we shall find a, b, x_1 such that $\{e, a, b, x_1\}$ forms the Klein 4-group. We see that in fact the triads

$$\{g_1,g_2,g_4\} \quad \{g_1,g_3,g_5\} \quad \{g_4,g_6,g_7\} \quad \{g_2,g_8,g_9\} \tag{19}$$

form the Klein 4-group. Given any one of these triads, we do not know which objects will be a and b. For example, if we work with $\{g_1,g_2,g_4\}$, who should we define as a, b, x_1? All the non trivial objects of $K(4)$ are equivalent, so we can not decide upon this yet. Let us add a new object c_1 and $x_2 = a * c_1$

$$\begin{array}{cccccc}
e & a & b & x_1 & c_1 & x_2 \\
a & e & x_1 & b \\
b & x_1 & e & a \\
x_1 & b & a & e \\
c_1 & x_2 \\
x_2 & c_1
\end{array}$$

We also need a new object $c_2 = b * c_1$, and $x_3 = a * c_2$.

$$\begin{array}{cccccccc}
e & a & b & x_1 & c_1 & x_2 & c_2 & x_3 \\
a & e & x_1 & b \\
b & x_1 & e & a \\
x_1 & b & a & e \\
c_1 & x_2 & c_2 & x_3 \\
x_2 & c_1 & x_3 & c_2 \\
c_2 & x_3 & c_1 & x_2 \\
x_3 & c_2 & x_2 & c_1
\end{array}$$

In summary, the canonical naming function will involve one of the Klein 4-subgroups. And, we need an object c_1 that commutes with a, if it should exist. This maximizes the last table. We will see that there are still several options to do this. In fact, all our candidate naming functions admit an object c_1 that commutes with a. This gives the table

$$\begin{array}{cccccccc}
e & a & b & x_1 & c_1 & x_2 & c_2 & x_3 \\
a & e & x_1 & b & x_2 & c_1 \\
b & x_1 & e & a \\
x_1 & b & a & e \\
c_1 & x_2 & c_2 & x_3 \\
x_2 & c_1 & x_3 & c_2 \\
c_2 & x_3 & c_1 & x_2 \\
x_3 & c_2 & x_2 & c_1
\end{array}$$

determined by the equations

$$e = a^2 = b^2$$
$$a * b = b * a$$
$$a * c_1 = c_1 * a.$$

For the triads in (19), we need to find an object c_1 that commutes with a. For example, all the objects in $H_1 = \{g_1,g_2,g_4\}$ commute with at least one object not in H_1. In the case of $H_2 = \{g_2,g_8,g_9\}$, only g_2 commutes with objects not in H_2. This means if we are working with the triad $\{g_2,g_8,g_9\}$ we must have $a = g_2$. For $\{g_1,g_3,g_5\}$ we must have $a = g_1$, and for $\{g_4,g_6,g_7\}$ we must assign $a = g_4$. We list the objects that commute with each second order object g_i.

$$\begin{aligned}
Comm(g_1) &= \{g_2, g_4, g_3, g_5, h_5, h_6\} \quad Comm(g_2) = \{g_1, g_4, g_8, g_9, h_3, h_4\} \quad Comm(g_3) = \{g_1, g_5\} \\
Comm(g_4) &= \{g_1, g_2, g_6, g_7, h_1, h_2\} \quad\quad\quad Comm(g_5) = \{g_1, g_3\} \quad\quad\quad Comm(g_6) = \{g_4, g_7\} \\
Comm(g_7) &= \{g_4, g_6\} \quad\quad\quad\quad\quad\quad Comm(g_8) = \{g_2, g_9\} \quad\quad\quad Comm(g_9) = \{g_2, g_8\}
\end{aligned} \quad (20)$$

This information reduces our possible naming functions because now we know a little more about a. Our possible naming functions are more than we would like to list, but they are easy to describe. We need an object $a \in \{g_1, g_2, g_4\}$, and we need a second order object b to determine the subgroup $K(4)$. For example, if we choose $a = g_4$ we can choose $b \in \{g_1, g_2, g_6, g_7\}$; find a second order object that commutes with $a = g_4$. In the case of $a = g_1$ we need to choose $b \in \{g_2, g_4, g_3, g_5\}$. If $a = g_2$ then $b \in \{g_1, g_4, g_8, g_9\}$. After determining the subgroup $K(4)$, we need an object c_1 that commutes with a. The expressions of (20) let us know which combinations allow c_1. We shall start representing naming functions with finite sequences. We will write naming functions in the form $(a, b, x_1, c_1, x_2, c_2, x_3)$. For example, the naming function $a = g_4$, $b = g_2$, $x_1 = a*b = g_1$, $c_1 = g_7$, $x_2 = a*c_1 = g_6$, $c_2 = b*c_1 = h_1$, $x_3 = a*c_2 = h_2$ is given by the expression $(g_4, g_2, g_1, g_7, g_6, h_1, h_2)$. We know $a \in g_1, g_2, g_4$ for any of the triads giving $K(4)$. Choose a second order object, b, that commutes with a, and then we choose an object c_1 that also commutes with a. We list all possible naming functions below.

$$\begin{aligned}
&(g_1, g_2, g_4, g_3, g_5, h_5, h_6) \quad (g_2, g_1, g_4, g_8, g_9, h_3, h_4) \quad (g_4, g_1, g_2, g_6, g_7, h_1, h_2) \\
&(g_1, g_2, g_4, g_5, g_3, h_6, h_5) \quad (g_2, g_1, g_4, g_9, g_8, h_4, h_3) \quad (g_4, g_1, g_2, g_7, g_6, h_2, h_1) \\
&(g_1, g_2, g_4, h_5, h_6, g_3, g_5) \quad (g_2, g_1, g_4, h_3, h_4, g_8, g_9) \quad (g_4, g_1, g_2, h_1, h_2, g_6, g_7) \\
&(g_1, g_2, g_4, h_6, h_5, g_5, g_3) \quad (g_2, g_1, g_4, h_4, h_3, g_9, g_8) \quad (g_4, g_1, g_2, h_2, h_1, g_7, g_6) \\[6pt]
&(g_1, g_4, g_2, g_3, g_5, h_6, h_5) \quad (g_2, g_4, g_1, g_8, g_9, h_4, h_3) \quad (g_4, g_2, g_1, g_6, g_7, h_2, h_1) \\
&(g_1, g_4, g_2, g_5, g_3, h_5, h_6) \quad (g_2, g_4, g_1, g_9, g_8, h_3, h_4) \quad (g_4, g_2, g_1, g_7, g_6, h_1, h_2) \\
&(g_1, g_4, g_2, h_5, h_6, g_5, g_3) \quad (g_2, g_4, g_1, h_3, h_4, g_9, g_8) \quad (g_4, g_2, g_1, h_1, h_2, g_7, g_6) \\
&(g_1, g_4, g_2, h_6, h_5, g_3, g_5) \quad (g_2, g_4, g_1, h_4, h_3, g_8, g_9) \quad (g_4, g_2, g_1, h_2, h_1, g_6, g_7) \\[6pt]
&(g_1, g_3, g_5, g_2, g_4, h_6, h_5) \quad (g_2, g_8, g_9, g_1, g_4, h_4, h_3) \quad (g_4, g_6, g_7, g_1, g_2, h_2, h_1) \\
&(g_1, g_3, g_5, g_4, g_2, h_5, h_6) \quad (g_2, g_8, g_9, g_4, g_1, h_3, h_4) \quad (g_4, g_6, g_7, g_2, g_1, h_1, h_2) \\
&(g_1, g_3, g_5, h_5, h_6, g_4, g_2) \quad (g_2, g_8, g_9, h_3, h_4, g_4, g_1) \quad (g_4, g_6, g_7, h_1, h_2, g_2, g_1) \\
&(g_1, g_3, g_5, h_6, h_5, g_2, g_4) \quad (g_2, g_8, g_9, h_4, h_3, g_1, g_4) \quad (g_4, g_6, g_7, h_2, h_1, g_1, g_2) \\[6pt]
&(g_1, g_5, g_3, g_2, g_4, h_5, h_6) \quad (g_2, g_9, g_8, g_1, g_4, h_3, h_4) \quad (g_4, g_7, g_6, g_1, g_4, h_1, h_2) \\
&(g_1, g_5, g_3, g_4, g_2, h_6, h_5) \quad (g_2, g_9, g_8, g_4, g_1, h_4, h_3) \quad (g_4, g_7, g_6, g_2, g_1, h_2, h_1) \\
&(g_1, g_5, g_3, h_5, h_6, g_2, g_4) \quad (g_2, g_9, g_8, h_3, h_4, g_1, g_4) \quad (g_4, g_7, g_6, h_1, h_2, g_1, g_2) \\
&(g_1, g_5, g_3, h_6, h_5, g_4, g_2) \quad (g_2, g_9, g_8, h_4, h_3, g_4, g_1) \quad (g_4, g_7, g_6, h_2, h_1, g_2, g_1)
\end{aligned} \quad (21)$$

In (20) we can also observe that given any choice of a, b, x_1 that satisfies $K(4) = \{e, a, b, x_1\}$, there is no object $g \notin K(4)$ that commutes with both a and b. None of our candidate triads satisfy $a*c_1 = c_1*a$ and $b*c_1 = c_1*b$ simultaneously. Although we can not find c_1 that commutes with a and b, we still have to maximize our representation. The next highest object we can have in the position of c_1*b is x_3. Each of the finite sequences above satisfies $a*c_1 = c_1*a$ and $x_3 = c_1*b$. Any one of our naming functions in (21) will give the table

$$\begin{array}{llllllll}
e & a & b & x_1 & c_1 & x_2 & c_2 & x_3 \\
a & e & x_1 & b & x_2 & c_1 \\
b & x_1 & e & a & x_3 & c_2 \\
x_1 & b & a & e & c_2 & x_3 \\
c_1 & x_2 & c_2 & x_3 \\
x_2 & c_1 & x_3 & c_2 \\
c_2 & x_3 & c_1 & x_2 \\
x_3 & c_2 & x_2 & c_1
\end{array}$$

It is possible to choose c_1 with the additional restraint $|c_1| = 2$, maximizing the representation. The naming functions

$$\begin{aligned}
&(g_1, g_2, g_4, g_3, g_5, h_5, h_6) \quad (g_2, g_1, g_4, g_8, g_9, h_3, h_4) \quad (g_4, g_1, g_2, g_6, g_7, h_1, h_2) \\
&(g_1, g_2, g_4, g_5, g_3, h_6, h_5) \quad (g_2, g_1, g_4, g_9, g_8, h_4, h_3) \quad (g_4, g_1, g_2, g_7, g_6, h_2, h_1) \\[6pt]
&(g_1, g_4, g_2, g_3, g_5, h_6, h_5) \quad (g_2, g_4, g_1, g_8, g_9, h_4, h_3) \quad (g_4, g_2, g_1, g_6, g_7, h_2, h_1) \\
&(g_1, g_4, g_2, g_5, g_3, h_5, h_6) \quad (g_2, g_4, g_1, g_9, g_8, h_3, h_4) \quad (g_4, g_2, g_1, g_7, g_6, h_1, h_2) \\[6pt]
&(g_1, g_3, g_5, g_2, g_4, h_6, h_5) \quad (g_2, g_8, g_9, g_1, g_4, h_4, h_3) \quad (g_4, g_6, g_7, g_1, g_2, h_2, h_1) \\
&(g_1, g_3, g_5, g_4, g_2, h_5, h_6) \quad (g_2, g_8, g_9, g_4, g_1, h_3, h_4) \quad (g_4, g_6, g_7, g_2, g_1, h_1, h_2) \\[6pt]
&(g_1, g_5, g_3, g_2, g_4, h_5, h_6) \quad (g_2, g_9, g_8, g_1, g_4, h_3, h_4) \quad (g_4, g_7, g_6, g_1, g_4, h_1, h_2) \\
&(g_1, g_5, g_3, g_4, g_2, h_6, h_5) \quad (g_2, g_9, g_8, g_4, g_1, h_4, h_3) \quad (g_4, g_7, g_6, g_2, g_1, h_2, h_1)
\end{aligned} \quad (22)$$

give the table

$$\begin{array}{cccccccc}
e & a & b & x_1 & c_1 & x_2 & c_2 & x_3 \\
a & e & x_1 & b & x_2 & c_1 & x_3 & c_2 \\
b & x_1 & e & a & x_3 & c_2 & x_2 & c_1 \\
x_1 & b & a & e & c_2 & x_3 & c_1 & x_2 \\
c_1 & x_2 & c_2 & x_3 & e & a & b & x_1 \\
x_2 & c_1 & x_3 & c_2 & a & e & x_1 & b \\
c_2 & x_3 & c_1 & x_2 & x_1 & b & a & e \\
x_3 & c_2 & x_2 & c_1 & b & x_1 & e & a
\end{array}$$

This is the table obtained for the canonical naming of the Dihedral Group D_8. We add a new object d_1 and $x_4 = a * d_1$, $d_2 = b * d_1$, $x_5 = a * d_2$ to the table above, and obtain

$$\begin{array}{cccccccccccc}
e & a & b & x_1 & c_1 & x_2 & c_2 & x_3 & d_1 & x_4 & d_2 & x_5 \\
a & e & x_1 & b & x_2 & c_1 & x_3 & c_2 \\
b & x_1 & e & a & x_3 & c_2 & x_2 & c_1 \\
x_1 & b & a & e & c_2 & x_3 & c_1 & x_2 \\
c_1 & x_2 & c_2 & x_3 & e & a & b & x_1 \\
x_2 & c_1 & x_3 & c_2 & a & e & x_1 & b \\
c_2 & x_3 & c_1 & x_2 & x_1 & b & a & e \\
x_3 & c_2 & x_2 & c_1 & b & x_1 & e & a \\
d_1 & x_4 & d_2 & x_5 \\
x_4 & d_1 & x_5 & d_2 \\
d_2 & x_5 & d_1 & x_4 \\
x_5 & d_2 & x_4 & d_1
\end{array}$$

We find we have to add another new object $p_1 = c_1 * d_1$. Then, we have to add the objects $x_6 = a * p_1$, $p_2 = b * p_1$, $x_7 = a * p_2$.

$$\begin{array}{cccccccccccccccc}
e & a & b & x_1 & c_1 & x_2 & c_2 & x_3 & d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & p_2 & x_7 \\
a & e & x_1 & b & x_2 & c_1 & x_3 & c_2 \\
b & x_1 & e & a & x_3 & c_2 & x_2 & c_1 \\
x_1 & b & a & e & c_2 & x_3 & c_1 & x_2 \\
c_1 & x_2 & c_2 & x_3 & e & a & b & x_1 \\
x_2 & c_1 & x_3 & c_2 & a & e & x_1 & b \\
c_2 & x_3 & c_1 & x_2 & x_1 & b & a & e \\
x_3 & c_2 & x_2 & c_1 & b & x_1 & e & a \\
d_1 & x_4 & d_2 & x_5 & p_1 & x_6 \\
x_4 & d_1 & x_5 & d_2 & x_6 & p_1 \\
d_2 & x_5 & d_1 & x_4 & p_2 & x_7 \\
x_5 & d_2 & x_4 & d_1 & x_7 & p_2 \\
p_1 & x_6 \\
x_6 & p_1 \\
p_2 & x_7 \\
x_7 & p_2
\end{array}$$

Use $|c_1| = 2$ to find $c_1 * p_1 = d_1$, etc. It is not hard to find $c_2 * d_1 = x_7$.

$$\begin{array}{cccccccccccccccc}
e & a & b & x_1 & c_1 & x_2 & c_2 & x_3 & d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & p_2 & x_7 \\
a & e & x_1 & b & x_2 & c_1 & x_3 & c_2 \\
b & x_1 & e & a & x_3 & c_2 & x_2 & c_1 \\
x_1 & b & a & e & c_2 & x_3 & c_1 & x_2 \\
c_1 & x_2 & c_2 & x_3 & e & a & b & x_1 \\
x_2 & c_1 & x_3 & c_2 & a & e & x_1 & b \\
c_2 & x_3 & c_1 & x_2 & x_1 & b & a & e \\
x_3 & c_2 & x_2 & c_1 & b & x_1 & e & a \\
d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & x_7 & p_2 \\
x_4 & d_1 & x_5 & d_2 & x_6 & p_1 & p_2 & x_7 \\
d_2 & x_5 & d_1 & x_4 & p_2 & x_7 & x_6 & p_1 \\
x_5 & d_2 & x_4 & d_1 & x_7 & p_2 & p_1 & x_6 \\
\end{array}$$

$$\begin{array}{cccc}
p_1 & x_6 & \quad d_1 & x_4 \\
x_6 & p_1 & \quad x_4 & d_1 \\
p_2 & x_7 & \quad d_2 & x_5 \\
x_7 & p_2 & \quad x_5 & d_2
\end{array}$$

Now we can use $b = c_2 * c_1$ to find $b * p_1 = x_7$. We similarly find $b * p_2 = x_6$. Finding $c_2 * p_1 = d_2$ is easy using $c_2 = c_1 * x_1$.

$$
\begin{array}{cccccccccccccccc}
e & a & b & x_1 & c_1 & x_2 & c_2 & x_3 & d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & p_2 & x_7 \\
a & e & x_1 & b & x_2 & c_1 & x_3 & c_2 \\
b & x_1 & e & a & x_3 & c_2 & x_2 & c_1 \\
x_1 & b & a & e & c_2 & x_3 & c_1 & x_2 \\
c_1 & x_2 & c_2 & x_3 & e & a & b & x_1 \\
x_2 & c_1 & x_3 & c_2 & a & e & x_1 & b \\
c_2 & x_3 & c_1 & x_2 & x_1 & b & a & e \\
x_3 & c_2 & x_2 & c_1 & b & x_1 & e & a \\
d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & x_7 & p_2 \\
x_4 & d_1 & x_5 & d_2 & x_6 & p_1 & p_2 & x_7 \\
d_2 & x_5 & d_1 & x_4 & p_2 & x_7 & x_6 & p_1 \\
x_5 & d_2 & x_4 & d_1 & x_7 & p_2 & p_1 & x_6 \\
p_1 & x_6 & x_7 & p_2 & d_1 & x_4 & d_2 & x_5 \\
x_6 & p_1 & p_2 & x_7 & x_4 & d_1 & x_5 & d_2 \\
p_2 & x_7 & x_6 & p_1 & d_2 & x_5 & d_1 & x_4 \\
x_7 & p_2 & p_1 & x_6 & x_5 & d_2 & x_4 & d_1 \\
\end{array}
$$

The last table tells us that if we add an object d_1, to any of the naming functions in (22), we will have to add all the objects $(d_1, x_4, d_2, x_5, p_1, x_6, p_2, x_7)$ defined by

$$
\begin{array}{ll}
x_4 = a * d_1 & p_1 = c_1 * d_1 \\
d_2 = b * d_1 & x_6 = a * p_1 \\
x_5 = a * d_2 & p_2 = b * p_1 \\
 & x_7 = a * p_2
\end{array}
$$

How do we choose d_1? If we had any more objects that commute with a, those would be the candidates to d_1. However, in each of our naming functions, there are no more objects that commute with a. The next largest value we can place in $d_1 * a$ is d_2. We see that only some of our naming functions will satisfy this. For example, the naming function with $a = g_1$, $b = g_3$ is disqualified from being a canonical naming function. We can not find a new $d_1 \notin D_8$ such that $d_1 * a = b * d_1$. The only cases when we can find this d_1 is if we have $a, b \in \{g_1, g_2, g_4\}$. The easiest way to find the candidates for d_1, is to compare the row of a and the column of b. If the i-th object in the row of a coincides with the i-th object in the column of b, then the i-th object on the first column (or first row) is a candidate for d_1. For example, with the naming function $(g_1, g_2, g_4, g_3, g_5, h_5, h_6)$, the candidates for d_1 are the objects $g_6, g_7, h_1, h_2, h_9, h_{10}, h_{13}, h_{14}$. The candidates for d_1 are determined by a, b. If $a = g_1$ and $b = g_3$ we have no candidate for d_1. If $a = g_1$ and $b = g_4$ the candidates for d_1 are $g_8, g_9, h_3, h_4, h_7, h_8, h_{11}, h_{12}$, etc. The naming functions that satisfy this condition are those that have a, b in g_1, g_2, g_4. Now we know more about the canonical naming function. We have $K(4) = \{e, g_1, g_2, g_4\}$ as the first four objects of the naming function. Then we have to choose a second order object c_1 that commutes with a. Then we choose d_1 so that $b * d_1 = d_1 * a$. Below we give twelve naming functions. Each of these has eight possible candidates for d_1. We have a total of ninety-six possible naming functions.

$$
\begin{array}{lll}
(g_1, g_2, g_4, g_3, g_5, h_5, h_6, d_1, \ldots, x_7) & (g_2, g_1, g_4, g_8, g_9, h_3, h_4, d_1, \ldots, x_7) & (g_4, g_1, g_2, g_6, g_7, h_1, h_2, d_1, \ldots, x_7) \\
(g_1, g_2, g_4, g_5, g_3, h_6, h_5, d_1, \ldots, x_7) & (g_2, g_1, g_4, g_9, g_8, h_4, h_3, d_1, \ldots, x_7) & (g_4, g_1, g_2, g_7, g_6, h_2, h_1, d_1, \ldots, x_7) \\
\\
(g_1, g_4, g_2, g_3, g_5, h_6, h_5, d_1, \ldots, x_7) & (g_2, g_4, g_1, g_8, g_9, h_4, h_3, d_1, \ldots, x_7) & (g_4, g_2, g_1, g_6, g_7, h_2, h_1, d_1, \ldots, x_7) \\
(g_1, g_4, g_2, g_5, g_3, h_5, h_6, d_1, \ldots, x_7) & (g_2, g_4, g_1, g_9, g_8, h_3, h_4, d_1, \ldots, x_7) & (g_4, g_2, g_1, g_7, g_6, h_1, h_2, d_1, \ldots, x_7)
\end{array}
\tag{23}
$$

Let us reduce the possible choices, further. Some of our candidate naming functions (not all) give us $d_1 * b = a * d_1$, which maximizes the representation. We will keep the naming functions that satisfy $d_1 * b = a * d_1$ and $b * d_1 = d_1 * a$, simultaneously. In the case of $a = g_1$, $b = g_2$ the candidates for d_1 are reduced to g_6, g_7, h_1, h_2.

$$
\begin{array}{cccccccccccccccc}
e & a & b & x_1 & c_1 & x_2 & c_2 & x_3 & d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & p_2 & x_7 \\
a & e & x_1 & b & x_2 & c_1 & x_3 & c_2 & d_2 & x_5 & d_1 & x_4 & p_2 & x_7 & p_1 & x_6 \\
b & x_1 & e & a & x_3 & c_2 & x_2 & c_1 \\
x_1 & b & a & e & c_2 & x_3 & c_1 & x_2 \\
c_1 & x_2 & c_2 & x_3 & e & a & b & x_1 \\
x_2 & c_1 & x_3 & c_2 & a & e & x_1 & b \\
c_2 & x_3 & c_1 & x_2 & x_1 & b & a & e \\
x_3 & c_2 & x_2 & c_1 & b & x_1 & e & a \\
d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & x_7 & p_2 \\
x_4 & d_1 & x_5 & d_2 & x_6 & p_1 & p_2 & x_7 \\
d_2 & x_5 & d_1 & x_4 & p_2 & x_7 & x_6 & p_1 \\
x_5 & d_2 & x_4 & d_1 & x_7 & p_2 & p_1 & x_6 \\
p_1 & x_6 & x_7 & p_2 & d_1 & x_4 & d_2 & x_5 \\
x_6 & p_1 & p_2 & x_7 & x_4 & d_1 & x_5 & d_2 \\
p_2 & x_7 & x_6 & p_1 & d_2 & x_5 & d_1 & x_4 \\
x_7 & p_2 & p_1 & x_6 & x_5 & d_2 & x_4 & d_1
\end{array}
$$

The naming functions $(a, b, x_1, c_1, x_2, c_2, x_3, d_1, x_4, d_2, x_5)$, without the components (p_1, x_6, p_2, x_7) are given below.

$(g_1, g_2, g_4, g_3, g_5, h_5, h_6, g_6, h_1, h_2, g_7, h_7, h_{11}, h_8, h_{12})$ $(g_2, g_1, g_4, g_8, g_9, h_3, h_4, g_6, h_2, h_1, g_7, h_{13}, h_{10}, h_9, h_{14})$
$(g_1, g_2, g_4, g_3, g_5, h_5, h_6, g_7, h_2, h_1, g_6, h_8, h_{12}, h_7, h_{11})$ $(g_2, g_1, g_4, g_8, g_9, h_3, h_4, g_7, h_1, h_2, g_6, h_9, h_{14}, h_{13}, h_{10})$
$(g_1, g_2, g_4, g_3, g_5, h_5, h_6, h_1, g_6, g_7, h_2, h_{11}, h_7, h_8, h_{12})$ $(g_2, g_1, g_4, g_8, g_9, h_3, h_4, h_1, g_7, g_6, h_2, h_{14}, h_9, h_{13}, h_{10})$
$(g_1, g_2, g_4, g_3, g_5, h_5, h_6, h_2, g_7, g_6, h_1, h_{12}, h_8, h_7, h_{11})$ $(g_2, g_1, g_4, g_8, g_9, h_3, h_4, h_2, g_6, g_7, h_1, h_{10}, h_{13}, h_{14}, h_9)$

$(g_1, g_2, g_4, g_5, g_3, h_6, h_5, g_6, h_1, h_2, g_7, h_{11}, h_7, h_{12}, h_8)$ $(g_2, g_1, g_4, g_9, g_8, h_4, h_3, g_6, h_2, h_1, g_7, h_{10}, h_{13}, h_{14}, h_9)$
$(g_1, g_2, g_4, g_5, g_3, h_6, h_5, g_7, h_2, h_1, g_6, h_{12}, h_8, h_7, h_{11})$ $(g_2, g_1, g_4, g_9, g_8, h_4, h_3, g_7, h_1, h_2, g_6, h_{14}, h_9, h_{10}, h_{13})$
$(g_1, g_2, g_4, g_5, g_3, h_6, h_5, h_1, g_6, g_7, h_2, h_7, h_{11}, h_8, h_{12})$ $(g_2, g_1, g_4, g_9, g_8, h_4, h_3, h_1, g_7, g_6, h_2, h_9, h_{14}, h_{13}, h_{10})$
$(g_1, g_2, g_4, g_5, g_3, h_6, h_5, h_2, g_7, g_6, h_1, h_8, h_{12}, h_7, h_{11})$ $(g_2, g_1, g_4, g_9, g_8, h_4, h_3, h_2, g_6, g_7, h_1, h_{13}, h_{10}, h_9, h_{14})$

$(g_1, g_4, g_2, g_3, g_5, h_5, h_6, g_8, h_3, h_4, g_9, h_9, h_{13}, h_{10}, h_{14})$ $(g_2, g_4, g_1, g_8, g_9, h_3, h_4, g_3, h_5, h_6, g_5, h_8, h_7, h_{11}, h_{12})$
$(g_1, g_4, g_2, g_3, g_5, h_5, h_6, g_9, h_4, h_3, g_8, h_{10}, h_{14}, h_9, h_{13})$ $(g_2, g_4, g_1, g_8, g_9, h_3, h_4, g_5, h_6, h_5, g_3, h_{11}, h_{12}, h_8, h_7)$
$(g_1, g_4, g_2, g_3, g_5, h_5, h_6, h_3, g_8, g_9, h_4, h_{13}, h_9, h_{14}, h_{10})$ $(g_2, g_4, g_1, g_8, g_9, h_3, h_4, h_5, g_3, g_5, h_6, h_7, h_8, h_{12}, h_{11})$
$(g_1, g_4, g_2, g_3, g_5, h_5, h_6, h_4, g_9, g_8, h_3, h_{14}, h_{10}, h_9, h_{13})$ $(g_2, g_4, g_1, g_8, g_9, h_3, h_4, h_6, g_5, g_3, h_5, h_{12}, h_{11}, h_7, h_8)$

$(g_1, g_4, g_2, g_5, g_3, h_6, h_5, g_8, h_3, h_4, g_9, h_{13}, h_9, h_{14}, h_{10})$ $(g_2, g_4, g_1, g_9, g_8, h_4, h_3, g_3, h_5, h_6, g_5, h_7, h_8, h_{12}, h_{11})$
$(g_1, g_4, g_2, g_5, g_3, h_6, h_5, g_9, h_4, h_3, g_8, h_{14}, h_{10}, h_{13}, h_9)$ $(g_2, g_4, g_1, g_9, g_8, h_4, h_3, g_5, h_6, h_5, g_3, h_{12}, h_{11}, h_7, h_8)$
$(g_1, g_4, g_2, g_5, g_3, h_6, h_5, h_3, g_8, g_9, h_4, h_9, h_{13}, h_{10}, h_{14})$ $(g_2, g_4, g_1, g_9, g_8, h_4, h_3, h_5, g_3, g_5, h_6, h_8, h_7, h_{11}, h_{12})$
$(g_1, g_4, g_2, g_5, g_3, h_6, h_5, h_4, g_9, g_8, h_3, h_{10}, h_{14}, h_9, h_{13})$ $(g_2, g_4, g_1, g_9, g_8, h_4, h_3, h_6, g_5, g_3, h_5, h_{11}, h_{12}, h_8, h_7)$

$(g_4, g_1, g_2, g_6, g_7, h_1, h_2, g_8, h_4, h_3, g_9, h_{11}, h_8, h_7, h_{12})$
$(g_4, g_1, g_2, g_6, g_7, h_1, h_2, g_9, h_3, h_4, g_8, h_7, h_{12}, h_{11}, h_8)$
$(g_4, g_1, g_2, g_6, g_7, h_1, h_2, h_3, g_9, g_8, h_4, h_{12}, h_7, h_8, h_{11})$
$(g_4, g_1, g_2, g_6, g_7, h_1, h_2, h_4, g_8, g_9, h_3, h_8, h_{11}, h_{12}, h_7)$

$(g_4, g_1, g_2, g_7, g_6, h_2, h_1, g_8, h_4, h_3, g_9, h_8, h_{11}, h_{12}, h_7)$
$(g_4, g_1, g_2, g_7, g_6, h_2, h_1, g_9, h_3, h_4, g_8, h_{12}, h_7, h_8, h_{11})$
$(g_4, g_1, g_2, g_7, g_6, h_2, h_1, h_3, g_9, g_8, h_4, h_7, h_{12}, h_{11}, h_8)$
$(g_4, g_1, g_2, g_7, g_6, h_2, h_1, h_4, g_8, g_9, h_3, h_{11}, h_8, h_7, h_{12})$

(24)

$(g_4, g_2, g_1, g_6, g_7, h_1, h_2, g_3, h_6, h_5, g_5, h_{10}, h_9, h_{13}, h_{14})$
$(g_4, g_2, g_1, g_6, g_7, h_1, h_2, g_5, h_5, h_6, g_3, h_{13}, h_{14}, h_{10}, h_9)$
$(g_4, g_2, g_1, g_6, g_7, h_1, h_2, h_5, g_5, g_3, h_6, h_{14}, h_{13}, h_9, h_{10})$
$(g_4, g_2, g_1, g_6, g_7, h_1, h_2, h_6, g_3, g_5, h_5, h_9, h_{10}, h_{14}, h_{13})$

$(g_4, g_2, g_1, g_7, g_6, h_2, h_1, g_3, h_6, h_5, g_5, h_9, h_{10}, h_{14}, h_{13})$
$(g_4, g_2, g_1, g_7, g_6, h_2, h_1, g_5, h_5, h_6, g_3, h_{14}, h_{13}, h_9, h_{10})$
$(g_4, g_2, g_1, g_7, g_6, h_2, h_1, h_5, g_5, g_3, h_6, h_{13}, h_{14}, h_{10}, h_9)$
$(g_4, g_2, g_1, g_7, g_6, h_2, h_1, h_6, g_3, g_5, h_5, h_{10}, h_9, h_{13}, h_{14})$

The careful reader will start to notice what objects might turn out to be equivalent objects. For example, it is quite clear g_1, g_2, g_4 might probably be equivalent, but also g_3, g_5 and g_6, g_7 and h_1, h_2, etc. We shall see how we can reduce our possible choices. The table we have up to this point is

$$
\begin{array}{llllllllllllllll}
e & a & b & x_1 & c_1 & x_2 & c_2 & x_3 & d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & p_2 & x_7 \\
a & e & x_1 & b & x_2 & c_1 & x_3 & c_2 & d_2 & x_5 & d_1 & x_4 & p_2 & x_7 & p_1 & x_6 \\
b & x_1 & e & a & x_3 & c_2 & x_2 & c_1 & x_4 & d_1 & x_5 & d_2 & x_6 & p_1 & x_7 & p_2 \\
x_1 & b & a & e & c_2 & x_3 & c_1 & x_2 & x_5 & d_2 & x_4 & d_1 & x_7 & p_2 & x_6 & p_1 \\
c_1 & x_2 & c_2 & x_3 & e & a & b & x_1 \\
x_2 & c_1 & x_3 & c_2 & a & e & x_1 & b \\
c_2 & x_3 & c_1 & x_2 & x_1 & b & a & e \\
x_3 & c_2 & x_2 & c_1 & b & x_1 & e & a \\
d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & x_7 & p_2 \\
x_4 & d_1 & x_5 & d_2 & x_6 & p_1 & p_2 & x_7 \\
d_2 & x_5 & d_1 & x_4 & p_2 & x_7 & x_6 & p_1 \\
x_5 & d_2 & x_4 & d_1 & x_7 & p_2 & p_1 & x_6 \\
p_1 & x_6 & x_7 & p_2 & d_1 & x_4 & d_2 & x_5 \\
x_6 & p_1 & p_2 & x_7 & x_4 & d_1 & x_5 & d_2 \\
p_2 & x_7 & x_6 & p_1 & d_2 & x_5 & d_1 & x_4 \\
x_7 & p_2 & p_1 & x_6 & x_5 & d_2 & x_4 & d_1
\end{array}
$$

The naming functions of (24) all give a new object $d_1 * c_1$. For example, in the naming function $(g_1, g_2, g_4, g_3, g_5, h_5, h_6, g_6, h_1, h_2, g_7)$, we have $d_1 * c_1 = g_6 * g_3 = h_{10}$ which is an object not yet named. Including this new object, $q_1 = d_1 * c_1$, gives the table

$$
\begin{array}{llllllllllllllllll}
e & a & b & x_1 & c_1 & x_2 & c_2 & x_3 & d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & p_2 & x_7 & q_1 & x_8 & q_2 & x_9 \\
a & e & x_1 & b & x_2 & c_1 & x_3 & c_2 & d_2 & x_5 & d_1 & x_4 & p_2 & x_7 & p_1 & x_6 & x_8 & q_1 & x_9 & q_2 \\
b & x_1 & e & a & x_3 & c_2 & x_2 & c_1 & x_4 & d_1 & x_5 & d_2 & x_6 & p_1 & x_7 & p_2 & x_9 & q_2 & x_8 & q_1 \\
x_1 & b & a & e & c_2 & x_3 & c_1 & x_2 & x_5 & d_2 & x_4 & d_1 & x_7 & p_2 & x_6 & p_1 & q_2 & x_9 & q_1 & x_8 \\
c_1 & x_2 & c_2 & x_3 & e & a & b & x_1 & q_1 & x_8 & q_2 & x_9 & & & & & d_1 & x_4 & d_2 & x_5 \\
x_2 & c_1 & x_3 & c_2 & a & e & x_1 & b & q_2 & x_9 & q_1 & x_8 & & & & & d_2 & x_5 & d_1 & x_4 \\
c_2 & x_3 & c_1 & x_2 & x_1 & b & a & e & x_8 & q_1 & x_9 & q_2 & & & & & x_5 & d_2 & x_4 & d_1 \\
x_3 & c_2 & x_2 & c_1 & b & x_1 & e & a & x_9 & q_2 & x_8 & q_1 & & & & & x_4 & d_1 & x_5 & d_2 \\
d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & x_7 & p_2 \\
x_4 & d_1 & x_5 & d_2 & x_6 & p_1 & p_2 & x_7 \\
d_2 & x_5 & d_1 & x_4 & p_2 & x_7 & x_6 & p_1 \\
x_5 & d_2 & x_4 & d_1 & x_7 & p_2 & p_1 & x_6 \\
p_1 & x_6 & x_7 & p_2 & d_1 & x_4 & d_2 & x_5 \\
x_6 & p_1 & p_2 & x_7 & x_4 & d_1 & x_5 & d_2 \\
p_2 & x_7 & x_6 & p_1 & d_2 & x_5 & d_1 & x_4 \\
x_7 & p_2 & p_1 & x_6 & x_5 & d_2 & x_4 & d_1 \\
q_1 & x_8 & q_2 & x_9 \\
x_8 & q_1 & x_9 & q_2 \\
q_2 & x_9 \\
x_9 & q_2
\end{array}
$$

This last table tells us that if we want to maximize the representation, we will have to consider the naming functions that have $|d_1| = 2$. These are

$(g_1, g_2, g_4, g_3, g_5, h_5, h_6, g_6, h_1, h_2, g_7, h_7, h_{11}, h_8, h_{12}, h_{10}, h_{14}, h_{13}, h_9)$ $(g_1, g_4, g_2, g_3, g_5, h_5, h_6, g_8, h_3, h_4, g_9, h_9, h_{13}, h_{10}, h_{14}, h_8, h_{12}, h_{11}, h_7)$
$(g_1, g_2, g_4, g_3, g_5, h_5, h_6, g_7, h_2, h_1, g_6, h_8, h_{12}, h_7, h_{11}, h_9, h_{13}, h_{14}, h_{10})$ $(g_1, g_4, g_2, g_3, g_5, h_5, h_6, g_9, h_4, h_3, g_8, h_{10}, h_{14}, h_9, h_{13}, h_7, h_{11}, h_{12}, h_8)$
$(g_1, g_2, g_4, g_5, g_3, h_6, h_5, g_6, h_1, h_2, g_7, h_{11}, h_7, h_{12}, h_8, h_{13}, h_9, h_{10}, h_{14})$ $(g_1, g_4, g_2, g_5, g_3, h_6, h_5, g_8, h_3, h_4, g_9, h_{13}, h_9, h_{14}, h_{10}, h_{11}, h_7, h_8, h_{12})$
$(g_1, g_2, g_4, g_5, g_3, h_6, h_5, g_7, h_2, h_1, g_6, h_{12}, h_8, h_7, h_{11}, h_{14}, h_{10}, h_{13}, h_9)$ $(g_1, g_4, g_2, g_5, g_3, h_6, h_5, g_9, h_4, h_3, g_8, h_{14}, h_{13}, h_{10}, h_9, h_{12}, h_8, h_7, h_{11})$

$(g_2, g_1, g_4, g_8, g_9, h_3, h_4, g_6, h_2, h_1, g_7, h_{13}, h_{10}, h_9, h_{14}, h_{11}, h_{12}, h_7, h_8)$ $(g_2, g_4, g_1, g_8, g_9, h_3, h_4, g_3, h_5, h_6, g_5, h_8, h_7, h_{11}, h_{12}, h_9, h_{14}, h_{10}, h_{13})$
$(g_2, g_1, g_4, g_8, g_9, h_3, h_4, g_7, h_1, h_2, g_6, h_9, h_{14}, h_{13}, h_{10}, h_8, h_7, h_{12}, h_{11})$ $(g_2, g_4, g_1, g_8, g_9, h_3, h_4, g_5, h_6, h_5, g_3, h_{11}, h_{12}, h_8, h_7, h_{13}, h_{10}, h_{14}, h_9)$
$(g_2, g_1, g_4, g_9, g_8, h_4, h_3, g_6, h_2, h_1, g_7, h_{10}, h_{13}, h_{14}, h_9, h_7, h_8, h_{11}, h_{12})$ $(g_2, g_4, g_1, g_9, g_8, h_4, h_3, g_3, h_5, h_6, g_5, h_7, h_8, h_{12}, h_{11}, h_{10}, h_{13}, h_9, h_{14})$
$(g_2, g_1, g_4, g_9, g_8, h_4, h_3, g_7, h_1, h_2, g_6, h_{14}, h_9, h_{10}, h_{13}, h_{12}, h_{11}, h_8, h_7)$ $(g_2, g_4, g_1, g_9, g_8, h_4, h_3, g_5, h_6, h_5, g_3, h_{12}, h_{11}, h_7, h_8, h_{14}, h_9, h_{13}, h_{10})$

$(g_4, g_1, g_2, g_6, g_7, h_1, h_2, g_8, h_4, h_3, g_9, h_{11}, h_8, h_7, h_{12}, h_{13}, h_{14}, h_9, h_{10})$ $(g_4, g_2, g_1, g_6, g_7, h_1, h_2, g_3, h_6, h_5, g_5, h_{10}, h_9, h_{13}, h_{14}, h_7, h_{12}, h_8, h_{11})$
$(g_4, g_1, g_2, g_6, g_7, h_1, h_2, g_9, h_3, h_4, g_8, h_7, h_{12}, h_{11}, h_8, h_{10}, h_9, h_{14}, h_{13})$ $(g_4, g_2, g_1, g_6, g_7, h_1, h_2, g_5, h_5, h_6, g_3, h_{13}, h_{14}, h_{10}, h_9, h_{11}, h_8, h_7, h_{12})$
$(g_4, g_1, g_2, g_7, g_6, h_2, h_1, g_8, h_4, h_3, g_9, h_8, h_{11}, h_{12}, h_7, h_9, h_{10}, h_{13}, h_{14})$ $(g_4, g_2, g_1, g_7, g_6, h_2, h_1, g_3, h_6, h_5, g_5, h_9, h_{10}, h_{14}, h_{13}, h_8, h_{11}, h_7, h_{14})$
$(g_4, g_1, g_2, g_7, g_6, h_2, h_1, g_9, h_3, h_4, g_8, h_{12}, h_7, h_8, h_{11}, h_{14}, h_{13}, h_{10}, h_9)$ $(g_4, g_2, g_1, g_7, g_6, h_2, h_1, g_5, h_5, h_6, g_3, h_{14}, h_{13}, h_9, h_{10}, h_{12}, h_7, h_{11}, h_8)$

These naming functions give the table

$$
\begin{array}{llllllllllllllllllllllll}
e & a & b & x_1 & c_1 & x_2 & c_2 & x_3 & d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & p_2 & x_7 & q_1 & x_8 & q_2 & x_9 \\
a & e & x_1 & b & x_2 & c_1 & x_3 & c_2 & d_2 & x_5 & d_1 & x_4 & p_2 & x_7 & p_1 & x_6 & x_8 & q_1 & x_9 & q_2 \\
b & x_1 & e & a & x_3 & c_2 & x_2 & c_1 & x_4 & d_1 & x_5 & d_2 & x_6 & p_1 & x_7 & p_2 & x_9 & q_2 & x_8 & q_1 \\
x_1 & b & a & e & c_2 & x_3 & c_1 & x_2 & x_5 & d_2 & x_4 & d_1 & x_7 & p_2 & x_6 & p_1 & q_2 & x_9 & q_1 & x_8
\end{array}
$$

$$
\begin{array}{lllllllllll}
c_1 & x_2 & c_2 & x_3 & e & a & b & x_1 & q_1 & x_8 & q_2 & x_9 \\
x_2 & c_1 & x_3 & c_2 & a & e & x_1 & b & q_2 & x_9 & q_1 & x_8 \\
c_2 & x_3 & c_1 & x_2 & x_1 & b & a & e & x_8 & q_1 & x_9 & q_2 \\
x_3 & c_2 & x_2 & c_1 & b & x_1 & e & a & x_9 & q_2 & x_8 & q_1
\end{array}
\qquad
\begin{array}{llll}
d_1 & x_4 & d_2 & x_5 \\
d_2 & x_5 & d_1 & x_4 \\
x_5 & d_2 & x_4 & d_1 \\
x_4 & d_1 & x_5 & d_2
\end{array}
$$

$$
\begin{array}{llllllllllllll}
d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & x_7 & p_2 & e & a & b & x_1 & c_1 & x_2 & x_3 & c_2 \\
x_4 & d_1 & x_5 & d_2 & x_6 & p_1 & p_2 & x_7 & b & x_1 & e & a & x_3 & c_2 & c_1 & x_2 \\
d_2 & x_5 & d_1 & x_4 & p_2 & x_7 & x_6 & p_1 & a & e & x_1 & b & x_2 & c_1 & c_2 & x_3 \\
x_5 & d_2 & x_4 & d_1 & x_7 & p_2 & p_1 & x_6 & x_1 & b & a & e & c_2 & x_3 & x_3 & c_2
\end{array}
$$

$$
\begin{array}{lllllll}
p_1 & x_6 & x_7 & p_2 & d_1 & x_4 & d_2 & x_5 \\
x_6 & p_1 & p_2 & x_7 & x_4 & d_1 & x_5 & d_2 \\
p_2 & x_7 & x_6 & p_1 & d_2 & x_5 & d_1 & x_4 \\
x_7 & p_2 & p_1 & x_6 & x_5 & d_2 & x_4 & d_1
\end{array}
\qquad
\begin{array}{llll}
e & a & b & x_1 \\
b & x_1 & e & a \\
a & e & x_1 & b \\
x_1 & b & a & e
\end{array}
$$

$$
\begin{array}{llll}
q_1 & x_8 & q_2 & x_9 \\
x_8 & q_1 & x_9 & q_2 \\
q_2 & x_9 & q_1 & x_8 \\
x_9 & q_2 & x_8 & q_1
\end{array}
\qquad
\begin{array}{lllllll}
c_1 & x_2 & c_2 & x_3 & e & a & x_1 & b \\
c_2 & x_3 & c_1 & x_2 & x_1 & b & e & a \\
x_2 & c_1 & x_3 & c_2 & a & e & b & x_1 \\
x_3 & c_2 & x_2 & c_1 & b & x_1 & a & e
\end{array}
$$

We see that we have to add a new object $r_1 = c_1 * q_1$. We finally have $x_{10} = a * r_1$, $r_2 = b * r_1$, $x_{11} = a * r_2$. This completes our naming functions.

$$
\begin{aligned}
&(g_1, g_2, g_4, g_3, g_5, h_5, h_6, g_6, h_1, h_2, g_7, h_7, h_{11}, h_8, h_{12}, h_{10}, h_{14}, h_{13}, h_9, g_9, h_4, g_8, h_3) \\
&(g_1, g_2, g_4, g_3, g_5, h_5, h_6, g_7, h_2, h_1, g_6, h_8, h_{12}, h_7, h_{11}, h_9, h_{13}, h_{14}, h_{10}, g_8, h_3, g_9, h_4) \\
&(g_1, g_2, g_4, g_5, g_3, h_6, h_5, g_6, h_1, h_2, g_7, h_{11}, h_7, h_{12}, h_8, h_{13}, h_9, h_{10}, h_{14}, g_8, h_3, g_9, h_4) \\
&(g_1, g_2, g_4, g_5, g_3, h_6, h_5, g_7, h_2, h_1, g_6, h_{12}, h_8, h_7, h_{11}, h_{14}, h_{10}, h_{13}, h_9, g_9, h_4, g_8, h_3) \\
&(g_1, g_4, g_2, g_3, g_5, h_5, h_6, g_8, h_3, h_4, g_9, h_9, h_{13}, h_{10}, h_{14}, h_8, h_{12}, h_{11}, h_7, g_7, h_2, g_6, h_1) \\
&(g_1, g_4, g_2, g_3, g_5, h_5, h_6, g_9, h_4, h_3, g_8, h_{10}, h_{14}, h_9, h_{13}, h_7, h_{11}, h_{12}, h_8, g_6, h_1, g_7, h_2) \\
&(g_1, g_4, g_2, g_5, g_3, h_6, h_5, g_8, h_3, h_4, g_9, h_{13}, h_9, h_{14}, h_{10}, h_{11}, h_7, h_8, h_{12}, g_6, h_1, g_7, h_2) \\
&(g_1, g_4, g_2, g_5, g_3, h_6, h_5, g_9, h_4, h_3, g_8, h_{14}, h_{13}, h_{10}, h_9, h_{12}, h_8, h_7, h_{11}, g_7, h_2, g_6, h_1)
\end{aligned}
$$

$$
\begin{aligned}
&(g_2, g_1, g_4, g_8, g_9, h_3, h_4, g_6, h_2, h_1, g_7, h_{13}, h_{10}, h_9, h_{14}, h_{11}, h_{12}, h_7, h_8, g_5, h_6, g_3, h_5) \\
&(g_2, g_1, g_4, g_8, g_9, h_3, h_4, g_7, h_1, h_2, g_6, h_9, h_{14}, h_{13}, h_{10}, h_8, h_7, h_{12}, h_{11}, g_3, h_5, g_5, h_6) \\
&(g_2, g_1, g_4, g_9, g_8, h_4, h_3, g_6, h_2, h_1, g_7, h_{10}, h_{13}, h_{14}, h_9, h_7, h_8, h_{11}, h_{12}, g_3, h_5, g_5, h_6) \\
&(g_2, g_1, g_4, g_9, g_8, h_4, h_3, g_7, h_1, h_2, g_6, h_{14}, h_9, h_{10}, h_{13}, h_{12}, h_{11}, h_8, h_7, g_5, h_6, g_3, h_5) \\
&(g_2, g_4, g_1, g_8, g_9, h_3, h_4, g_3, h_5, h_6, g_5, h_8, h_7, h_{11}, h_{12}, h_9, h_{14}, h_{10}, h_{13}, g_7, h_1, g_6, h_2) \\
&(g_2, g_4, g_1, g_8, g_9, h_3, h_4, g_5, h_6, h_5, g_3, h_{11}, h_{12}, h_8, h_7, h_{13}, h_{10}, h_{14}, h_9, g_6, h_2, g_7, h_1) \\
&(g_2, g_4, g_1, g_9, g_8, h_4, h_3, g_3, h_5, h_6, g_5, h_7, h_8, h_{12}, h_{11}, h_{10}, h_{13}, h_9, h_{14}, g_6, h_2, g_7, h_1) \\
&(g_2, g_4, g_1, g_9, g_8, h_4, h_3, g_5, h_6, h_5, g_3, h_{12}, h_{11}, h_7, h_8, h_{14}, h_9, h_{13}, h_{10}, g_7, h_1, g_6, h_2)
\end{aligned}
$$

$$
\begin{aligned}
&(g_4, g_1, g_2, g_6, g_7, h_1, h_2, g_8, h_4, h_3, g_9, h_{11}, h_8, h_7, h_{12}, h_{13}, h_{14}, h_9, h_{10}, g_5, h_5, g_3, h_6) \\
&(g_4, g_1, g_2, g_6, g_7, h_1, h_2, g_9, h_3, h_4, g_8, h_7, h_{12}, h_{11}, h_8, h_{10}, h_9, h_{14}, h_{13}, g_3, h_6, g_5, h_5) \\
&(g_4, g_1, g_2, g_7, g_6, h_2, h_1, g_8, h_4, h_3, g_9, h_8, h_{11}, h_{12}, h_7, h_9, h_{10}, h_{13}, h_{14}, g_3, h_6, g_5, h_5) \\
&(g_4, g_1, g_2, g_7, g_6, h_2, h_1, g_9, h_3, h_4, g_8, h_{12}, h_7, h_8, h_{11}, h_{14}, h_{13}, h_{10}, h_9, g_5, h_5, g_3, h_6) \\
&(g_4, g_2, g_1, g_6, g_7, h_1, h_2, g_3, h_6, h_5, g_5, h_{10}, h_9, h_{13}, h_{14}, h_7, h_{12}, h_8, h_{11}, g_9, h_3, g_8, h_4) \\
&(g_4, g_2, g_1, g_6, g_7, h_1, h_2, g_5, h_5, h_6, g_3, h_{13}, h_{14}, h_{10}, h_9, h_{11}, h_8, h_7, h_{12}, g_8, h_4, g_9, h_3) \\
&(g_4, g_2, g_1, g_7, g_6, h_2, h_1, g_3, h_6, h_5, g_5, h_9, h_{10}, h_{14}, h_{13}, h_8, h_{11}, h_7, h_{14}, g_8, h_4, g_9, h_3) \\
&(g_4, g_2, g_1, g_7, g_6, h_2, h_1, g_5, h_5, h_6, g_3, h_{14}, h_{13}, h_9, h_{10}, h_{12}, h_7, h_{11}, h_8, g_9, h_3, g_8, h_4)
\end{aligned}
$$

We have found the canonical naming function of the permutation group Δ_4. We have also been able to identify equivalent objects of the group. The equivalence classes of objects are

$$
\begin{gathered}
\{e\} \\
\{g_1, g_2, g_4\} \\
\{g_3, g_5, g_6, g_7, g_8, g_9\} \\
\{h_1, h_2, h_3, h_4, h_5, h_6,\} \\
\{h_7, h_8, h_9, h_{10}, h_{11}, h_{12}, h_{13}, h_{14}\}
\end{gathered}
$$

There is a total of twenty four canonical naming functions and automorphisms of Δ_4. The naming functions above give us the canonical table in block form.

$$
\begin{array}{cccccccccccccccccccccccc}
e & a & b & x_1 & c_1 & x_2 & c_2 & x_3 & d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & p_2 & x_7 & q_1 & x_8 & q_2 & x_9 & r_1 & x_{10} & r_2 & x_{11} \\
a & e & x_1 & b & x_2 & c_1 & x_3 & c_2 & d_2 & x_5 & d_1 & x_4 & p_2 & x_7 & p_1 & x_6 & x_8 & q_1 & x_9 & q_2 & x_{10} & r_1 & x_{11} & r_2 \\
b & x_1 & e & a & x_3 & c_2 & x_2 & c_1 & x_4 & d_1 & x_5 & d_2 & x_6 & p_1 & x_7 & p_2 & x_9 & q_2 & x_8 & q_1 & r_2 & x_{11} & r_1 & x_{10} \\
x_1 & b & a & e & c_2 & x_3 & c_1 & x_2 & x_5 & d_2 & x_4 & d_1 & x_7 & p_2 & x_6 & p_1 & q_2 & x_9 & q_1 & x_8 & x_{11} & r_2 & x_{10} & r_1 \\
c_1 & x_2 & c_2 & x_3 & e & a & b & x_1 & q_1 & x_8 & q_2 & x_9 & r_1 & x_{10} & x_{11} & r_2 & d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & x_7 & p_2 \\
x_2 & c_1 & x_3 & c_2 & a & e & x_1 & b & q_2 & x_9 & q_1 & x_8 & x_{11} & r_2 & r_1 & x_{10} & d_2 & x_5 & d_1 & x_4 & p_2 & x_7 & x_6 & p_1 \\
c_2 & x_3 & c_1 & x_2 & x_1 & b & a & e & x_8 & q_1 & x_9 & q_2 & x_{10} & r_1 & r_2 & x_{11} & x_5 & d_2 & x_4 & d_1 & x_7 & p_2 & p_1 & x_6 \\
x_3 & c_2 & x_2 & c_1 & b & x_1 & e & a & x_9 & q_2 & x_8 & q_1 & r_2 & x_{11} & x_{10} & r_1 & x_4 & d_1 & x_5 & d_2 & x_6 & p_1 & p_2 & x_7 \\
d_1 & x_4 & d_2 & x_5 & p_1 & x_6 & x_7 & p_2 & e & a & b & x_1 & c_1 & x_2 & x_3 & c_2 & r_1 & x_{10} & r_2 & x_{11} & q_1 & x_8 & q_2 & x_9 \\
x_4 & d_1 & x_5 & d_2 & x_6 & p_1 & p_2 & x_7 & b & x_1 & e & a & x_3 & c_2 & c_1 & x_2 & r_2 & x_{11} & x_{10} & r_1 & x_9 & q_2 & x_8 & q_1 \\
d_2 & x_5 & d_1 & x_4 & p_2 & x_7 & x_6 & p_1 & a & e & x_1 & b & x_2 & c_1 & c_2 & x_3 & x_{11} & r_2 & r_1 & x_{10} & q_2 & x_9 & q_1 & x_8 \\
x_5 & d_2 & x_4 & d_1 & x_7 & p_2 & p_1 & x_6 & x_1 & b & a & e & c_2 & x_3 & x_3 & c_2 & x_{10} & r_1 & x_{11} & r_2 & x_8 & q_1 & x_9 & q_2 \\
p_1 & x_6 & x_7 & p_2 & d_1 & x_4 & d_2 & x_5 & r_1 & x_{10} & r_2 & x_{11} & q_1 & x_8 & q_2 & x_9 & e & a & b & x_1 & c_1 & x_2 & c_2 & x_3 \\
x_6 & p_1 & p_2 & x_7 & x_4 & d_1 & x_5 & d_2 & r_2 & x_{11} & r_1 & x_{10} & x_9 & q_2 & q_1 & x_8 & b & x_1 & e & a & x_3 & c_2 & x_2 & c_1 \\
p_2 & x_7 & x_6 & p_1 & d_2 & x_5 & d_1 & x_4 & x_{11} & r_2 & x_{10} & r_1 & q_2 & x_9 & x_8 & q_1 & a & e & x_1 & b & x_2 & c_1 & x_3 & c_2 \\
x_7 & p_2 & p_1 & x_6 & x_5 & d_2 & x_4 & d_1 & x_{10} & r_1 & x_{11} & r_2 & x_8 & q_1 & x_9 & q_2 & x_1 & b & a & e & c_2 & x_3 & c_1 & x_2 \\
q_1 & x_8 & q_2 & x_9 & r_1 & x_{10} & r_2 & x_{11} & c_1 & x_2 & c_2 & x_3 & e & a & x_1 & b & p_1 & x_6 & p_2 & x_7 & d_1 & x_4 & d_2 & x_5 \\
x_8 & q_1 & x_9 & q_2 & x_{10} & r_1 & x_{11} & r_2 & c_2 & x_3 & c_1 & x_2 & x_1 & b & e & a & x_7 & p_2 & p_1 & x_6 & x_5 & d_2 & x_4 & d_1 \\
q_2 & x_9 & q_1 & x_8 & x_{11} & r_2 & x_{10} & r_1 & x_2 & c_1 & x_3 & c_2 & a & e & b & x_1 & p_2 & x_7 & x_6 & p_1 & d_2 & x_5 & d_1 & x_4 \\
x_9 & q_2 & x_8 & q_1 & r_2 & x_{11} & r_1 & x_{10} & x_3 & c_2 & x_2 & c_1 & b & x_1 & a & e & x_6 & p_1 & x_7 & p_2 & x_4 & d_1 & x_5 & d_2 \\
r_1 & x_{10} & r_2 & x_{11} & q_1 & x_8 & q_2 & x_9 & p_1 & x_6 & p_2 & x_7 & d_1 & x_4 & d_2 & x_5 & c_1 & x_2 & c_2 & x_3 & e & a & b & x_1 \\
x_{10} & r_1 & x_{11} & r_2 & x_8 & q_1 & x_9 & q_2 & p_2 & x_7 & x_6 & p_1 & d_2 & x_5 & d_1 & x_4 & x_2 & c_1 & x_3 & c_2 & a & e & x_1 & b \\
r_2 & x_{11} & r_1 & x_{10} & x_9 & q_2 & x_8 & q_1 & x_6 & p_1 & x_7 & p_2 & x_4 & d_1 & x_5 & d_2 & x_3 & c_2 & x_2 & c_1 & b & x_1 & e & a \\
x_{11} & r_2 & x_{10} & r_1 & q_2 & x_9 & q_1 & x_8 & x_7 & p_2 & p_1 & x_6 & x_5 & d_2 & x_4 & d_1 & c_2 & x_3 & c_1 & x_2 & x_1 & b & a & e \\
\end{array}
$$

The canonical representation is easily obtained if we write this table in terms of the numerical values. If we wish to verify isomorphism of two groups, we simply have to find the numerical tables and these have to coincide.

5 Infinite Sets and Real Numbers

In this section we will build the structure of real numbers, using the same principles of our construction of natural numbers. We simply have to extend our methods to the case of infinite sets. First of all, notice that any real number in the unit interval $(0,1]$ can be given in negative powers of 2. For example, the number $\frac{1}{2} = 2^{-1}$ and $\frac{3}{4} = 2^{-1} + 2^{-2}$.

We make a second observation. Consider the energy level graph of a sum, as in Figure 1. Notice that we can vertically displace the configuration of points, and still obtain a true statement. What happens if we make a displacement into negative integers? The statement still holds. See Figure 3. This is true because negative powers of two are still operated with the same rule. The expression $2^n + 2^n = 2^{n+1}$ holds for any integer n, not only positive integers. For example, to add the numbers $\frac{1}{2} + \frac{3}{4}$ we have $2^{-1} + 2^{-1} + 2^{-2} = 2^0 + 2^{-2} = 1 + \frac{1}{4}$. We use this to our advantage in formalizing the concept of real number.
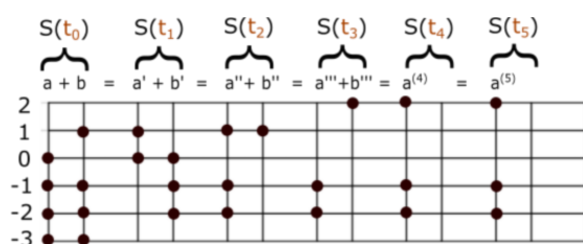
Fig. 3 The energy level interpretation can be taken to negative levels. Particles occupying these levels represent negative powers of 2. In Figure 1 this represented $15 + 23 = 38$. Here, we have the statement $1.875 + 2.875 = 4.75$.

We have seen how to represent natural numbers as hereditarily finite sets, and $\mathbb{N} = \mathbf{HFS}$. We know, because of the union axiom, that $\mathbf{HFS} = \bigcup_n \oplus 1^n(0)$ is a set. In our first axiom we accept that the sub collection of any set, is also a set. This means that any infinite sub collection of $\mathbf{HFS}$, is a set. In this section we will prove that these sets are the real numbers. We divide this section in three main parts.

1. **Continuum $[0,1]$.** Any real number in the unit interval is the sum of infinitely many negative powers of 2. Moreover, every infinite set of natural numbers defines a unique real number in the unit interval.
2. **Real Numbers.** We generalize the constructions of $\mathbb{N}$ and $[0,1]$ to represent positive real numbers as infinite subsets of $\mathbb{Z}$. Then, we give the structure of $\mathbb{R}$ to the set of infinite subsets of $\mathbf{HFS}$.
3. **Límits and Continuity.** The concept of limit and continuity has a simple description in terms of our constructions. We give an initial description of Analysis, in terms of the order for natural numbers, $\mathbb{N}_<$.

We give a brief description of these developments, and leave some of the proofs for a separate publication on real numbers.

5.1 Continuum $[0,1]$

A real number $x \in (0,1]$ can be expressed as a sum of negative powers of 2, so that $x = \sum_{i \in X} 2^{-i}$ for some set $X \subseteq \mathbb{N}$. The set $X \subset \mathbb{N}$ is the set number corresponding to x. The set number X can be a finite set (for some rational numbers). However, notice that any rational number $x = \sum_{i=1}^{n} 2^{-i}$ can be seen as an infinite sum $x = \left(\sum_{i=1}^{n-1} 2^{-i} \right) + \left(\sum_{i=n}^{\infty} 2^{-i} \right)$. Thus, every $x \in (0,1]$ is represented by a unique infinite set of natural numbers greater than 0. We use the symbol $\mathbb{N}_1 = \{1,2,3,\ldots\}$ for the set of natural numbers greater than 0. We have a bijection $\mathbb{N}_{inf} \to (0,1]$, where $\mathbb{N}_{inf}$ is the set of all infinite subsets of $\mathbb{N}_1$. We call these sets, *infinite set numbers* and they are ordered similarly to finite set numbers, but with one difference. The smaller powers of 2 represent larger numbers. For example, $2^{-5} < 2^{-1}$. Instead of using the maximum of the set difference, now we look for the minimum. Therefore, we define $A < B$ if and only if

$$\min(A \triangle B) \in B.$$

Notice that $1 = \mathbb{N} \in \mathbb{N}_{inf}$. Let us verify this is a transitive order on $\mathbb{N}_{inf}$, because it is trivial to verify it is anti symmetric. Suppose $A < B$ and $B < C$. We know there exists an object $c_0 \in C/B$ such that $c_0 < b$ for every $b \in B/C$. We also know there is an object $b_1 \in B/A$ such that $b_1 < a$ for every $a \in A/B$. Suppose there exists $a_2 \in A/C$ such that $a_2 < c$ for every $c \in C/A$. We treat two cases and in each we arrive at a contradiction, proving $A < C$.

Let us suppose $a_2 \in B$. Then $c_0 < a_2$. This means c_0 must be in A. This implies $b_1 < c_0$. Thus, $b_1 \in C/A$ and $a_2 < b_1$ which is a contradiction.

Let us suppose $a_2 \notin B$. This implies $b_1 < a_2$. We know $b_1 \notin A$ so that $b_1 \in C$ implies $a_2 < b_1$ which is a contradiction. Therefore, we must have $b_1 \notin C$. Then, $c_0 < b_1$. For $c_0 < a_2$ to be true, we need $c_0 \in A$. But, this would imply $b_1 < c_0$, again a contradiction.

This proves our order on $\mathbb{N}_{inf}$ is transitive. Obviously, any two objects in $\mathbb{N}_{inf}$ are comparable in terms of this relation, $<$, because the symmetric difference is non empty for different set numbers $A \neq B$. Then, we know $\min(A \triangle B)$ exists because of the well order principle. We have ordered $\mathbb{N}_{inf}$ isomorphic to $(0,1]$. The real number, 1, is the set $\mathbb{N}$. To include the real number 0, in our order, we consider $\mathbb{N}_{inf}^* = \mathbb{N}_{inf} \cup \{\emptyset\}$. This is the set whose objects are the infinite subsets of $\mathbb{N}$, plus the empty set. Now we have the order of $[0,1]$ in terms of sets, where $0 = \emptyset$ and every $x \in (0,1]$ is an infinite set of natural numbers. The most important aspect in the order of a continuum, is the the supremum property. This is what characterizes a continuum from a discrete order. Now we will show that the supremum exists, for our order $\mathbb{N}_{inf}^*$. Let $\mathbf{X} \subseteq \mathbb{N}_{inf}^*$; every element of $\mathbf{X}$ is an infinite set of natural numbers. Define $x_1 = \min(\bigcup \mathbf{X})$ and $Y_1 = \{A \in \mathbf{X} | x_1 \in A\}$. Let

$$x_{n+1} = \min \left(\bigcup Y_n - \{x_i\}_{i=1}^{n} \right),$$

where $Y_n = \{A \in Y_{n-1} | x_n \in A\}$. The set number $\{x_i\}_i \in \mathbb{N}_{inf}^*$ is the supremum of X, by construction. This is shown in Figure 4.
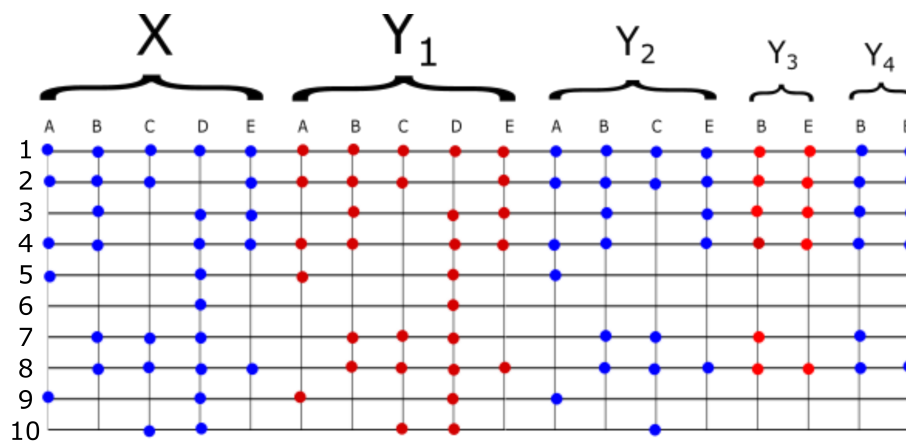
Fig. 4 Here we represent the process of finding the supremeum of the family $X = \{A,B,C,D,E\}$. The elements of X are set numbers in the unit interval. For example, $A = 2^{-1} + 2^{-2} + 2^{-4} + 2^{-5} + 2^{-9} = 0.845703125$.

The next step, after defining our order for infinite set numbers, is to define the addition of infinite set numbers. Let $r = s^{-1}$; the inverse function of s. Recall, this function subtracts 1 one unit to the elements of the argument. Given two infinite set numbers $A = \{a_1, a_2, \ldots\}$ and $B = \{b_1, b_2, \ldots\}$, let $A_n = \{a_k\}_{k=1}^{n}$ and $B_n = \{b_k\}_{k=1}^{n}$ be the sets of the first n objects. Define

$$A_n \oplus B_n = (A_n \triangle B_n) \oplus r(A_n \cap B_n).$$

The addition $A \oplus B$ is the supremum of the finite sums,

$$A \oplus B = \sup_n (A_n \oplus B_n).$$

5.2 Real Numbers

We can generalise our previous constructions of $\mathbb{N}$ and $[0,1]$, into a single structure, $\mathbb{R}_0^+$, based on the observation of Figure **??**. But, first we need to prove that the integers are sets. Take the integer $1 \in \mathbb{Z}$; it is the function $\oplus 1$. We know that finite function is a finite set of set numbers. Then, the function $\oplus 1$ is the object $\{\{1,4\},\{3,6\},\{5,8\},\{7,10\},\ldots\}$. Thus, the integer $1 \in \mathbb{Z}$ is an infinite set number and, in particular, a set. The integer $2 \in \mathbb{Z}$ is the infinite set $\{\{1,6\},\{3,8\},\{5,10\},\{7,12\},\ldots\} \in \mathbb{N}_{inf}^*$, etc. The negative integer $-1 \in \mathbb{Z}$ is the object $\{\{3,2\},\{5,4\},\{7,6\},\{9,8\},\ldots\}$. The negative integer $-2 \in \mathbb{Z}$ is the object $\{\{\{5,2\},\{7,4\},\{9,6\},\{11,8\},\ldots\}$, etc. Now we wish to show that the collection of integers is a set. Given that $\mathbb{Z}$ is a sub collection of $\mathbb{N}_{inf}^*$, it is sufficient to prove $\mathbb{N}_{inf}^*$ is a set (because of Axiom 1). We know the elements of $\mathbb{N}_{inf}^*$ are sets. But we can not go any further with our axioms. Our axioms allow us to build sets using union and intersection, and sub collections. If we take the union of the infinite set numbers we get $\mathbb{N} = \bigcup_{i \in \mathbb{N}_{inf}^*} i$. We can not prove $\mathbb{N}_{inf}^*$ is a set. We need a new axiom.

Axiom 3 *Let X a collection of constructed sets, then X is a set.*

Here we have to be very careful to avoid the commonly known paradox of the set of all sets, so let us be clear on this. If we have a collection of concrete sets, then that collection is a set. We will see the implications of this in the last section. Intuitively, every set is in a larger set. For now, we only care that $\mathbb{N}_{inf}^*$ is a set because it is a collection of sets. Thus we have proven $\mathbb{Z}$ is a set. Let $\bar{\mathbb{Z}} \subset \mathbb{N}_{inf}^*$ the set whose objects are subsets of $\mathbb{Z}$, that are bounded above. Put differently, $A \in \bar{\mathbb{Z}}$ if and only if $A \subset \mathbb{Z}$ and $\max(A)$ exists. We can treat A as a positive real number because a positive real number is well represented by a sum of integer powers of 2. The non negative integers represent the whole part of the real number, while the negative integers are the decimal part of the real number, as in Figure **??**. This simply means $A \cap \mathbb{N}$ is the whole part of A, and $A \cap -\mathbb{N}$ is the decimal part. The set of all non negative real numbers is $\mathbb{R}_0^+ = \bar{\mathbb{Z}} \cup \{\emptyset\}$. Two positive real numbers are order related $A < B$ if and only if $\max(A \triangle B) \in B$. The addition is defined as before by $A \oplus B = (A \triangle B) \oplus s(A \cap B)$. The supremum can also be found in this structure of sets. At this point, we can proceed to build the negative real numbers using the same technique we used to build the negative integers. Every $A \in \mathbb{R}_0^+$ is identified with a function $\oplus A : \mathbb{R}_0^+ \to A$. Namely, we build a new set of positive real numbers, which will be the bijections $\mathbb{R}_0^+ \to A$. We can then identify negative real numbers as the inverse functions of these. We do not focus on this construction, in this work, because we use a different path to define the structure of all real numbers.

Our alternative method of building the set of real numbers, $\mathbb{R}$, does not depend on integers, only on natural numbers. Using our construction of the unit interval $[0,1]$, we can represent every real number as an object in $\mathbb{N}_{inf}^*$.
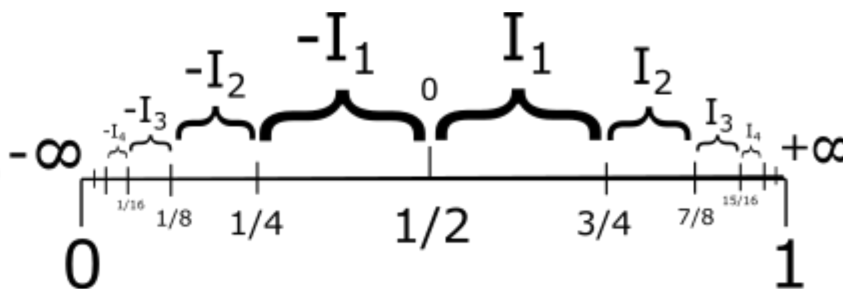
Fig. 5 We use the fact that $\mathbb{R}$ is bijective to any interval $(\frac{n}{2^k}, \frac{n+1}{2^k}]$. Under this representation, the real number $0 \in \mathbb{R}$ is the set $\{2,3,4,5,\ldots\}$. We also have $-\infty \in \mathbb{R} = \emptyset$ and $+\infty = \mathbb{N}_1$

Each of the positive intervals $I_1 = (0,1]$, $I_2 = (1,2]$,..., and negative intervals $-I_1 = (-1,0]$, $-I_2 = (-2,-1]$,..., is isomorphic to the interval $(\frac{n}{2^k}, \frac{n+1}{2^k}]$, for any $n \leq 2^k - 1$ in $\mathbb{N}$. Intuitively, what we will do is to compress and fit all the intervals I_i, into the unit interval, as in Figure 5. The interval $I_1 \subset \mathbb{R}$ is identified with the interval $(\frac{1}{2}, \frac{3}{4}] \subset [0,1]$. The interval $I_2 \subset \mathbb{R}$ is the interval $(\frac{3}{4}, \frac{7}{8}] \subset [0,1]$, etc. The negative interval $-I_1 \subset \mathbb{R}$ is the interval $(\frac{1}{4}, \frac{1}{2}] \subset [0,1]$, etc.

Let $X \in [0,1] = \mathbb{N}_{inf}^*$. Notice that a number $x \in (\frac{1}{2}, \frac{3}{4}] \in \mathbb{N}_{inf}^*$ is an infinite set number such that $1 \in X$ and $2 \notin X$. A set number $x \in (\frac{3}{4}, \frac{7}{8}] \in \mathbb{N}_{inf}^*$ is an infinite set number such that $1 \in X$ and $2 \in X$, but $3 \notin X$, etc. A set number $X \in (\frac{1}{4}, \frac{1}{2}] \in \mathbb{N}_{inf}^*$ is an infinite set number such that $1 \notin X$ and $2 \in X$. A set number $X \in (\frac{1}{8}, \frac{1}{4}] \in \mathbb{N}_{inf}^*$ is an infinite set number such that $1,2 \notin X$ and $3 \in X$, etc. This has a simple form, that we can easily interpret in defining the set of all real numbers. Let $X = \{1,2,3,\ldots,n,k_1,k_2,k_3,\ldots\} \in \mathbb{N}_{inf}^*$, where $3 \leq n+2 \leq k_1 < k_2 < k_3 < \cdots$, then we will say X is positive real number. A negative real number is $X = \{n,k_1,k_2,k_3,\ldots\}$ with $3 \leq n+1 \leq k_1 < k_2 < k_3 < \cdots$. This simply means we will define a positive real number with whole part equal to n, as an infinite set number X with $1,2,\ldots,n+1, \in X$ and $n+2 \notin X$. A negative real number with whole part equal to $-n$ is an infinite set number X with $\min(X) = n+1$. The decimal part will be given by the remaining objects $k_1,k_2,k_3\ldots$. We can immediately differentiate a set positive set number from a negative set number. For example, The set number $\{1,2,3,4,10,11,12,13,\ldots\}$ is positive with whole part equal to 3. The set number $\{5,10,11,12,13,\ldots\}$ is negative with whole part equal to -3. The set number $\{1,2,6,7,8,\ldots\}$ has whole part equal to 1, while $\{6,8,9,10,\ldots\}$ has whole part equal to -4.

How do we find the decimal part of a set number, in this context? We simply used the first natural numbers as place holders for identifying the whole part. Let $X \in \mathbb{N}_{inf}^*$ be an infinite set number. The objects $k_1,k_2,k_3,\ldots$ are representing the decimal part of X. We assign X the decimal part $r^{n+1}(\{k_1,k_2,k_3,\ldots\})$. Let us look at the problem backwards, to better understand why. If we

want to store the information of a real number $x \in \mathbb{R}$ as an infinite set number, how would we do it? We already saw that we need the first n natural numbers to determine the whole. But then we still have infinitely many natural numbers left to determine the decimal part. So all we have to do, is displace the decimal part $n+1$ places, so that the decimal part and whole part do not interfere. Notice that in the case of positive real numbers, we need to leave one natural number out, as a queue that the whole part ends there, and now we start with the representation of the decimal part. Displacement up, $n+1$ times, is equivalent to applying s^{n+1}. Now, to recover the decimal part, we have to displace the k_i's back $n+1$ times by applying r^{n+1}.

Let us look at this in formal manner. For every $x \in \mathbb{N}_{inf}^*$, the numbers $\min(x)$ and $\min(x^c)$ are well defined, because of the well ordering principle. Exactly one of these two is equal to 1 and the other is larger than 1. A *positive real number* is an infinite set number with $\min(x) = 1$. A *negative real number* is an infinite set number with $\min(x^c) = 1$. More specifically, if $0 < x \le 1$ then $\min(x^c) = 2$, and if $-1 < x \le 0$ then $\min(x) = 2$. The equality $\min(x^c) = 3$ is equivalent to $1 \le x < 2$, and $\min(x) = 3$ is equivalent to $-2 < x \le -1$. If $2 < x \le 3$ then we have $\min(x^c) = 4$, and if $-3 < x \le -2$ then we have $\min(x) = 4$. In general, $x \in (n-1,n]$ if and only if $\min(x^c) = n+1$, and $x \in (-n, -(n-1)]$ if and only if $\min(x) = n+1$.

For example, the decimal part of π is given by the set

$$\{3, 6, 11, 12, 13, 14, 15, 16, 18, \ldots\}.$$

because it is equal to $2^{-3} + 2^{-6} + 2^{-11} + 2^{-12} + 2^{-13} + 2^{-14} + \cdots$. Therefore, the numbers π and $-\pi$ are represented by

$$
\begin{aligned}
\pi &= \{1, 2, 3, 4, 3+5, 6+5, 11+5, 12+5, 13+5, 14+5, 15+5, 16+5, 18+5, \ldots\} \\
&= \{1, 2, 3, 4, 8, 11, 16, 17, 18, 19, 20, 21, 23, \ldots\} \\
-\pi &= \{5, 3+5, 6+5, 11+5, 12+5, 13+5, 14+5, 15+5, 16+5, 18+5, \ldots\} \\
&= \{5, 8, 11, 16, 17, 18, 19, 20, 21, 23, \ldots\}
\end{aligned}
$$

The set of infinite set numbers $\mathbb{N}_{inf}^*$ is $\mathbb{R}$. Real numbers and natural numbers are different types of sets. Natural numbers are the elements of **HFS**, while real numbers are the infinite subsets of **HFS**. Of course we can make adequate definitions for addition of real numbers, in this definition.

5.3 Limits and Continuity

Now we have the task of finding suitable and practical expressions of the concepts of analysis. We begin by defining the concept of *limit point*. Let $P, X \in \mathbb{N}_{inf}^*$ two infinite set numbers. Intuitively, these two objects are close, if their first terms coincide. Take as an example the set numbers $P = \{2, 4, 5, 8, 9, 10, 11, 12, 13, \ldots\} = 2^{-2} + 2^{-4} + 2^{-5} + 2^{-8} + 2^{-9} + 2^{-10} + \ldots$ and $X = \{2, 4, 5, 8, 9, 14, 15, 16, 17 \ldots\} = 2^{-2} + 2^{-4} + 2^{-5} + 2^{-8} + 2^{-9} + 2^{-14} + \ldots$. They are relatively close because the first terms (the largest terms) coincide. So we know we need to ask that the first elements coincide, for two numbers to be close. Another way of saying this is that $\min(P \triangle X)$ is a large number. The larger $\min(P \triangle X)$, the larger the elements of $P \triangle X$ become, making the smaller powers (larger terms) coincide. Remember, that in the decimal part, larger natural numbers represent the smaller terms of the real number.

Let us give a formal definition of this. Let $P \in \mathbb{N}_{inf}^*$ an infinite set number, and let $\mathbf{X}$ a set of infinite set numbers. We say *P is a limit point of* $\mathbf{X}$ if there exists $X_N \in \mathbf{X}$ such that $\min(P \triangle X_N) > N$, for every $N \in \mathbb{N}$. There is one exception to this definition. When we started to describe real numbers as infinite set numbers we noticed some real numbers had decimal part that could be expressed as sum of finite many negative powers of 2. We will treat these numbers separately in defining limit points. Suppose $P \in \mathbb{N}_{inf}^*$ is an infinite set number that has finite representation $P = \{p_1, p_2, \ldots, p_k\}$, where $p_1 < p_2 < \cdots < p_k$. That is to say, we can write it as $P = \{p_1, p_2, \ldots, p_{k-1}, p_k+1, p_k+2, p_k+3, \ldots\}$. We simply replace the last term 2^{-p_k} with infinite terms, $2^{-(p_k+1)} + 2^{-(p_k+2)} + 2^{-(p_k+3)} + \ldots$. We give aset of infinite set numbers that get as close to P as we would like, using larger numbers than P. Let $X_1 = \{p_1, p_2, \ldots, p_k, p_k+1\}$, and $X_2 = \{p_1, p_2, \ldots, p_k, p_k+2\}$. In general define $X_i = \{p_1, p_2, \ldots, p_k, p_k+i\}$. These set numbers X_i are getting closer to P but our rule is not satisfied. The minimum element of the symmetric difference is not getting larger. In fact, it is constant, $\min(P \triangle X_i) = p_k$. Therefore, we must make a different definition for this case. If P is an infinite set number with finite representation, then we say P is a limit point of $\mathbf{X}$ if for every $N \in \mathbb{N}$, there exists $X_N \in \mathbf{X}$ such that $X_N = \{p_1, p_2, \ldots, p_k, p_k+N, p_{n_1}, p_{n_2}, \ldots\}$, where $p_k+N < p_{n_1} < p_{n_2} < \cdots$.

In both cases we are requiring an infinite set number X_N such that $|P - X_N| \le \frac{1}{2^N} = \{N\}$. Let P, X two infinite set numbers with their whole parts equal and suppose their decimal parts coincide in the first elements. We have

$$
\begin{aligned}
P &= 2^{m_1} + 2^{m_2} + \ldots + 2^{m_k} + 2^{n_1} + 2^{n_2} + 2^{n_3} + \ldots + 2^N + 2^{\alpha_1} + 2^{\alpha_2} + 2^{\alpha_3} + \ldots \\
X &= 2^{m_1} + 2^{m_2} + \ldots + 2^{m_k} + 2^{n_1} + 2^{n_2} + 2^{n_3} + \ldots + 2^N + 2^{\beta_1} + 2^{\beta_2} + 2^{\beta_3} + \ldots
\end{aligned}
$$

where $m_1 < m_2 < \ldots < m_k < n_1 < n_2 < \ldots < N < \alpha_1 < \alpha_2 < \cdots$ and $N < \beta_1 < \beta_2 < \cdots$. The numbers m_i determine the whole part and n_i, N are the elements that coincide in the decimal part (the first negative powers of 2 that coincide). Then, the difference $|P - X| < \frac{1}{2^{N-(m_k+1)}}$ is bounded by $\frac{1}{2^{N-(m_k+1)}}$.

We see that infinite set numbers with finite representations can be handled in another, informal, manner. For example, $1/2 \in [0,1]$ has the representations $\{1\} = \{2, 3, 4, \ldots\}$. We know $P = 1/2$ should be a limit point of the set $\mathbf{X} = \{A_1, A_2, A_3, A_4, \ldots\}$ where A_i are

$$
\begin{aligned}
A_1 &= \quad 1 \quad = \{1,2,3,4,5,6,\ldots\} \\
A_2 &= \quad 3/4 \quad = \{1,3,4,5,6,7,\ldots\} \\
A_3 &= \quad 5/8 \quad = \{1,4,5,6,7,8,\ldots\} \\
A_4 &= 9/16 = \{1,5,6,7,8,9,\ldots\}
\end{aligned}
$$

$$\vdots \quad \vdots \qquad \vdots$$

If $P = \{2,3,4,5,\ldots\}$ then $\min(P \triangle A_i) = 1$, for every A_i. But, if we use the finite representation $P = \{1\}$, then the symmetric differences are: $P \triangle A_1 = \{2,3,4,\ldots\}$, $P \triangle A_2 = \{3,4,5,\ldots\}$, $P \triangle A_3 = \{4,5,6,\ldots\}$, $P \triangle A_4 = \{5,6,7,\ldots\}$,... In effect, complying with our condition that for every $N \in \mathbb{N}$ there exists $X_N \in \mathbf{X}$ such that $\min(P \triangle X_N) > N$.

If P has finite representation and we where to get closer to P, using smaller numbers, we can not have the same problem that we had when we were getting closer from above. For example, take $P = 1/2 = \{2,3,4,5,\ldots\}$ and the set $\mathbf{X} = \{A_1, A-2, \ldots\}$ defined by

$$
\begin{aligned}
A_1 &= \quad 3/8 \quad = \{2,4,5,6,7,8\ldots\} \\
A_2 &= \quad 7/16 \quad = \{2,3,5,6,7,8\ldots\} \\
A_3 &= \quad 15/32 \quad = \{2,3,4,6,7,8\ldots\} \\
A_4 &= \quad 31/64 \quad = \{2,3,4,5,7,8\ldots\} \\
A_5 &= 63/128 = \{2,3,4,5,6,8\ldots\}
\end{aligned}
$$

$$\vdots \quad \vdots \qquad \vdots$$

We can easily verify that for every $N \in \mathbb{N}$ there exists X_N such that $\min(P \triangle X_N) > N$. We have $P \triangle A_1 = \{3\}$, $P \triangle A_2 = \{4\}$, $P \triangle A_3 = \{5\}$, $P \triangle A_4 = \{6\}$, $P \triangle A_5 = \{7\}$,...

Continuity is described in terms of the order of natural orders, consequently. In the next section we will provide a formal definition for real function. We use it provisionally, for the sake of illustration.

Definition 10 *Let $f : A \subseteq \mathbb{R} \to B \subseteq \mathbb{R}$ a real function, and let p a limit point of the domain A. We say f has limit point p, and the limit is equal to q, if and only if for every $N \in \mathbb{N}$ there exists $M \in \mathbb{N}$ such that $\min(p \triangle x) > M$ implies $\min(f(p) \triangle q) > N$.*

The function is continuous in p if and only if for every $N \in \mathbb{N}$ there exists $M \in \mathbb{N}$ such that $\min(p \triangle x) > M$ implies $\min(f(p) \triangle f(x)) > N$.

The theory of convergence and topological aspects of $\mathbb{R}$ are expressed directly in terms of the order of natural numbers. Using these general indications and the subtraction algorithm, given in [I], it is possible to define the derivative. We can treat the derivative in two ways. If we use the subtraction algorithm we can define the derivative in the traditional manner to find the numerical value $f'(p)$. If, however, we only wish to prove the *existence* of the derivative, we will have an alternative definition of a *discrete derivative*. We know the quotient of two powers of 2 is obtained by subtracting the powers, $\frac{2^n}{2^m} = 2^{n-m}$. The derivative of f exists at p if there exists $M \in \mathbb{N}$ such that $\min(fp \triangle fx) + M > \min(p \triangle x)$ for every $x \in A$. In the case that $\min(fp \triangle fx) > \min(p \triangle x)$ for every $x \in A$, we have $0 \le |f'(p)| < 1$. The derivative is exactly equal to 0 when $\min(fp \triangle fx) - \min(p \triangle x)$ is not bounded; $\min(p \triangle x)$ goes to infinity but $\min(fp \triangle fx)$ goes to infinity faster so that $\min(fp \triangle fx) - \min(p \triangle x)$ goes to infinity. If $\min(fp \triangle fx) = \min(p \triangle x)$ for every $x \in A$ then $|f'(p)| = 1$. If we need to add $M \in \mathbb{N}$ to get $\min(fp \triangle fx) + M > \min(p \triangle x)$ for every $x \in A$ we have $|f'(p)| > 1$.

The discrete derivative is a criteria for the existence and absolute value of the magnitude of the derivative. In exchange, for not knowing the exact numerical value of the derivative, we can say that finding the discrete derivative is computationally much faster. We are substituting the quotient $\frac{fp-fx}{p-x}$ of floating point numbers, with finding the difference of natural numbers, $|\min(fp \triangle fx) - \min(p \triangle x)|$. The end result is that instead of having to calculate two subtractions and one division of real numbers, we find the minimum element for two sets of natural numbers and the difference of these natural numbers.

6 Trees and Type Theory

In this section we will give an account of how to build and represent general objects used in modern mathematics. This will be a very superficial description but we will show enough of these constructions to be clear on the extent of constructions possible. We also show how this universe of sets can be well represented in terms of trees. We also give a brief description of the theory of types this axiomatic base provides. We see how to give a consistent hierarchy of types and universes.

6.1 Basic Objects In Mathematics

Ordered pairs, and finite sets of ordered pairs, are natural numbers. Now let us define an ordered n-tuple of natural numbers. Recall that to define an ordered pair of natural numbers we used a simple trick. We used even and odd natural numbers to tell apart our first component from the second. One might initially want to go about this in the following manner. If we wish to

well represent ordered 3-tuples we could use numbers $\{1,4,7,10,\ldots,3k-2,\ldots\}$ to represent the first component, then we use $\{2,5,8,11,\ldots,3k-1,\ldots\}$ to represent the second component, and multiples of three, $\{3,6,9,12,\ldots,3k,\ldots\}$ to represent the third component. This will give us a table similar to (6), when we defined ordered pairs. Table 6 gives us ordered 3-tuples.

Table 6 The elements of this table allow us to represent an ordered 3-tuple as a natural number.

X	$3k-2$	$3k-1$	$3k$
0	1	2	3
1	4	5	6
2	7	8	9
3	10	11	12
4	13	14	15
5	16	17	18
6	19	20	21
$\vdots$	$\vdots$	$\vdots$	$\vdots$

The ordered 3-tuple $(0,0,0)$ is the set number $2^1 + 2^2 + 2^3 = \{1,2,3\}$. We also have $(1,2,3)$ equal to $2^4 + 2^8 + 2^{12} = \{4,8,12\}$. If we want to represent 4-tuples we would have to come up with a new table 7.

Table 7 The elements of this table allow us to represent an ordered 4-tuple as a natural number.

X	$4k-3$	$4k-2$	$4k-1$	$4k$
0	1	2	3	4
1	5	6	7	8
2	9	10	11	12
3	13	14	15	16
4	17	18	19	20
5	21	22	23	24
6	25	26	27	28
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

This manner of defining finite sequences has two big disadvantages that will become clear, when we define a second method for representing ordered n-tuples. The first is quite obvious: we can not define an infinite sequence of natural numbers. The easiest way to solve this is by going back to the definition of ordered pairs. The sets given in (6) are of great importance in the constructions of this section. We include it again, for reference in Table 8. Here we will use it differently. Only the first two rows are needed to define all ordered pairs. To define an ordered pair of natural numbers it will only be necessary to use the first two sets $(0,)$ and $(1,)$. The pair (i,j) will be a set of two numbers; its elements will be the $i+1$-th object of the first row and the $j+1$-th object of the second row.

Table 8 The elements of this table allow us to represent an ordered pair as a natural number. The elements of the first row are used to represent the first component, while the elements of the second row are used to represent the second component. This table is also used for finding a good representation of sequences of real numbers.

6	18	66	258	1026	$\ldots$	$2+2^{2(n+1)}$	$\ldots$
12	24	72	264	1032	$\ldots$	$8+2^{2(n+1)}$	$\ldots$
36	48	96	288	1056	$\ldots$	$32+2^{2(n+1)}$	$\ldots$
128	144	192	382	1152	$\ldots$	$128+2^{2(n+1)}$	$\ldots$
516	528	576	768	1536	$\ldots$	$512+2^{2(n+1)}$	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	
$2^{2m+1}+4$	$2^{2m+1}+16$	$2^{2m+1}+64$	$2^{2m+1}+256$	$2^{2m+1}+1024$	$\ldots$	$2^{2m+1}+2^{2(n+1)}$	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	

We give a definition of ordered pair that supersedes the one given before. An ordered pair is a set number (i,j) where $i \in (0,)$ and $j \in (1,)$. Specifically, the ordered pair (i,j), is the set number $\{2^1 + 2^{2(i+1)}, 2^3 + 2^{2(j+1)}\}$. We include the $i+1$-st element of $(0,)$ to show that i is in the first component. We include the $j+1$-st element of $(1,)$ to indicate j is in the second component. For example, the ordered pair $(0,0)$ is the set number $2^6 + 2^{12} = \{6,12\}$. The ordered pair $(0,1)$ is $2^6 + 2^{24} = \{6,24\}$.

We are defining *data types* for different mathematical objects. Different kinds of mathematical objects and relations can be translated represented as natural and real numbers. An *infinite sequence of natural numbers* is easy to define. Take one element n_k from the set $(k,)$, for every $k \in \mathbb{N}$. Then, $2^1 + 2^{2(n_1+1)} \in S$ means n_1 is the first natural number of the sequence. The second number is given by $2^3 + 2^{2(n_2+1)} \in S$, and so on. The set number $\{2^1 + 2^{2(n_1+1)}, 2^3 + 2^{2(n_2+1)}, 2^5 + 2^{2(n_3+1)}, \dots\}$ represents the sequence $(n_1, n_2, n_3, \dots)$. For example, the sequence $(1, 3, 2, 5, 4, 7, 6, 9, 8, 11, 10, 13, 12, \dots)$ is given by the infinite set number $\{2 + 2^{2(1+1)}, 8 + 2^{2(3+1)}, 32 + 2^{2(2+1)}, 128 + 2^{2(5+1)}, 512 + 2^{2(4+1)}, \dots\} = \{18, 264, 96, 4224, 1536, \dots\}$. Of course, to define a finite sequence, an k-tuple, we use the first k sets, $(1,), (2,), \dots (k,)$. A finite sequence of natural numbers is a natural number $\{2^1 + 2^{2(n_1+1)}, 2^3 + 2^{2(n_2+1)}, 2^5 + 2^{2(n_3+1)}, \dots, 2^{2k+1} + 2^{2(n_k+1)}\}$. We can easily describe a *natural function*, $\mathbb{N} \to \mathbb{N}$ as an infinite set of ordered pairs. A function of this form is a set number

$$\{\{6, B_1\}, \{18, B_2\}, \{66, B_3\}, \{258, B_4\}, \dots\}$$

where B_i are elements of $(1,)$. If the B_i are all distinct, we have an injection. If every element of $(1,)$ is a B_i the function is onto $\mathbb{N}$. This represents natural functions as real numbers. We have a bijective function from the set of all natural functions, onto a proper subset of real numbers.

How would we go on about representing a *sequence of real numbers*? The same question stated differently, How can we represent a sequence of infinite sets of natural numbers? We wish to find the best way of storing and rescuing the information that determines a sequence $\xi = (r_1, r_2, r_3, \dots)$ where each $r_i = \{n_1^i, n_2^i, n_3^i, \dots\}$ is a real number. Use the set $(0,)$ to represent the elements of r_1. Use the set $(1,)$ to represent the elements of r_2, etc. We have $2^{2(i)+1} + 2^{2(n_j^i+1)} \in \xi$ if and only if $n_j^i \in r_i$. The infinite sequence of real numbers, $(r_1, r_2, \dots)$, is represented by the real number $\bigcup_i r_i$. The union of all the r_i's is a real number that represents the infinite sequence $(r_1, r_2, \dots)$; it is an infinite set number with infinitely many objects from each set $(i,)$. Actually, any set number with infinitely many elements of each $(i,)$ is representing a unique sequence of real numbers. If we have an infinite set $X \subset (0,)$ this determines a real number. The set $X = \{2 + 2^{2(x_1+1)}, 2 + 2^{2(x_2+1)}, 2 + 2^{2(x_3+1)}, \dots\}$ determines the real number $X^* = \{x_1, x_2, x_3, \dots\}$. In the same manner, $Y = \{8 + 2^{2(y_1+1)}, 8 + 2^{2(y_2+1)}, 8 + 2^{2(y_3+1)}, \dots\} \subset (1,)$ determines the real number $Y^* = \{y_1, y_2, y_3, \dots\}$. Observe that the infinite set number $X^* \cup Y^*$ is a real number, whose objects are in $(0,) \cup (1,)$, and we can distinguish the objects of $(0,)$ from the objects of $(1,)$. The objects in $(0,)$ give us the first component, and the second component is given by the elements of $(1,)$. Thus, we are able to represent the ordered pair of real numbers, (X^*, Y^*), as a single real number $X \cup Y$. If we wish to represent ordered 3-tuples of real numbers, we can do so by additionally using $(2,)$. Let $Z^* = \{z_1, z_2, z_3, \dots\} \subset \mathbb{N}$ a real number, then we have $Z = \{32 + 2^{2(z_1+1)}, 32 + 2^{2(z_2+1)}, 32 + 2^{2(z_3+1)}, \dots\} \subset (2,)$. And, the ordered 3-tuple (X^*, Y^*, Z^*) is the real number $X \cup Y \cup Z$. An infinite sequence of real numbers $x_1, x_2, \dots$ is represented by a single real number. We are giving a bijective function from the set of all real sequences onto a proper subset of real numbers. A sequence of real numbers is well represented by a single real number. A function $\mathbb{N} \to \mathbb{N}$ is well represented by a real number. Consequently, we can represent a *sequence* $(f_1, f_2, \dots)$, *of functions* $f_i : \mathbb{N} \to \mathbb{N}$, as a single real number. In summary, we have provided a second definition for ordered pairs, that is a more powerful definition than the first because it allows to represent an infinite sequence of natural numbers, as a real number. Moreover, if ξ is a countable sequence of real numbers, it is also represented as a real number. As a consequence we were also able to find good representations of functions $\mathbb{N} \to \mathbb{N}$, and sequences of these functions.

Let us find a way of representing sequences of sequences. Start with the simplest kind, a *sequence* $T = (S_1, S_2, \dots)$ *of sequences,* S_i, *of natural numbers*. We use subsets of $(i,)$ to find these representations. We will work with a subset of $(0,)$ to represent the first sequence $S_1 = (n_1^1, n_2^1, n_3^1, \dots)$. We have

$$2 + 2^{2\left(\left(2 + 2^{2\left(n_1^1 + 1\right)}\right) + 1\right)}, \ 2 + 2^{2\left(\left(2 + 2^{2\left(n_2^1 + 1\right)}\right) + 1\right)}, \dots \in T$$

for every $i = 1, 2, 3, \dots$. We use a subset of $(1,)$ to represent the second sequence. If $S_2 = (n_1^2, n_2^2, n_3^2, \dots)$ is the second sequence, then we have

$$8 + 2^{2\left(\left(2 + 2^{2\left(n_1^2 + 1\right)}\right) + 1\right)}, \ 8 + 2^{2\left(\left(2 + 2^{2\left(n_2^2 + 1\right)}\right) + 1\right)}, \dots \in T$$

for every $i = 1, 2, 3 \dots$. The third term is

$$32 + 2^{2\left(\left(2 + 2^{2\left(n_1^3 + 1\right)}\right) + 1\right)}, \ 32 + 2^{2\left(\left(2 + 2^{2\left(n_2^3 + 1\right)}\right) + 1\right)}, \dots \in T,$$

etc. In general, the set $(k,)$ is used to represent the sequence S_k, for every $k \in \mathbb{N}$. We are able to reconstruct the sequence of sequences, from the real number

$$T = 2^{2 + 2^{2\left(\left(2 + 2^{2\left(n_1^1 + 1\right)}\right) + 1\right)}} + 2^{2 + 2^{2\left(\left(2 + 2^{2\left(n_2^1 + 1\right)}\right) + 1\right)}} + \dots + 2^{8 + 2^{2\left(\left(8 + 2^{2\left(n_1^2 + 1\right)}\right) + 1\right)}} + 2^{8 + 2^{2\left(\left(2 + 2^{2\left(n_2^2 + 1\right)}\right) + 1\right)}} + \dots +$$

$$+ 2^{32 + 2^{2\left(\left(2 + 2^{2\left(n_1^3 + 1\right)}\right) + 1\right)}} + 2^{32 + 2^{2\left(\left(2 + 2^{2\left(n_2^3 + 1\right)}\right) + 1\right)}} + \dots + \dots + \dots \dots$$

Now, let $\xi_i = (r_1^i, r_2^i, r_3^i, \dots)$ a sequence of real numbers, for every $i \in \mathbb{N}$, and let $\Xi = (\xi_1, \xi_2, \xi_3, \dots)$ the sequence of those. It is easy to see we can construct a real number to represent this object. This is true because every sequence ξ_i, of real numbers, is represented by a real number. The sequence of real numbers, Ξ, can in turn be reduced to a single real number. We can represent a real matrix of infinitely (countable) many columns and rows, with a single real number.

There are similarities between natural numbers and real numbers. A finite natural function is a finite set of natural numbers. An infinite natural function is a set of infinitely many natural numbers. Similarly, a real function will be represented by a set of real numbers. We have defined an ordered pair of real numbers, so now we can define a *real function*. Let us proceed with this construction. A function is a collection of components $f_x = (x, fx)$, and every ordered pair of real numbers $f_x \in \mathbb{R}$ is a real number. Therefore, the function $f : \mathbb{R} \to \mathbb{R}$ can be represented by a set of real numbers $\{f_x\}_{x \in \mathbb{R}}$. Every real function $\mathbb{R} \to \mathbb{R}$ is an uncountable set of real numbers

$$f = \{\{a_1^x, a_2^x, \ldots, b_1^x, b_2^x, \ldots\}\}_{x \in \mathbb{R}},$$

where $x = \{a_i^x\}_i \subset (0,)$ and $f(x) = \{b_i^x\}_i \subset (1,)$. This means $f_x = x \cup f(x) = \{a_1^x, a_2^x, \ldots, b_1^x, b_2^x, \ldots\}$. The function is injective if $f(x) \cap f(y) = \emptyset$ for $x \neq y$. The function f is onto $\mathbb{R}$ if for every infinite subset $A \subset (1,)$, there exists an object $x \in \mathbb{R}$ such that $A = f_x \cap (1,)$. A real function is bijective if for every infinite subset $A \subset (1,)$ there exists exactly one $x \in \mathbb{R}$ such that $A = f_x \cap (1,)$.

We can extend our results to represent any sequence of real functions, $(f_1, f_2, \ldots)$, as a set of real numbers. Just as we use $(0,)$ and $(1,)$ to define a function $f_1 : \mathbb{R} \to \mathbb{R}$, we can also use $(2,)$ and $(3,)$ to define a function $f_2 : \mathbb{R} \to \mathbb{R}$. We use $(4,)$ and $(5,)$ to define a function $f_3 : \mathbb{R} \to \mathbb{R}$, etc.

There is another consequence of representing a real function as a set of real numbers. Given that any function $\mathbb{R} \to \mathbb{R}$ is a subset of $\mathbb{R}$, we can represent any function $\mathbb{R} \to (\mathbb{R} \to \mathbb{R})$ as a set of real numbers, also. For any finite amount of iterations, an object $\mathbb{R} \to (\mathbb{R} \to (\mathbb{R} \to (\mathbb{R} \to \cdots (\mathbb{R} \to \mathbb{R}) \cdots)))$ is a set of real numbers. In the next subsection, we describe objects of higher type. We will give an easy way of defining the type of any mathematical object, by using trees.

6.2 Trees

We have seen that natural numbers are the finite sets we can build recursively with the function $\oplus 1$. These sets can be well represented by finite tree structures. We will use trees to represent natural numbers first, then all types of objects. Our concept of set is equivalent to the concept of tree, we will define. A finite set number is an object that contains smaller set numbers. Every element of that set is in turn a set of set numbers, etc. The definition of trees is equivalent. We will think of a *trunk*, which is the principle node, as the set X. Every branch on that trunk is an element of the set X. For example, a single trunk with no branches is the set number 0. Suppose we know what tree X is, how do we find the tree corresponding to $X \oplus 1$? We add a branch that is a 0-tree (add 1 unit). So the set number 1 is a trunk with one 0-branch because $1 = \{0\}$; this branch has to be the tree representing 0. We can see this in Figure 6.

A tree is a graph of nodes and edges such that (i) We can identify a *trunk*: a principle edge with a finite number of *branches* attached to one of the nodes. All branches are attached to the same node of the trunk. (ii) Each branch on the tree is a tree. (iii) A single edge is a tree; we call it the 0-tree. The successor of a tree is obtained by adding a single edge to the trunk; attach a 0-tree to the trunk. Adding an edge to the 0-tree gives its successor, the 1-tree, which is two edges joined together at one node. Adding an edge to the 1-tree, we find its successor, the 2-tree, etc.

We need an extra rule for defining an equivalence class on finite trees. If a tree has two branches that are identical we substitute these two identical branches with a single branch, the successor. This process is called *reduction*. If a tree can be reduced to obtain another tree, they are in the same equivalence class. An irreducible tree is said to be in canonical form. Reducing the 2-tree, we find the canonical form. To reduce the 2-tree we substitute the two identical 0-trees with a single 1-tree. Adding a single edge to the result of that, we obtain the 3-tree in canonical form because there are no identical branches. If we add an edge to the 3-tree we have to apply reduction of branches, two times. We first take away the two 0-trees and add a 1-tree. But, we already had a 1-tree so now we have two identical 1-trees. We take those trees away and add a 2-tree. Every natural number is associated an equivalence class of finite trees, and a single canonical tree. Every branch on the canonical tree of a set number X corresponds to a natural number $k \in X$. Every tree is made up of smaller trees, and we give a well defined method of building trees. The canonical tree associated to the set number X, has $\#(X)$ many branches. Each branch is defined in the same way. A natural number is defined by its cardinality; and the cardinality of its elements; and the cardinality of the elements of its' elements; etc. We use trees to represent real numbers also. We simply use trees with infinite many branches. Each branch must be a finite tree and we do not allow these to be repeated. If the two branches are identical, we reduce the tree. Consider a third kind of tree, with infinite many branches. But, each of these branches is a tree of infinite branches. This is a collection of real numbers. In this next sub section we formalize the concept of types.
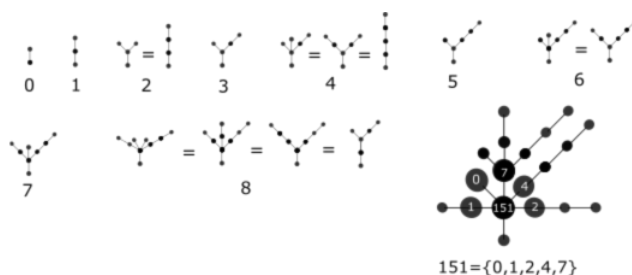
Fig. 6 Canonical trees can be built easily, given a set number. The canonical tree for $7 = \{0, 1, 2\}$ has three branches. One branch is the 0-tree, the second branch is the 1-tree and the third branch is the 2-tree. The canonical tree of $8 = \{3\}$ is a trunk with one branch, which is the 3-tree. The canonical tree of $151 = \{0, 1, 2, 4, 7\}$ has five branches: $0, 1, 2, 4, 7$-trees.

6.3 Type Theory

Finite trees are what we will call *objects of Type-0*. Trees of infinite branches with each branch being an object of type-0 are called *objects of Type-1*. For example, a real number is an object of Type-1 and a natural number is an object of Type-0. A tree whose branches are all objects of Type-1 is an *object of Type-2*. An example of an object of Type-2 is a set of real numbers. A tree with branches of Type-0 and Type-1 is an *object of Type-3*. This would be an object that has two types of elements. For example, a set consisting of natural and real numbers is an object of Type-3. An object of Type-4 is a tree with all its branches being objects of Type-2. An example of a Type-4 object is a family of sets of real numbers. For example, a *collection of subsets of $\mathbb{R}$* is an *object of Type-4*. In general, we build the Type-n objects in the same manner we build natural numbers.

The next step in classifying types of objects is to consider trees with infinite many types of branches. This means our tree has branches of Type-n_1, Type-n_2, Type-n_3... for infinite many types. This is called an *object of infinite Type-1,0*. An *object of infinite Type-1,1* is a tree that only has branches of infinite Type-1,0. An *object of Type-1,2* is a tree with all branches of Type-1,1. A tree with branches of both Type-1,0 and infinite Type-1,1 is an *object of infinite Type-1,3*. If all the branches of a tree are objects of Type-1,2, we say it is an *object of infinite Type-1,4*. We can construct all infinite Types-1,k.

Consider a tree whose branches are all objects of infinite type, and suppose there are infinite many types of objects of infinite type. We have objects of Type-1,n_1, Type-1,n_2, Type-1,n_3,.... A tree built with objects of infinite many infinite-types, is an object of infinite Type-2,0. Trees whose objects are only objects of Type-2,0 are called *objects of Type-2,1*. A tree with all objects of Type-2,1 is an *object of Type-2,2*. A tree with objects of Type-2,0 and Type-2,1 is an *object of Type-2,3*, etc.

Now we have objects of infinite Type-3,0, which are trees whose branches are of finite type and infinite type. A tree with objects of Type-3,0 is an object of Type-3,1, and so on. An object of infinite Type-4,0 is a tree with infinite many types of objects of Type-2,k. This means an object of Type-4,0 has objects of Type-2,n_1, Type-2,n_2, Type-2,n_3... for infinite many types 2,k. Of course an objects of Type 4,1 is a tree with branches of Type-4,0, etc. An infinite Type-5,0 object consists of branches of finite type and types 2,k. A Type-6,0 object consists of objects of types 1,k and types 2,k, etc. We continue in this manner until we have built all objects of Type-m,n, for every $m,n \in \mathbb{N}$. And, leave it at this for now.

Conclusions

The importance of the axiomatic base is usually undermined because it does not bring any new results or methods into most practical areas of mathematics. Instead, the axiomatic base of mathematics is seen as a *stone in the path*; an obstacle to be dealt with and forgotten. The axiomatic base we provide here differs from others in the fact that we acquire natural constructions for classic structures of mathematics. The construction we provide of natural numbers allowed a natural description of finite structures. Then we extended our methods to describe infinite mathematical objects. More results can be pursued in future work. This can include a thorough description of groups, rings, fields and linear spaces, in the finite and infinite cases. This work has only served as introduction of these set theoretic results in the area of finite groups. Another line of work will include a description of the calculus of real numbers. Revisions on the theory of types and the Continuum Hypothesis are also in order.

Algebraically, we are describing finite groups using natural numbers, in such a way that we have a good criteria for distinguishing finite groups. We have given a linear order, isomorphic to $\mathbb{N}$, to the set of all finite groups. This linear order of groups is well behaved with respect to cardinality. This order on finite groups organizes groups amongst each other. We are also provided with a method for organizing finite groups internally; we order the elements of any finite group through the canonical naming function. A criteria for defining equivalent objects in a group is also obtained. Given any finite group, we have to find a minimum set of independent equations that define the group. Finding all finite groups of n objects is still not trivial but we have a better notion of attacking this problem. We hace a method for proving isomorphism of two groups. We must build the canonical representation of both groups, and they should be the same natural number. Or simply put, the numerical table of the groups should be identical. There are a variety of ways for codifying the information of mathematical structures, and we have provided the data types for some structures, although this library of types must be completed. We briefly discuss the most general case, where we are using trees to represent any type of mathematical object. We describe the general procedure for expressing mathematical objects using the smallest type possible. For example, real functions have the same data type as sets of real numbers.

Computational aspects can also be treated with detail, focusing on finding physical methods to represent the arithmetic of Energy Levels. If this can be done, it could have applications in computing. We need a superposition rule to model the process carried out in the addition of two set numbers. Aside from classic computational schemes that can be improved, we can also think of modern computational schemes. Two options can be explored, initially. The first is the linear superposition of identical waves, which satisfies our numeric principle, $2^n + 2^n = 2^{n+1}$. The linear sum of two equally phased waves with equal wavelength and frequency, is equal a wave with double the amplitude. Thus, measuring the amplitude of waves can be used as a computational arithmetic model. This could provide a valid approach, for a linear optical quantum computing scheme. Encoding and storing mathematical objects (structures of information), at a quantum level, is a second option to be considered for future work. The N-particle problem is considered in terms of Fock States, which can be used to store information if the N-particles are *distinguishable*. The N particles must form an ordered sequence. Perhaps it is not necessary to consider particles of different species, but simply to consider particles with different values of some specific attribute. For example, instead of using the amplitude of the wave, we may use a sequence of photons $p_1, p_2, \ldots, p_N$ where the energies satisfy inequality $E_{p_1} < E_{p_2} < \cdots < E_{p_N}$, through time.

Acknowledgements Special Thanks to my Professors at undergraduate school. I am specifically thankful to Ms. Sofia Ortega Castillo who has helped me to prepare and organize this material, for talks given at the National Congress of Mathematics (2019, Monterrey, México), and encouraged me to pursue publication of the material. I am indebted to my professor in group theory, Alonso Castillo Ramírez who has assisted me with all kinds of questions that came up during the time I wrote some of the details. And, to my professor in analysis and probability theory, Victor Pérez Abreu Carreón who has always been a great teacher and friend, whose conversations and classes have inspired a great deal of the work I have tried to carry out. Any corrections or changes to be made are sole responsibility of the author.

References

[Ramirez(2019)] Ramírez, J.P. A New Set Theory for Analysis.*Axioms* **2019**, *8, 31.*

[Ramirez(2015)] Ramírez, J.P. Systems and Categories. *arXiv* **2015**, arXiv:1509.03649v5.

[Bernays(1991)] Bernays, P. *Axiomatic Set Theory*; Dover: New York, NY, USA, 1991.

[Benacerraf(1965)] Benacerraf, P. What Numbers Could Not Be. *Philos. Rev.* **1965**, *74*, 47–73.