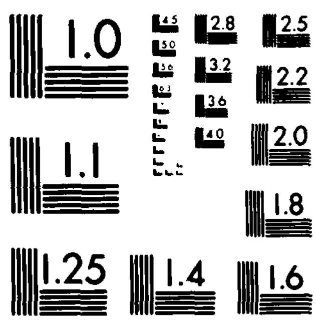
AD-A133 630 SYMMETRIC SET THEORY A GENERAL THEORY OF ISOMORPHISM 1/1
ABSTRACTION AND REPR..(U) MASSACHUSETTS INST OF TECH
CAMBRIDGE ARTIFICIAL INTELLIGENCE L..
UNCLASSIFIED D A MCALLESTER ET AL. AUG 83 AI-M-710 F/G 12/1 NL


1.0
2.8
2.5
3.2
2.2
3.6
4.0
2.0
1.1
1.8
1.25
1.4
1.6

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: AIM 710	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle): Symmetric Set Theory, A General Theory of Isomorphism, Abstraction, and Representation		5. TYPE OF REPORT & PERIOD COVERED: memorandum
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s): T. Poggio and B.L. Rosser		8. CONTRACT OR GRANT NUMBER(s): N00014-80-C-0505
9. PERFORMING ORGANIZATION NAME AND ADDRESS: Artificial Intelligence Laboratory, 545 Technology Square, Cambridge, Massachusetts 02139		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS: Advanced Research Projects Agency, 1400 Wilson Blvd, Arlington, Virginia 22209		12. REPORT DATE: August 1983
		13. NUMBER OF PAGES: 30
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office): Office of Naval Research, Information Systems, Arlington, Virginia 22217		15. SECURITY CLASS. (of this report): UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Distribution of this document is unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

Distribution is unlimited

18. SUPPLEMENTARY NOTES

None

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Set theory
Isomorphism
Essential Properties
Data Structures
Abstraction
Representation
Context

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

It is possible to represent a finite set of points (atoms) by a finite sequence of points. However a finite set of points has no distinguished member and therefore it is impossible to define a function which takes a finite set of points and returns a "first" point in that set. Thus it is impossible to represent a finite sequence of points by a finite set of points. The theory of symmetric sets provides a framework in which this observation about sets and sequences can be proven. The theory of symmetric sets is similar to classical (Zermello-Fraenkel) set theory with the exception that the universe of symmetric sets includes points

- I -

Massachusetts Institute of Technology
Artificial Intelligence Laboratory

AI Memo No. 710 August 1983

Symmetric Set Theory
A General Theory of Isomorphism, Abstraction, and Representation

by

David Allen McAllester

Abstract:

It is possible to represent a finite set of points (atoms) by a finite sequence of points. However a finite set of points has no distinguished member and therefore it is impossible to define a function which takes a finite set of points and returns a "first" point in that set. Thus it is impossible to represent a finite sequence of points by a finite set of points. The theory of symmetric sets provides a framework in which this observation about sets and sequences can be proven. The theory of symmetric sets is similar to classical (Zermello-Fraenkel) set theory with the exception that the universe of symmetric sets includes points (ur-elements). Points provide a basis for general notions of isomorphism and symmetry. The general notions of isomorphism and symmetry in turn provide a basis for natural, simple, and universal definitions of abstractness, essential properties and functions, canonicality, and representations. It is expected that these notions will play an important role in the theory of data structures and in the construction of general techniques for reasoning about data structures.

Keywords: Set Theory, Abstraction, Symmetry, Representation, Essential Properties, Context, Metamathematics.

This report describes work done at the Artificial Intelligence Laboratory of the Massachusetts Institute of Technology. Support for the laboratory's artificial intelligence research is provided in part by the Advanced Research Projects Agency of the Department of Defense under Office of Naval Research contract N00014-80-C-0505

Acknowledgments: There are many people who supported and encouraged this work. In many ways this work provides a precise account of intuitions derived from discussions with Gerald Sussman. Discussions with David Israel, Rusty Bobrow, Pat Hayes, David Chapman, John Lamping, and Andrew Haas have also been very helpful. Much of the inspiration and intuition behind this work was derived from listening to Gian-Carlo Rota talk about the importance of viewing mathematical objects as tools.

CONTENTS

1. INTRODUCTION

Finite sets of points can be represented by finite lists of points, but it is impossible to represent finite lists of points with finite sets of points. This is because a set of points has no distinguished member and therefore it is impossible to define a function which maps a set of points to a "first" point in that set. While this simple observation seems straightforward and correct, it is very difficult to prove. What is meant by "represent" or by "a distinguished member"? Intuitively a list has more structure or contains more information than a set. But what does this mean? One approach to defining the meaning of "representations", "distinguished members" and "more structure" is to study the general nature of mathematical objects (such as sets and sequences). One approach to the general nature of mathematical objects is set theory. Symmetric set theory is a new set theory which provides simple universal definitions of the above notions.

Currently the most widely studied formal theory of mathematics as a whole is Zermello-Fraenkel set theory (ZF) and its variants. The primary difference between ZF set theory and symmetric set theory involves *points*. A point is an object which has no members (and is thus not a set). In ZF set theory there is only one point (the null set) while symmetric set theory requires the existence of many points. The following discussion of this issue is from the introduction to **Foundations of Set Theory** by Fraenkel, Bar-Hillel, and Levy [Fraenkel et. al. 58] (they refer to points as individuals).

> Let us refer to those elements which have members as *sets* and to those elements which have no members as *individuals*. ...
>
> The existence of at least one individual is called for by both philosophical and practical reasons. ... Let us, however, stress that referring to one of the individuals as the null set is done only for reasons of convenience and simplicity, and can be regarded as a mere notational convention.
>
> Having decided that we need an individual we now face the question of whether we need *more than one* individual. It turns out that for mathematical purposes there seems to be no real need for individuals other than the null set. Therefore we shall not admit any such individuals into ZF.

While it is true that most mathematics can be done in a framework where the null set is the only point there are notions which are best defined in a framework where many points are present. For example every mathematical object seems to have a natural notion of isomorphism associated with it. There is a natural notion of what it means for two Turing machines, or context free grammars, or topological spaces to be isomorphic. ZF set theory provides no satisfactory general notion of isomorphism. The terms "representation", "distinguished element", and "more structure" are very hard to define in a framework where only one point is present. However these notions can be given simple universal definitions in the presence of many points.

The notion of isomorphism can be approached from two different directions. The first is to extend standard notions of isomorphism for particular types of objects to a notion of isomorphism for arbitrary sets which are built up out of points. This type of isomorphism will be called a structural isomorphism. The second approach to the notion of isomorphism is to consider the symmetries (automorphisms) of a universe

$\langle U\ \in \rangle$. A pair $\langle U\ \in \rangle$ is a universe of objects where U is a universal domain and $\in$ is a binary relation on U where $x \in y$ is read "x is an element of y". A point of $\langle U\ \in \rangle$ is an element p of U such that there is no x in U such that $x \in p$. The universe of symmetric sets has lots of points and lots of automorphisms. In particular there is a natural one to one correspondence between the the permutations of the points of $\langle U\ \in \rangle$ and the automorphisms of $\langle U\ \in \rangle$ (since ZF set theory allows only one point there are no non-trivial symmetries of $\langle U\ \in \rangle$ in ZF set theory). In the theory of symmetric sets it can be shown that two objects x and y are structurally isomorphic just in case there is an automorphism (a symmetry) of $\langle U\ \in \rangle$ which maps x to y. This result justifies the intuition that isomorphic objects are indistinguishable.

Philosophers of mathematics have observed that mathematical descriptions of structures such as the natural numbers do not determine the identity of those structures [Benacerraf 65]. The best one can hope to do is to determine identity "up to isomorphism". The theory of symmetric sets reflects this observation. A specification for a particular object x might be a sentence Φ such that $\Phi(y)$ holds just in case y is x. However consider any first order formula Φ of one free variable whose only non-logical symbol is $\in$. If x and y are isomorphic objects then there is a symmetry of $\langle U\ \in \rangle$ which maps x to y and thus $\Phi(x)$ holds in $\langle U\ \in \rangle$ just in case $\Phi(y)$ holds in $\langle U\ \in \rangle$. Thus if there are several different objects which are isomorphic to x then no such sentence Φ can name x. In the theory of symmetric sets there are always *many* objects which are isomorphic to x.

The theory of symmetric sets provides a simple and natural measure of the "abstractness" of objects. A more abstract object is an object with "less structure". A precise definition of this notion can be approached in three different ways. First the symmetries of the universe of symmetric sets greatly restricts the predicates and functions which can be defined in terms of the structure of $\langle U\ \in \rangle$. A function F will be called essential if it commutes with any symmetry (automorphism) of $\langle U\ \in \rangle$, i.e. for any symmetry ρ of $\langle U\ \in \rangle$ and any element x of U, $\rho(F(x))$ must equal $F(\rho(x))$. Given two elements x and y of U there may not exist any essential function F which maps x to y. For example there is no essential function which maps a set of points to an element of that set. An object y is called *an abstraction* of an object x just in case there is an essential function F which maps x to y. This notion of abstraction can also be approached by studying the symmetries of particular objects. The symmetry group of an object x, denoted $\Delta(x)$, is the set of all automorphisms of $\langle U\ \in \rangle$ which leave x fixed. The notion of an abstraction can also be defined by saying that y is an abstraction of x just in case $\Delta(y)$ contains $\Delta(x)$. A third approach to the notion of abstraction is via the notion of contextual isomorphism and the general notion of a "canonical" object. Two objects x and y are said to be isomorphic in the context of z just in case there is a symmetry of z which maps x to y. For example consider a circle and two points p and q which are in the same plane as the circle. The points p and q are isomorphic in the context of the circle just in case they are the same distance from the center of the circle. An object y is said to be *canonical* in the context of an object z just in case the isomorphism class of y in the context of z, $|y|_z$, is a singleton set (there is no canonical point on a circle or canonical corner on a square). It turns out that y is an abstraction of x just in case y is canonical in the context of x.

Given the above notion of abstractness it is possible to provide a precise notion of "representation". For example finite sets can be represented as finite sequences because there is an essential function which maps any sequence to to the corresponding set. However it is easy to show that there is no essential function which maps finite sets of points to finite sequences of points. Thus sequences can not be represented as sets.

Mathematics is often done in the framework of some fixed but arbitrary context. Intuitively a context is a collection of objects which are taken to be fixed during the course of a mathematical discussion. The natural numbers, the real numbers, and the empty set are all usually assumed to be fixed objects even though their "true identity" can not be specified. The result relating essential functions, symmetry groups, and canonical objects can be generalized to account for context.

In addition to the different treatment of points there is another less important distinction between symmetric set theory and ZF set theory. The axioms of ZF set theory are (an infinite number of) sentences of first order logic while the axioms of symmetric set theory are precise conditions on the universe $\langle U\ \in \rangle$ which are stated in English rather than first order logic. Thus symmetric set theory avoids all of the clumsiness of first order logic. Furthermore it is shown in an appendix that a simple extension of the axioms of symmetric set theory specify the structure of $\langle U\ \in \rangle$ up to isomorphism, something which could never be done in first order logic.

2. THE AXIOMS OF SYMMETRIC SET THEORY

In deciding on axioms for a universe of mathematical objects there are several considerations. First the axioms should be as clear, simple, and natural as possible. Second, since ZF set theory is well established the axioms should not differ unnecessarily from ZF set theory. Finally, and most interestingly, the axioms should provide a basis for defining universal notions of isomorphism, abstraction, and representation. However one should not expect to immediately see how the axioms of symmetric set theory provide a basis for general notions of isomorphism, abstraction, and representation. These notions can be defined only after the consequences of the simple set theoretic axioms have been investigated.

No proof of the consistency of the axioms of symmetric set theory is presented in this section. However it is shown in an appendix that the consistency of the axioms is equivalent to the existence of a strongly inaccessible cardinal. The appendix also shows that any universe satisfying the axioms is determined up to isomorphism by a "height" and a "width" where the height can be any strongly inaccessible cardinal and the width can be any cardinal at least as large as the height. Thus if there are strongly inaccessible cardinals then there are many different (non-isomorphic) universes satisfying the axioms. There is however a unique (up to isomorphism) *minimal* universe $\langle U \in \rangle$ whose height and width are both the least strongly inaccessible cardinal. Throughout the following sections however the universe will be taken to be some fixed but arbitrary model of the axioms.

2.1. The Nature of the Universe $\langle U \in \rangle$

The universe of symmetric sets is taken to be a pair $\langle U \in \rangle$ where U is some domain and $\in$ is a binary relation on U. Some elements of U can be thought of as sets in the standard way. For example consider the pair $\langle U \in \rangle$ given as follows:

U is the set {a b c d e f}. The relation $\in$ is given by:

$$a \in d \quad b \in d \quad c \in d$$
$$a \in e \quad b \in e$$
$$a \in f \quad c \in f$$

In this situation a, b, and c are points.

Definition: A *point* is an element p of U which has no members, i.e. $x \notin p$ for all x in U.

In the above example the element d represents the set {a b c}, e represents the set {a b}, and f represents the set {a c}. Note that the relationship between d and the set {a b c} is given by the relation $\in$

and can not be defined purely in terms of the set U or the element d. Not all subsets of U need have representations in U. In the above example there is no representation for the set {e f}.

Definition: A subset C of U is *represented* in <U ∈> just in case there is an element z of U such that x∈z just in case x is in C; in this case z is called a representation of C.

It is important to note that the notion of representation expressed in the above definition is not the same as the notion of representation intended in the title of this paper. A more general notion of representation will be presented section four. However in this section the term "representation" will be used only in the sense given in the above definition.

The axioms of the theory of symmetric sets imply that the universe U is not empty. While a special axiom to this effect is not needed, the fact that U is not empty will be emphasized with an explicit axiom.

Axiom zero: U is non-empty.

The first axiom of symmetric set theory is that representations are unique.

Axiom One, Extensionality: Representations of non-empty sets are unique, i.e. for any non-empty subset C of U there is at most one element x of U which represents C.

The universe <U ∈> should be thought of as containing representations for tuples, functions, and relations as well as representations for subsets of U. For example if x and y are elements of U then z will be called a representation for the pair <x y> just in case z represents the set {x {x y}}, or more precisely z represents a set {x w} where w represents the set {x y}. Functions and relations are represented by sets of tuples in the standard way (or more precisely a function is represented by a set of elements of U each of which represents a tuple). Again the term "representation" is being used here in a different sense from that intended in the title of the paper and a more general definition is given in section four.

2.2. The Comprehension Axioms

Given the above axioms it is possible that U contains only points, i.e. that no element of U represents a non-empty subset of U. Axioms that require that certain non-empty subsets of U be represented in <U ∈> are called comprehension axioms. The first comprehension axiom makes use of the following definition:

Definition: A subset C of U will be called *small* just in case there is some subset C' of U which is represented in <U ∈> such that the cardinality of C' is as big as the cardinality of C. A subset C of U which is not small will be called *large*.

By definition every subset C of U which is represented in $\langle U \in \rangle$ is small. However it has not been guaranteed that every small subset of U is represented in $\langle U \in \rangle$. This is the first comprehension axiom.

Axiom Two, Strong Comprehension: Every small subset of U is represented in $\langle U \in \rangle$.

The above comprehension axiom implies that the cardinality of a subset C of U determines whether or not C is represented in $\langle U \in \rangle$. If C is small then it is represented in $\langle U \in \rangle$, if it is large then it is not. This leads to the following lemma:

Lemma 2.1: If two element sets are small then for any small subsets C and C' of U *all* functions from C to C' are represented in $\langle U \in \rangle$.

Proof: An ordered pair $\langle x\ y \rangle$ of elements of U is taken to be the set {x {x y}}. Thus if two element sets are small any ordered pair of elements of U is represented in $\langle U \in \rangle$. Any function from C to C' is a set of such pairs with the same cardinality as C and is therefore a small subset of U.

One model of the above comprehension axiom is a universe $\langle U \in \rangle$ where U is infinite and a non-empty subset C of U is small just in case it has less than seven members. To rule out such a universe some further axioms are needed.

Axiom Three, Infinity: There exists an element of U which represents a countably infinite subset of U.

Axiom Four, Power Set: If a subset C of U is small then any subset of U with the cardinality of the power set of C is also small.

Axiom Five, Union: A small union of small sets is small, i.e. for any family *F* of subsets of U if *F* is small (has cardinality less than or equal to some small subset of U) and if each set in *F* is small then the union of all sets in *F* is also small.

There is one final comprehension axiom which does not correspond to any axiom of ZF set theory. This final axiom will turn out to be important in later sections.

Definition: P(U) is the set of all points in $\langle U \in \rangle$.

Axiom Six, Point Comprehension: P(U) is large.

This axiom implies that for any small subset C of U there is a set *of points* C' which is the same size as C. Since both C and C' are small lemma 2.1 implies that the bijections (one to one onto functions) from C to C' are represented in $\langle U \in \rangle$. Thus any small set can be "identified" with a set of points.

2.3. The Foundation Axiom

The Foundation axiom is the final axiom of the theory of symmetric sets. It states that there are no infinitely decreasing membership chains.

Axiom Seven, Foundation: There is no infinitely decreasing sequence of elements of U, i.e. there is no infinite sequence $x_1 \ni x_2 \ni x_3 \ni \ldots$

The foundation axiom has important implications. It implies that there is no element x of U such that $x \in x$ (otherwise the infinite sequence all of whose elements were x would be an infinite decreasing sequence). In fact there can be no containment loops, i.e. no sequence $x_1 \in x_2 \in \ldots x_n$ such that $x_n \in x_1$. The foundation axiom is equivalent to the statement that every subset C of U contains a lower bound under $\in$, i.e. any subset C of U contains a lower bound x such that there is no y in C such that $y \in x$. The foundation axiom can also be characterized in terms of the transitive closure of $\in$.

Definition: The binary relation $\in^+$ is defined to be the transitive closure of $\in$, i.e. for any two elements x and y of U, $y \in^+ x$ just in case $y \in x$ or there is some finite sequence z_1, z_2, ... z_n such that $y \in z_1 \in z_2 \in \ldots z_n \in x$.

The foundation axiom ensures that the relation $\in^+$ is a partial order on U and that $\in^+$ is well founded. The fact that $\in^+$ is a well founded partial order on U allows one to define functions on U by recursion on $\in^+$. For example it is possible to define a function P which maps every element of U to its underlying set of points. This function is defined by recursion on $\in^+$ as follows:

Definition of the function P:

$$P(q) = \{q\} \text{ for any point } q$$

$$P(x) = \cup_{y \in x} P(y) \text{ for any non-point } x$$

Thus for any element x of U we can talk about the points P(x) of the element x. Note that P(x) is always a subset of U rather than being any particular element of U (in fact P(x) is always a subset of P(U), the set of all points). It is not immediately obvious that for any element x of U the set P(x) is small and therefore represented in $\langle U \in \rangle$. However this does follow from the axioms presented so far.

Theorem 2.2: For any element x of U, the set P(x) is small.

Proof: The proof is by induction on $\in^+$. For a point p the set P(p) is just {p} which is clearly small. Now consider any element x of U which is not a point and such that for every y such that $y \in^+ x$, P(y) is small. P(x) equals the union over $y \in x$ of P(y) and therefore P(x) is a small union of small sets and must be small.

3. ISOMORPHISMS

A point is that which has no part.
- Euclid

It seems that every precisely defined object has a natural notion of isomorphism associated with it. For example graphs, context free grammars, Turing machines, and topological spaces all have a natural associated notion of isomorphism. All of these notions of isomorphism are based on identifications between the points of one object and the points of another. This observation motivates a notion of structural isomorphism defined for arbitrary elements of the universe $\langle U\ \in\rangle$ of mathematical objects.

It is intuitively clear that isomorphic mathematical objects are in some sense identical. The strongest sense in which two elements x and y of U can be identical is if there is some symmetry (automorphism) of $\langle U\ \in\rangle$ which maps x to y. It turns out that under the aforementioned notion of structural isomorphism two objects are structurally isomorphic just in case there is a symmetry of $\langle U\ \in\rangle$ which maps one to the other.

The notion of isomorphism can be generalized to take into account an arbitrary but fixed context. At one level any two points p and q are isomorphic. However if p and q appear in some fixed context then p and q need not be considered isomorphic. For example p and q are isomorphic in the context of the set $\{p\ q\ \{r\ s\}\}$ but they are not isomorphic in the context of the set $\{p\ \{q\ r\}\}$. It turns out that for any element z of U which is taken as a fixed context there is a natural and general definition for when two elements of U are isomorphic in the context of z.

The universe $\langle U\ \in\rangle$ is intended to be a model of the universe of all mathematical objects. For this reason the term "object" will be used as a synonym for the phrase "an element of U".

3.1. The Symmetries of $\langle U\ \in\rangle$

An automorphism or symmetry of $\langle U\ \in\rangle$ is a one to one onto map ρ from U to U (a permutation of U) such that for any x and y in U, $\rho(x)\in\rho(y)$ just in case $x\in y$. It can be shown that for any symmetry ρ of $\langle U\ \in\rangle$ and any object x, $\rho(x)$ is a point just in case x is a point. Thus for any symmetry ρ of $\langle U\ \in\rangle$ the restriction $\rho|P(U)$ of ρ to the points P(U) is a one to one onto map from P(U) to P(U), i.e. $\rho|P(U)$ is a permutation of P(U). The first important theorem concerning the symmetries of $\langle U\ \in\rangle$ is that each symmetry is determined by its corresponding permutation of P(U).

> *Theorem 3.1*: If ρ and ρ' are two symmetries of $\langle U\ \in\rangle$ such that $\rho|P(U)$ equals $\rho'|P(U)$ then ρ equals ρ'.

Proof: The proof is by induction on $\in^+$. By assumption ρ and ρ' are the same function on points. Consider any x in U such that ρ and ρ' have the same value on all elements y of U such that $y\in^+x$. Since ρ preserves the membership relation the set represented by $\rho(x)$ equals $\{\rho(y)\colon y\in x\}$. Similarly the set represented by $\rho'(x)$ equals $\{\rho'(y)\colon y\in x\}$. But since ρ and ρ' are the same function on all $y \in^+ x$, $\rho(x)$ and $\rho'(x)$ must represent the same set. Thus by extensionality $\rho(x)$ must equal $\rho'(x)$.

Any symmetry of $\langle U\ \in \rangle$ determines a permutation of P(U) and theorem 3.1 shows that the induced permutation of P(U) uniquely determines the symmetry. It can also be shown that *every* permutation of P(U) corresponds to a symmetry of $\langle U\ \in \rangle$.

Theorem 3.2: Any permutation ρ of P(U) can be extended to a symmetry of $\langle U\ \in \rangle$.

Proof: Let ρ be any permutation of P(U). The extension of ρ to all of U is defined by induction on $\in^+$ via the following relation:

$$\rho(x) \ = \ \text{the representation of } \{\rho(y)\text{: } y \in x\}$$

The set $\{\rho(y): y \in x\}$ is guaranteed to be represented in $\langle U\ \in \rangle$ because it can be no larger than the set represented by x. It follows from the above equation that if $y \in x$ then $\rho(y) \in \rho(x)$ and further if $\rho(y) \in \rho(x)$ then $y \in x$. It remains only to show that the extension of ρ to all of U is one to one and onto. Consider the inverse permutation ρ^{-1} of P(U) and the extension of this inverse to all of U. It can be shown by a standard induction on $\in^+$ that $\rho^{-1}(\rho(x))$ equals x for all x in U and thus the extension of ρ is one to one. Similarly it can be shown that $\rho(\rho^{-1}(x))$ must equal x and thus the extension of ρ is onto.

Theorems 3.1 and 3.2 imply that there is a natural one to one relationship between the permutations of the points P(U) and the symmetries (automorphisms) of $\langle U\ \in \rangle$. In classical set theory there is only one point and there is only one symmetry of $\langle U\ \in \rangle$, namely the identity function.

If there is a symmetry of $\langle U\ \in \rangle$ which maps x to y then x and y are truly indistinguishable. More concretely let Φ be any first order formula of one free variable whose only non-logical symbol is $\in$. If there is a symmetry of $\langle U\ \in \rangle$ which maps x to y then $\Phi(x)$ holds in $\langle U\ \in \rangle$ just in case $\Phi(y)$ holds in $\langle U\ \in \rangle$.

Theorem 2.2 says that for any object x the set P(x) is small and thus P can be thought of as a mapping from U to U. A simple induction on $\in^+$ can be used to show that the mapping P commutes with symmetries of $\langle U\ \in \rangle$, i.e. that for any symmetry ρ of $\langle U\ \in \rangle$ and any object x, $P(\rho(x))$ equals $\rho(P(x))$.

Lemma 3.3: For any symmetry ρ of $\langle U\ \in \rangle$ and any object x, $P(\rho(x))$ equals $\rho(P(x))$.

3.2. Structural Isomorphisms

There is a natural definition for what it means for two graphs, or languages, or lists of points to be isomorphic. All of these objects can be represented by elements of U and it would be nice if the notion of isomorphism which is defined for elements of U corresponded to the natural notion of isomorphism for such objects. This observation leads to the definition of *structural* isomorphism presented below.

Any two points have the same structure simply because neither has any structure. Larger objects are structurally isomorphic just in case there is an identification between the points of the objects which preserves the structure of those objects. For example let p, q, r, and s be any four distinct points. The set $\{p\ q\}$ is isomorphic to the set $\{r\ s\}$, but not the set $\{r\ s\ p\}$. In fact any two sets *of points* are isomorphic just in case they have the same number of elements. The triple $\langle p\ p\ q \rangle$ is isomorphic to the triple $\langle r\ r\ s \rangle$ but not to the triple $\langle r\ s\ s \rangle$.

To define the notion of structural isomorphism precisely it is necessary to build up some terminology. Let C be any set of points. U(C) is defined to be the set of all elements x of U such that P(x) is a subset of C. Thus U(C) is the set of objects which are built up out of the points in C. Let ρ be any function mapping C to arbitrary points. Any such function ρ can be extended to a function ρ' defined on all of U(C) via the following inductive definition:

$$\rho'(p) \;=\; \rho(p) \text{ for points p}$$

$$\rho'(z) \;=\; \text{The representation of } \{\rho'(y)\text{: } y \in z\} \text{ for any non-point } z \text{ in U(C).}$$

For example if $\rho(p)$ is r and $\rho(q)$ is s then $\rho'(\langle p\ q \rangle)$ is $\langle r\ s \rangle$. Thus the function ρ' "replaces" the points of an object by their image under ρ. In the inductive definition of $\rho'(z)$ the set $\{\rho'(y)\text{: } y \in z\}$ is guaranteed to be represented in $\langle U\ \in \rangle$ because it can be no larger than the set represented by z. In the following discussion any function ρ defined on the points C will be assumed to be defined in the above way on all of U(C).

> *Definition*: A *structural isomorphism* between two elements x and y of U is a bijection ρ from P(x) to P(y) such that $\rho(x)$ equals y (any function defined on P(x) will be assumed to be defined on x via the above relation). The elements x and y are said to be *structurally isomorphic* just in case there exists a structural isomorphism between them.

As an example let a group $\langle G\ \circ \rangle$ be a pair of a set of points G and a function $\circ$ from $G \times G$ to G satisfying the standard axioms for a group. Notice that $P(\langle G\ \circ \rangle)$ equals G. Now consider two groups $\langle G\ \circ \rangle$ and $\langle G'\ \circ' \rangle$ and let ρ be any bijection from G to G'. Clearly $\rho(G)$ equals G' so $\rho(\langle G\ \circ \rangle)$ equals $\langle G'\ \rho(\circ) \rangle$. Thus the bijection ρ is a structural isomorphism between $\langle G\ \circ \rangle$ and $\langle G'\ \circ' \rangle$ just in case $\rho(\circ)$ equals $\circ'$. Since functions are represented by sets of tuples an element of $\circ$ is a triple of points $\langle p\ q\ r \rangle$ where r is the value of $p \circ q$. Thus $\rho(\circ)$ is a set of triples of the form $\langle \rho(p)\ \rho(q)\ \rho(r) \rangle$. The set of triples $\rho(\circ)$ will equal the set of triples $\circ'$ just in case for any triple $\langle p\ q\ r \rangle$ in $\circ$ the triple $\langle \rho(p)\ \rho(q)\ \rho(r) \rangle$ is in $\circ'$, i.e. just in case $\rho(r)$ equals $\rho(p) \circ' \rho(q)$. This statement is equivalent to the condition that $\rho(p) \circ' \rho(q)$ equals $\rho(p \circ q)$ which corresponds to the standard notion of isomorphism between groups.

The notion of a structural isomorphism can be related to the symmetries of $\langle U\ \in \rangle$. It has already been shown that there is a natural one to one correspondence between the automorphisms of $\langle U\ \in \rangle$ and the permutations of P(U). The following theorem relates bijections between sets of points and permutations of P(U).

Theorem 3.4: Any bijection between two small sets of points can be extended to a permutation of all of P(U).

Proof Sketch: Let C and C' be any two small sets of points and let ρ be any bijection from C to C'. Let p be any member of either C or C'. Since C and C' need not be disjoint p may be in both C and C' and thus both $\rho(p)$ and $\rho^{-1}(p)$ may be defined. In general any point p in either C or C' is contained in some minimal chain of the form ... $\rho^{-1}(\rho^{-1}(p)), \rho^{-1}(p), p, \rho(p), \rho(\rho(p))$... (more precisely the minimal chain containing p is the least subset of C∪C' which contains p and is closed under ρ and ρ^{-1}). The minimal chain containing p can be one of four types. First it might be a loop, in which case ρ is already a permutation of the minimal chain containing p. Second it might be infinite in both direction in which case ρ is also already a permutation of the chain. Third the chain may have a "first" member which is in C but not in C' and a last member which is in C' but not in C. Finally the minimal chain containing p may have only one endpoint, either a starting point or an ending point. In these cases ρ is not a permutation of the minimal chain containing p. To remedy this situation one can extend the function ρ to more points and convert any chain of the these last types into either a cycle or a chain which is infinite in both directions. To make such an extension there must be enough points in P(U) which are not in C or C'. But since both C and C' are assumed to be small this last condition can be readily shown.

The main result of this section can now be proven.

Theorem 3.5 Two elements x and y of U are structurally isomorphic just in case there is a symmetry of <U ∈> which maps x to y.

Proof: If x and y are structurally isomorphic then there is a bijection ρ from P(x) to P(y) which maps x to y. Any extension of ρ to more points will still map x to y. Thus theorem 3.4 implies that ρ can be extended to a permutation of P(U) which maps x to y. On the other hand if there is a permutation ρ of P(U) which maps x to y lemma 3.3 implies that $P(\rho(x))$ equals $\rho(P(x))$ so $\rho(P(x))$ equals P(y) and thus ρ maps P(x) onto P(y). Thus the restriction of ρ to P(x) is a bijection from P(x) to P(y) which maps x to y.

Theorem 3.5 demonstrates that the two natural notions of isomorphism between symmetric sets coincide. Thus there is never any ambiguity in what is meant by two elements of U being isomorphic.

3.3. Symmetry and Contextual Isomorphisms

Since there is a natural notion of isomorphism for elements of U there is also a natural notion of automorphism or symmetry. For example there are two structural symmetries of {p q}, the identity map on the points p and q and the function which exchanges p and q. Since any structural isomorphism can be extended to a symmetry of <U ∈> there is no need to distinguish between structural isomorphisms and permutations of P(U).

Definition: The symmetry group of an object x, denoted $\Delta(x)$, is the set of all permutations ρ of P(U) such that $\rho(x)$ equals x.

There is a contextual notion of isomorphism where two objects x and y are isomorphic in a context z just in case x and y bear exactly the same relationship to z. For example let z be the set {p q {r s}} where p, q, r, and s are points. Clearly the point p is just like the point q with respect to z (both p and q are members of z and neither is a member of a member of z). Similarly the point r is just like the point s with respect to z. On the other hand p is not like the point r since p is a member of z while r is not.

As another example let y be the set {<p q> <q r> <r p>}. This represents a directed graph with nodes p, q, and r and edges from p to q, q to r, and r to p. In other words y represents a cyclic directed graph of three nodes. Notice that every node of y looks like every other node. More precisely y has three structural symmetries corresponding to three rotations of the graph. For any two nodes there is a rotation which maps one to the other.

> *Definition*: Two objects x and y will be called isomorphic in the context of an object z just in case there is a symmetry ρ of z such that $\rho(x)$ equals y. The set of things isomorphic to y in the context of z will be denoted $|y|_z$.

4. ABSTRACTION, REPRESENTATION, AND OTHER APPLICATIONS

There is an informal distinction in mathematics between essential and contextual properties. For example consider an open set of some topological space. The fact that the set is open is a contextual property of that set while the cardinality of the set is an essential property. In the framework of symmetric sets this distinction is easily made precise. Any two isomorphic objects have the same essential properties. An essential predicate Φ is any predicate on U such that $\Phi(x)$ is equivalent to $\Phi(\rho(x))$ for any object x and point permutation ρ. An essential function is one that commutes with automorphisms of $\langle U\ \in \rangle$, i.e. $F(\rho(x))$ always equals $\rho(F(x))$.

In mathematics one often encounters a notion of a "canonical" or "natural" transformation or relationship. For example a set of points has no natural or canonical element, there is no natural or canonical point on a circle, and a square has no canonical corner. On the other hand one can choose a canonical element of an ordered pair. One particularly well known example is the dual space of a linear vector space. The dual space D(X) of a linear vector space X is the set of linear functions from X to scalars. If there is a dot product operation • defined on X then there is a natural isomorphism between X and D(X) where the linear function associated with a vector x is $\lambda y.x{\bullet}y$. However if no dot product operation is specified for X then while X and D(X) are still isomorphic there is no natural or canonical isomorphism. On the other hand there is always a canonical or natural isomorphism between X and D(D(X)). A simple and natural definition for this notion of canonical is given by saying that y is canonical in the context of x just in case the isomorphism class of y in the context of x, $|y|_x$, contains only one object.

The theory of symmetric sets provides a simple general measure of the abstractness of objects. An object y can be said to be an abstraction of an object x just in case any one of the following three conditions hold: $\Delta(y)$ contains $\Delta(x)$, $|y|_x$ is a singleton set, or y equals F(x) for some essential function F. It turns out that these three criterion are equivalent and there is no ambiguity in what is meant by y being an abstraction of x.

There are many representation theorems in mathematics. For example every Boolean algebra can be represented by an algebra of sets. Of course the notion of a representation is also heavily used in computer science where alphabets are represented as binary codes and sets are represented as lists. This raises the natural question of what is meant in general by a representation. The theory of symmetric sets provides a natural framework in which to develop a general theory of representation.

Mathematicians often talk about fixed but arbitrary structures which form a context in which to investigate other structures. For example the natural numbers are assumed to be a fixed set even though their "true identity" can never be specified. The same holds for the real and complex numbers. Another example of contextual objects are the fixed constants "true" and "false" which are used in discussions of logic. Still another example from logic is the fixed but arbitrary alphabet from which the sentences of logic are constructed. Even the "empty set" can be viewed as an object which is taken to be fixed but whose identity is never specified. The general notion of a context can be handled in a natural way in the theory of symmetric sets. A context is an object z (which may have lots of internal structure) which is "taken to be fixed". This means that only symmetries of z are considered when talking about isomorphisms, symmetry groups, essential properties, and canonical objects.

4.1. Essential Functions, Canonicality, and Abstraction

The set {p q} can be thought of as essential property of the pair ⟨p q⟩. That is to say that given a pair of points one can derive in a natural way a set of two points. The reverse does not seem to hold, given a set of two points there is no natural or canonical way to derive a pair of two points. Similarly given a point p there is no natural or canonical set of two points which contains p. Conversely given a set of two points there is no natural or canonical element of that set. Recall that for any objects y and z, $|y|_z$ is the set of all things isomorphic to y in the context of z, i.e. $|y|_z$ is the set of things which can be written as $\rho(y)$ for some symmetry ρ of z.

Definition: An object y will be called *canonical* in the context of an object z just in case $|y|_z$ is a singleton set.

There are many intuitive examples of objects which are not natural or canonical. There is no natural or canonical point on the perimeter of a circle. There is no canonical corner on a square. There is no natural or canonical coordinate system for three dimensional space. On the other hand consider an oblique triangle (where no two sides have the same length). One can choose a canonical vertex for such a triangle by choosing the vertex connecting the two shorter sides.

There is another intuitively satisfying notion of what a canonical object is. Intuitively y is canonical in the context of z if one can define a function which takes z and unambiguously returns y. This notion of a canonical object is problematic because for any two objects z and y there is a function which maps z to y. However one wants a *definable* function. Remember that the universe ⟨U ∈⟩ has many non-trivial automorphisms and every function from U to U which is defined in terms of the structure of the universe ⟨U ∈⟩ must respect those automorphisms. In particular any function F defined in terms of the structure of ⟨U ∈⟩ must be *essential* in the following sense:

Definition: A function F from U to U will be called *essential* just in case for every symmetry ρ of ⟨U ∈⟩ and every element x of U, $F(\rho(x))$ equals $\rho(F(x))$.

Intuitively the image of an object x under an essential function F can contain no more information than the object x itself. Thus it might be said that F(x) is an abstraction of x.

Definition: An object y will be called *an abstraction* of an object z just in case y equals F(z) for some essential function F.

The main result of this section relates the the notion of canonicality, the notion of abstraction, and the symmetry groups of objects.

Theorem 4.1, The First Abstraction Theorem: For any objects y and z the following are equivalent:

1) $\Delta(y)$ contains $\Delta(z)$.
2) $|y|_z$ is a singleton set.
3) y equals F(z) for some essential function F.

Proof:
1<=>2: If $\Delta(y)$ contains $\Delta(z)$ then for any symmetry ρ of z, $\rho(y)$ equals y so $|y|_z$ contains only y. On the other hand if $|y|_z$ is a singleton set then $\rho(y)$ equals y for any symmetry ρ of z so $\Delta(z)$ is a subset of $\Delta(y)$.

1=>3: Given that $\Delta(y)$ contains $\Delta(z)$ an essential function F from U to U can be defined as follows: Of course F(z) is defined to be y. For any w which is isomorphic to z let ρ be some point permutation such that $\rho(z)$ equals w and define F(w) to be $\rho(y)$ (this is equivalent to defining $F(\rho(z))$ to be $\rho(F(z))$ for any point permutation ρ). It must be shown that this definition of F(w) is independent of the choice of ρ. In particular if ρ and ρ' are two point permutations such that $\rho(z)$ equals $\rho'(z)$ equals w then it must be shown that $\rho(y)$ equals $\rho'(y)$. If $\rho(z)$ equals $\rho'(z)$ then $\rho^{-1}(\rho'(z))$ equals z so $\rho^{-1}\circ\rho'$ is a symmetry of z. But since $\Delta(z)$ is a subset of $\Delta(y)$, $\rho^{-1}\circ\rho'$ is a symmetry of y and thus $\rho^{-1}(\rho'(y))$ equals y which implies that $\rho'(y)$ equals $\rho(y)$.

It will now be shown that for any w which is isomorphic to z and any point permutation ρ, $F(\rho(w))$ equals $\rho(F(w))$. Since w is isomorphic to z there is some point permutation ρ' such that w equals $\rho'(z)$. Now $F(\rho(w))$ equals $F(\rho\circ\rho'(z))$ which equals $\rho\circ\rho'(F(z))$ which equals $\rho(\rho'(F(z))$ which equals $\rho(F(\rho'(z))$ which equals $\rho(F(w))$. Thus for any w isomorphic to z, F satisfies the condition for being an essential function. To complete the definition of F let F(w) be w for any w not isomorphic to z.

3=>1: Suppose F is an essential function such that F(z) equals y and let ρ be any symmetry of z. Since F is an essential function $\rho(F(z))$ equals $F(\rho(z))$ which equals F(z). Thus ρ is a symmetry of F(z), i.e. ρ is a symmetry of y. Thus $\Delta(y)$ contains $\Delta(z)$.

4.2. Abstraction and Points

The notion of abstraction has some important relationships to points. The first lemma about points concerns the isomorphism classes of points in the context of an object x.

Lemma 4.2: For any object x and point p, $|p|_x$ is either a subset of P(x) or is all of P(U)-P(x).

Proof: For any symmetry ρ of x, $\rho(P(x))$ equals $P(\rho(x))$ equals P(x). Thus any symmetry ρ of x induces a permutation of P(x). Thus for any point p in P(x), $|p|_x$ is a subset of P(x). On the other hand for any two points r and s which are not in P(x) there is a symmetry of x which exchanges r and s. Thus if r is not in P(x) then $|r|_x$ contains all of P(U)-P(x). Furthermore for r not in P(x), $|r|_x$ can not intersect P(x) since otherwise there would be some point p in P(x) such that $|p|_x$ was not a subset of P(x). Thus either p is in P(x) and $|p|_x$ is a subset of P(x) or p is not in P(x) and $|p|_x$ equals P(U)-P(x).

Corollary 4.3: For any object x and point p, p is in P(x) just in case $|p|_x$ is small.

Corollary 4.3 immediately implies that for any object x the set P(x) is determined by the symmetry group of x. In fact Corollary 4.3 leads directly to the following theorem:

Theorem 4.4 For any objects y and x, if y is an abstraction of x then P(y) is a subset of P(x).

Proof: Let p be any point in P(y). Since $\Delta(y)$ contains $\Delta(x)$, $|p|_y$ contains $|p|_x$. But by Corollary 4.3 $|p|_y$ is small so $|p|_x$ must also be small and therefore p must be in P(x).

Theorem 4.4 immediately implies that for any for any essential function F and any object x, P(F(x)) is a subset of P(x). It is important to realize that the converse of theorem 4.4 does not hold, i.e. if P(y) is a subset of P(x) then y need not be an abstraction of x. For example {p q} is not an abstraction of {p q r}.

4.3. Representation and Transformational Isomorphisms

Any finite set of points can be represented by a finite list of points though there is no canonical representation for a set of points as a list of points. More precisely there is an essential function F which maps any finite list of points to the finite set of points contained in that list and any finite set y can be written as F(x) for some finite list x. Note that the function F is from the representations to the represented objects. Also note that the function from representations to represented objects is onto, i.e. every object which is to be represented must have a representation. These observations lead to the following definition of a uniform representation.

Definition: Let C and R be subsets of U, let F be an essential function, and let F(R) denote {F(x) for x in R}. F is said to be a uniform representation of elements of C as elements of R just in case F(R) contains C.

Note that lists of points can not be represented as sets of points because there is no essential function which maps a set of points to a list of those points (there is no canonical representation of a set of points as a list). A similar example involves multisets. A list of points can be used to represent a multiset of points, but multisets of points can not be used to represent lists.

There are certain cases in mathematics where two different (non-isomorphic) things are "essentially the same thing". For example an equivalence relation on a set of points C is a relation, i.e. a set of pairs, which is reflexive, symmetric, and transitive. A partition of C is a family of disjoint subsets of C. Any equivalence relation on C can be viewed as a partition of C and vice versa. Another simple example involves the representation of tuples. For example a tuple of points <p q> can be viewed as the set {p {p q}} or as the set {q {p q}}. The following definition makes the notion of "essentially the same" more concrete.

Definition: An essential function F from U to U which is also a permutation of U will be called a *transformational symmetry* of $\langle U \in \rangle$. Two objects x and y will be called *transformationally isomorphic* just in case there is a transformational symmetry of $\langle U \in \rangle$ which maps x to y.

If two objects x and y are transformationally isomorphic then there is a sense in which they are indistinguishable. More precisely the following lemma holds:

Lemma 4.5: For any transformational symmetry F there is a translation operator T which maps any monadic essential predicate Φ to a monadic essential predicate $T(\Phi)$ such that for any object x, $\Phi(x)$ holds just in case $T(\Phi)(F(x))$ holds.

Proof: Since F is a permutation of U it has an inverse F^{-1} which is easily shown to be an essential function. Let $T(\Phi)$ be the predicate $\lambda w.\Phi(F^{-1}(w))$. Clearly $\Phi(x)$ is equivalent to $T(\Phi)(F(x))$. Furthermore $T(\Phi)$ is easily seen to be an essential predicate.

Lemma 4.5 gives a precise relationship between objects which are transformationally isomorphic. In particular if x and y are transformationally isomorphic via the transformational symmetry F then any essential statement (or question) $\Phi(x)$ concerning x is equivalent to some essential statement $T(\Phi)(y)$ concerning y. It turns out that two objects x and y are transformationally isomorphic just in case $\Delta(x)$ equals $\Delta(y)$. However the condition that $\Delta(x)$ equals $\Delta(y)$ does not ensure that there is a *definable* transformational symmetry F which maps x to y.

Definition: A function F from U to U will be called *definable* just in case there is a first order formula Φ of two free variables whose only non-logical symbol is $\in$ such that for any two objects x and y, $\Phi(x\ y)$ holds in $\langle U \in \rangle$ just in case y equals F(x).

Consider the real numbers $\langle R + {}^{\bullet} \leq \rangle$ where R is a set of points, + and $^{\bullet}$ are binary operations on R, and $\leq$ is a total order on R. $\Delta(\langle R + {}^{\bullet} \leq \rangle)$ is the group of all symmetries which leave every point in R fixed (any symmetry of $\langle R + {}^{\bullet} \leq \rangle$ must leave one and zero fixed). Now consider a pair $\langle R \leq' \rangle$ where $\leq'$ is a well ordering of the set of points R. It is easy to show that $\Delta(\langle R \leq' \rangle)$ is also the group of all permutations which leave every point in R fixed. Since $\Delta(\langle R + {}^{\bullet} \leq \rangle)$ equals $\Delta(\langle R \leq' \rangle)$, $\langle R + {}^{\bullet} \leq \rangle$ is transformationally isomorphic to $\langle R \leq' \rangle$. However there is probably no *definable* transformational symmetry of $\langle U \in \rangle$ which maps $\langle R + {}^{\bullet} \leq \rangle$ to $\langle R \leq' \rangle$.

4.4. Context

Intuitively a context is a collection of objects which are taken to be "fixed". There are some objects which are taken to be fixed over all of mathematics. For example mathematicians often speak of "the" natural numbers, even though the identity of the natural numbers can not be specified (though the structure of the numbers can be specified up to isomorphism). The same holds for "the" real numbers, or "the" complex plain. In logic one often assumes that there is a particular thing which is the constant "true" and a particular thing which is the constant "false". A more controversial example is the empty set. There are other examples of "context" where the context is not even specified up to isomorphism. The phrase "fixed but arbitrary" is often used in mathematical writing and serves to specify a context for a mathematical discussion.

As another example of context consider a linear vector space. A linear vector space has an associated field (usually "the" real or complex numbers) such that any vector can be scaled by an element of the field. In discussions of linear vector spaces the field is usually taken to be fixed. Thus in relating two vector spaces one usually assumes they have the same associated field of scalars.

As yet another example consider a particular first order language L. The language L is taken to be a sequence of typed symbols which determines a set of well formed formulas. Such a language is usually taken to be arbitrary but fixed in discussions of logic.

To generalize the results of the previous section it is useful to define the notion of a contextual symmetry group.

Definition: The symmetry group of y in the context of z, denoted $\Delta_z(y)$, is the set of all symmetries of z which are also symmetries of y. More simply $\Delta_z(y)$ equals $\Delta(y)$ intersect $\Delta(z)$.

Note that any symmetry of the pair $\langle y\ z \rangle$ must be a symmetry of y and a symmetry of z, and anything which is a symmetry of both y and z must be a symmetry of the pair $\langle y\ z \rangle$. Thus $\Delta(\langle y\ z \rangle)$ is the intersection of $\Delta(y)$ and $\Delta(z)$ so $\Delta_z(y)$ equals $\Delta(\langle y\ z \rangle)$. The notion of an essential function can also be made contextual:

Definition: A function F from U to U will be called essential in the context of z just in case for any object x any symmetry ρ of z, $F(\rho(x))$ equals $\rho(F(x))$.

A good example of a contextually essential function is the cardinality function on finite sets. Let $\langle N \leq \rangle$ be "the" natural numbers where N is a set of points and $\leq$ is a binary relation which orders those points. The function F which maps any finite set x to the natural number representing the size of x is essential in the context of $\langle N \leq \rangle$. Note that this cardinality function is not essential outside of this context because F(x) can be a point not found in x. The following lemma provides an alternative characterization of functions which are contextually essential.

Lemma 4.7: A function F from U to U is essential in the context of z just in case it can be written as $\lambda x.G(\langle x\ z \rangle)$ for some essential function G.

Proof: If F can be written as $\lambda x.G(\langle x\ z \rangle)$ then it is easy to show that F is essential in the context of z. On the other hand assume F is essential in the context of z. First if w is not a pair whose second component is isomorphic to z then G(w) is defined to be w. If w is a pair whose second component is isomorphic to z then w can be written as $\rho(\langle x\ z \rangle)$ for some object x and point permutation ρ. In this case G(w), which can be written as $G(\rho(\langle x\ z \rangle))$, is defined to be $\rho(F(x))$. It must first be shown that G is well defined, i.e. that if $\rho(\langle x\ z \rangle)$ equals $\rho'(\langle y\ z \rangle)$ then $\rho(F(x))$ equals $\rho'(F(y))$. First note that $\rho^{-1}(\rho'(\langle y\ z \rangle))$ equals $\langle x\ z \rangle$ so $\rho^{-1}(\rho'(y))$ equals x and $\rho^{-1}(\rho'(z))$ equals z. Thus $\rho^{-1} \circ \rho'$ is a symmetry of z. Now since F is essential in the context of z, $\rho^{-1} \circ \rho'(F(y))$ equals $F(\rho^{-1} \circ \rho'(y))$ which equals F(x). But if F(x) equals $\rho^{-1} \circ \rho'(F(y))$ then $\rho(F(x))$ must equal $\rho'(F(y))$.

It follows directly from the definition of G that $G(\langle x\ z\rangle)$ equals F(x) and thus F can be written as $\lambda x.G(\langle x\ z\rangle)$. To show that G commutes with arbitrary point permutations let w be any object and ρ be any point permutation. If w can not be written as $\rho'(\langle x\ z\rangle)$ for some x and ρ' then G(w) equals w and $G(\rho(w))$ equals $\rho(w)$ so the result is trivial. On the other hand suppose w can be written as $\rho'(\langle x\ z\rangle)$. In this case $G(\rho(w))$ equals $G(\rho\circ\rho'(\langle x\ z\rangle))$ which equals $\rho\circ\rho'(F(x))$ which equals $\rho(G(\rho'(\langle x\ z\rangle)))$ which equals $\rho(G(w))$.

The following abstraction theorem is a generalization of the first abstraction theorem.

Theorem 4.8, The Second Abstraction Theorem: For any objects x and y and context z the following are equivalent:

1) $\Delta_z(y)$ contains $\Delta_z(x)$
2) $|y|_{\langle x\ z\rangle}$ is a singleton set
3) y equals F(x) for some function F which is essential in the context of z

Proof: The first condition is equivalent to the statement that $\Delta(\langle y\ z\rangle)$ contains $\Delta(\langle x\ z\rangle)$. The second condition is equivalent to the statement that $|\langle y\ z\rangle|_{\langle x\ z\rangle}$ is a singleton set. Finally lemma 4.7 implies that the third condition is equivalent to the statement that $\langle y\ z\rangle$ equals $G(\langle x\ z\rangle)$ for some essential function G. Thus the equivalence of these three statements follows directly from the first abstraction theorem.

4.5. Essential Predicates

Essential functions have been shown to play an important role in characterizing the nature of abstractions and the notion of a natural or canonical property. Essential predicates are closely related to essential functions and can play much the same role in constructing abstractions.

Definition: A binary predicate Φ on U is called essential if for any objects x and y and point permutation ρ, $\Phi(x\ y)$ holds just in case $\Phi(\rho(x)\ \rho(y))$ holds.

The relationship between predicates and functions can be made more explicit by defining a monadic function F_Φ for each binary predicate Φ.

Definition: For any binary predicate Φ on U, F_Φ is the function from U to subsets of U such that $F_\Phi(x)$ equals $\{y: \Phi(x\ y)\}$.

For example let Φ be the predicate such that $\Phi(x\ y)$ holds just in case y is a pair whose first component is x. In this case $F_\Phi(x)$ is the set of all pairs whose first component is x. Note that $F_\Phi(x)$ is a large set and thus has no representation in $\langle U\ \in\rangle$. Thus in general F_Φ can not be thought of as a function from U to U. The following definitions will be useful in discussing the functions associated with essential predicates.

Definition: Let C be any subset of U. P(C) is the union over x in C of P(x). For any point permutation ρ, $\rho(C)$ is the set $\{\rho(x): x \text{ in } C\}$. The symmetry group of C, denoted $\Delta(C)$, is the set of all point permutations ρ such that $\rho(C)$ equals C. The isomorphism class $|C|_z$ of C in the context of an object z is the family of all sets which can be written as $\rho(C)$ for some point permutation ρ.

For any essential predicate Φ the function F_Φ commutes with point permutations, i.e. $F_\Phi(\rho(x))$ equals $\rho(F_\Phi(x))$. Thus F_Φ can be thought of as an essential function. However as the above example shows $F_\Phi(x)$ can be large and $P(F_\Phi(x))$ can be all of $P(U)$. Thus some of the theorems concerning essential functions do not apply to F_Φ. However many of the results concerning essential functions can be generalized to the functions associated with essential predicates.

Theorem 4.9, The Third Abstraction Theorem: For any object z and (possibly large) subset C of U the following are equivalent:

1) $\Delta(C)$ contains $\Delta(z)$
2) $|C|_z$ is a singleton family
3) C equals $F_\Phi(z)$ for some essential predicate Φ.

The proof of the above theorem is analogous to the proof of the first abstraction theorem. In showing that 1) implies 3) the predicate Φ is defined by setting $\Phi(\rho(z)\,\rho(y))$ to be true for any point permutation ρ and any element y of C, and $\Phi(w\ x)$ to be false if $\langle w\ x\rangle$ can not be written as $\langle \rho(z)\,\rho(y)\rangle$ for some y in C.

Essential predicates can be thought of as defining abstraction functions from objects to more abstract objects. For an essential predicate Φ and object x it does not seem very important that $F_\Phi(x)$ may be large, the important point is that the symmetry group of $F_\Phi(x)$ contains the symmetry group of x.

A good example of the use of essential predicates in defining abstractions is a multiset. Let f and g be two finite functions (they each have a finite domain). The functions f and g will be said to represent the same multiset if there exists a bijection σ from the domain of f to the domain of g such that for any x in the domain of f, f(x) equals $g(\sigma(x))$. Intuitively f and g represent the same multiset if for any range element y, f and g map the same number of objects onto y. Let Φ be the binary predicate on U such that $\Phi(f\,g)$ holds just in case f and g are finite functions which represent the same multiset. It is easy to show that Φ is an equivalence relation on finite functions and that $F_\Phi(f)$ is the equivalence class of f under this relation. The symmetry group of $F_\Phi(f)$ is not the full permutation group on P(U) but is larger than the symmetry group of f. Thus $F_\Phi(f)$ can be thought of as the multiset abstraction of f.

5. RELATION TO OTHER WORK

The notions of isomorphism, symmetry, and representation are ubiquitous in mathematics and probably have numerous independent origins. The relationship between symmetry and permutation groups is also well known. This relationship has been studied in some detail and it has been shown, for example, that not every permutation group can be represented as the symmetry group of a graph [Biggs 74]. But while the notions of isomorphism and symmetry have been extensively used for objects of a given type (e.g. graphs, groups, algebras, languages, grammars) these particular notions of isomorphism do not provide a notion of isomorphism defined over all mathematical objects.

Category theory provides one general approach to the notion of isomorphism. A category can be thought of as a directed multigraph with an associative composition operator ∘ on arcs and for each node n an assigned "identity" arc from n to n. The nodes of a category are often associated with sets and the arcs with functions between these sets. Thus the arcs are called "morphisms". An isomorphism is defined to be an arc ρ which has an "inverse" arc ρ^{-1} such that both $\rho \circ \rho^{-1}$ and $\rho^{-1} \circ \rho$ are identity arcs [Schubert 72]. Category theory provides a general theory of isomorphism to the extent that every mathematical object can be thought of as a node ("object") in a category. For example a group can be thought of as a node in the category of groups, a graph as a node in the category of graphs, etc. However the category containing a given object must be defined separately for each type of object. In fact the category containing an object of a given type is usually defined *in terms of* the notion of isomorphism (and homomorphism) for objects of that type. Therefore category theory does not provide any satisfying general notion of isomorphism for arbitrary mathematical objects.

The notion of a *type* used in universal algebra and computer science provides another approach to a general definition of isomorphism. An algebra is a domain together with some functions defined over that domain. In the universal study of algebras each particular algebra has a *type* (or *signature* or *language*) which is a set of symbols which are interpreted by that algebra. For example the type of a group is the single binary function *symbol* ∘. There is a natural definition of isomorphism for the algebras of a fixed type such that two algebras A and B are isomorphic just in case there is a bijection from the domain of A to the domain of B which maps A's interpretation of any symbol to B's interpretation of that symbol.

The notion of type also plays a critical role in many modern computer languages [Tennant 81]. There is one particular outlook on the types of computer data structures which provides a basis for a notion of isomorphism. Under this view a type is a collection of objects which can be defined in a "natural" way from a collection of base types. For example if A and B are base types then the set of functions from A to B is also a type. Similarly the set of pairs A×B of an element of A and an element of B is a type. As another example let the type SubSets(A×A) be the collection of all sets of ordered pairs of elements of the base type A. More simply SubSets(A×A) is the type containing all directed graphs whose nodes are members of A. Several people studying such data types and have employed permutations of the elements of base types to define a notion of a "natural" function between types [Aho & Ullman 79] [Dunlaing & Yap 82]. In fact Dunlaing and

Yap implicitly use a notion of isomorphism based on permutations of the elements of base types in defining the automorphism group of an arbitrary typed object.

While there are strong similarities between symmetric set theory the above mentioned work on data types (especially that of Dunlaing and Yap) there is also an important difference. Symmetric set theory bases the notion of isomorphism on points rather than types. When the notion of isomorphism is based on points the isomorphism class of an object is an essential property of the object and does not depend on viewing that object as an instance of some type (or as a member of some category). Thus it can be argued that the need for types (or categories) in defining the notion of isomorphism is a byproduct of the fact that ur-elements were left out of set theory.

6. REFERENCES

[Aho & Ullman 79] A.V. Aho, J. D. Ullman
"Universality of Data Retrieval Languages"
Proc. 6th ACM Symposium on Principles of Programming Languages, 1979, pp.110-120

[Benacerraf 65] Paul Benacerraf
What Numbers Could Not Be.
The Philosophical Review, Vol LXXIV, No. 1, January 1965, pp. 47-73

[Biggs 74] N. Biggs
Algebraic Graph Theory
University Press, 1974

[Dunlaing & Yap 82] Colm O Dunlaing, Chee K. Yap.
Generic Transformations of Data Structures
23'rd Annual Symposium on the Foundations of Computer Science
November 3-5, 1982, pp. 186-195

[Fraenkel et. al. 58] A. A. Fraenkel, Y. Bar-Hillel, A. Levy
Foundations of Set Theory
North-Holland, 1958

[Schubert 72] Horst Schubert
Categories
Springer-Verlag, 1972

[Tennant 81] R. D. Tennant
Principles of Programming Languages
Prentice-Hall International, 1981

7. APPENDIX: CONSISTENCY AND CHARACTERIZATION THEOREMS

This section contains some results concerning the existence and nature of universes <U ∈> of symmetric sets. It is shown that the existence of a universe <U ∈> of symmetric sets is equivalent to the existence of a strongly inaccessible cardinal. It is also shown that a universe <U ∈> of symmetric sets is completely characterized by its "height" and "width". These results provide insight into two obvious questions. First, are the axioms for symmetric sets consistent? Second, to what extent are the axioms categorical, i.e. under what conditions are two universes isomorphic?

7.1. Consistency and Strongly Inaccesible Cardinals

There does not seem to be any satisfactory proof that there exists a universe of symmetric sets. However a simple condition can be given which is equivalent to the consistency of the axioms of symmetric set theory. In essence the consistency of the axioms depends purely on the consistency of axioms three through five (infinity, power set, and union). Axioms three through five characterize what is known as a strongly inaccessible cardinal. Thus the axioms of the theory of symmetric sets are consistent just in case there exists a strongly inaccessible cardinal. This result is of interest because strongly inaccessible cardinals have been studied in the context of Zermello-Fraenkel set theory and it is generally believed that it is impossible to prove that strongly inaccessible cardinals do not exist. Thus there is strong evidence that the theory of symmetric sets will never be proven inconsistent.

Definition: A set U will be said to have a *strongly inaccessible cardinality* just in case it meets the following conditions:

1) U is uncountably infinite

2) If C is a subset of U smaller than U then the power set of C is also smaller than U.

3) For any family F of subsets of U if F is smaller than U and every member of F is smaller than U then the union of all members of F is smaller than U.

The main result of this section will be proven in two parts. First it will be shown that any set U which is larger than some inaccessible cardinal can be expanded to a model <U ∈> of axioms one through six (the foundation axiom is initially ignored). It will then be shown that any model <U ∈> of axioms one through six contains a substructure <U' ∈> which also satisfies axiom seven (foundation). These two results will lead directly to the main result that a set U can be expanded to a universe <U ∈> just in case U is larger than some strongly inaccessible cardinal.

For any set C let Sm(C) be the family of all non-empty subsets of C which are smaller than C. The following lemma concerning Sm(C) is a standard result of set theory and will be stated without proof:

Lemma A.1: For any infinite set C, Sm(C) is the same size as C.

The next lemma is a direct predecessor to the main result of this section.

Lemma A.2: Any set U which is larger than some strongly inaccessible cardinal can be expanded to a model $\langle U \in \rangle$ of axioms one through six.

Proof: To ensure that there will be a large number of points a subset P(U) of U is chosen such that both P(U) and U-P(U) are the same size as U (this can always be done for any infinite set U). Since U is larger than some strongly inaccessible cardinal we can choose some subset U' of U with a strongly inaccessible cardinality. Let Sm(U U') denote the family of all non-empty subsets of U which are smaller than U'. Since since Sm(U U') is a subset of Sm(U) lemma A.1 implies that Sm(U U') can be no larger than U. On the other hand Sm(U U') contains all the singleton subsets of U and thus Sm(U U') is as large as U. Thus Sm(U U') has the same cardinality as U and there is a bijection f from U-P(U) to Sm(U U') such that each element x of U-P(U) represents some non-empty subset f(x) of U which is smaller than U' and every such subset has a unique such representation. The relation $\in$ is now defined such that $x \in y$ just in case y is in U-P(U) and and x is in f(y). The resulting structure $\langle U \in \rangle$ clearly satisfies axioms one and two (extensionality and strong comprehension). A subset of U is small in $\langle U \in \rangle$ just in case it is smaller than U'. The definition of a set with strongly inaccessible cardinality now directly implies that $\langle U \in \rangle$ satisfies axioms three through five (infinity, power set, and union). The fact that P(U) is as big as U implies that $\langle U \in \rangle$ satisfies axiom six.

It can also be shown that any model of axioms one through six can be used to generate a model which also satisfies foundation.

Lemma A.3: Any model $\langle U \in \rangle$ of axioms one through six contains a substructure which is a model of axioms one through seven.

Proof: An element x of U will be called a well founded element if there are no infinitely decreasing $\in$ chains containing it. Let U' be the subset of U consisting of the well founded elements of U. The substructure $\langle U' \in \rangle$ clearly satisfies the foundation axiom so it is sufficient to show that it also satisfies axioms one through six. Note that every point is well founded so P(U) is contained in U' and thus by the point comprehension axiom U' is a large subset of U. If x is a well founded element of U then every y such that $y \in x$ is also well founded and thus any well founded element represents the same subset of U whether it is viewed as an element of $\langle U \in \rangle$ or as an element of $\langle U' \in \rangle$. Since no two elements of U represent the same set under $\langle U \in \rangle$ no two elements of U' represent the same set under $\langle U' \in \rangle$ and so $\langle U' \in \rangle$ satisfies extensionality. To show that $\langle U' \in \rangle$ satisfies the strong comprehension axiom let C be any subset of U' which is small with respect to $\langle U \in \rangle$, i.e. there is an x in U which represents C. Since every member of C is well founded x must also be well founded and thus x is in U' and thus C is represented in $\langle U' \in \rangle$. Thus every subset of U' which is small with respect to $\langle U \in \rangle$ is represented in $\langle U' \in \rangle$. On the other hand no set which is large in $\langle U \in \rangle$ can be represented in $\langle U' \in \rangle$. Thus a subset of U' is represented in $\langle U' \in \rangle$ just in case it is small with respect to $\langle U \in \rangle$. The fact that U' is large and that a subset of U' is small in $\langle U' \in \rangle$ just in case it is small in $\langle U \in \rangle$ immediately implies that $\langle U' \in \rangle$ satisfies the axioms of infinity, power set and union. Since U' contains P(U) the number of points in U' is large so $\langle U' \in \rangle$ also satisfies the point comprehension axiom.

Lemmas A.2 and A.3 lead directly to the main result of this section.

Theorem A.4: A set U can be expanded to a model $\langle U \in \rangle$ of the axioms of symmetric set theory just in case U is larger than some strongly inaccessible cardinal.

Proof: If U is larger than some strongly inaccessible cardinal then by lemma A.2 it can be expanded to a model $\langle U \in \rangle$ of axioms one through six such that P(U) is the same size as U. By lemma A.3 there is a substructure $\langle U' \in \rangle$ of $\langle U \in \rangle$ which contains P(U) and which satisfies all of the axioms of symmetric set theory. But since U' has the same cardinality as U it is also possible to directly extend U to a model <U ∈> of all of the axioms.

On the other hand if U can be expanded to a model <U ∈> of axioms two through five (strong comprehension, infinity, power set, and union) then it is easily shown that U must be larger than some strongly inaccessible cardinal.

7.2. The Height and Width of a Universe

A universe <U ∈> of symmetric sets is characterized (up to isomorphism) by two "numbers", its height and its width. The height and width of a universe <U ∈> are defined as follows:

Definition: The *width* of a universe <U ∈> is defined to be the cardinality of its set of points P(U). A subset C of U will be said to be *minimally large* in <U ∈> if no subset of C which is smaller than C is large in <U ∈>. The *height* of a universe <U ∈> is defined to be the cardinality of any minimally large subset of U.

The following lemma can be demonstrated directly from the comprehension axioms.

Lemma A.5: The height of any universe <U ∈> is a strongly inaccessible cardinal.

The constructions used in the consistency theorems of the previous section show that for any strongly inaccessible cardinal there is a universe with that height. Since P(U) is required to be a large set the width of a universe must always be at least as large as its height. The constructions used in the consistency theorems further show that the width of a universe can be any cardinality larger than its height.

A universe can be thought of as a rectangle which is no higher than its width. The points of the universe should be thought of as lying along the bottom edge of this rectangle. The main theorem of this section can be proven directly.

Theorem A.6: Any two universes of symmetric sets with the same height and width are isomorphic.

Proof: Let the universe be $\langle U_1 \in_1 \rangle$ and $\langle U_2 \in_2 \rangle$. Since both universes have the same height a set is small with respect to one universe just in case it is small with respect to the other universe. Since $P(U_1)$ and $P(U_2)$ are the same size there exists a bijection ρ from $P(U_1)$ to $P(U_2)$. The function ρ can be extended to a function σ from all of U_1 into U_2 via the following inductive definition:

$$\sigma(p) = \rho(p) \text{ for any point p in } P(U_1)$$

$$\sigma(x) = \text{the representation for } \{\sigma(y): y \in_1 x\} \text{ for x not a point}$$

The set on the right side of the second equation is guaranteed to have a representation in U_2 because it is no larger than the set represented by x. It is easy to show by induction on x under $\in_1^{+}$ that $\sigma(y) \in_2 \sigma(x)$ just in case $y \in_1 x$. To show that σ is a bijection it is sufficient to construct an inverse function σ^{-1} such that for any x in U_1 $\sigma^{-1}(\sigma(x))$ equals x and for any y in U_2 $\sigma(\sigma^{-1}(y))$ equals y. The inverse function σ^{-1} is defined by extending ρ^{-1} from $P(U_2)$ to all of U via a relation analogous to that above. The two conditions relating σ and σ^{-1} can then be proven by induction on $\in_1{}^+$ and $\in_2{}^+$ respectively.

There a few other results which help to characterize a universe $\langle U \in \rangle$. These results will be stated briefly without proof. First it can be shown that in general the size of U equals the size of P(U) (which is at least as large as the height of U). Second the notion of "rank" used in ZF set theory can also be defined for symmetric sets. The details of this definition are not important but one result concerning a characterization of small sets will be mentioned. For any subset C of U let P(C) be the union over x in C of P(x). It turns out that a subset C of U is small just in case P(C) is small and the rank of C is less than the height of the universe.

END

DATE
FILMED

11 - 83

DTIC