

# The Expressive Power of Equality

Tom Etter  
Boundary Institute  
June 20, 2001

## Introduction

### Fractions

A *fraction*  $m/n$  is an *ordered pair* of whole numbers. What, then, does it mean to say that  $2/3 = 4/6$ ? Obviously it doesn't mean that they are the same ordered pair; 2 is not 4 and 3 is not 6. We must, however, keep track of both  $m$  and  $n$  when we add or multiply fractions. When we say that two fractions are *equal*, it's because we have finished our calculations and are no longer seeing them as ordered pairs but as the *rational numbers* that result from dividing their numerators by their denominators.

But what here is really equal to what? Curiously enough, questions like this rarely give us trouble. We seem able to successfully navigate around the threats to logic in this murky domain on automatic pilot, so-to-speak, and are seldom led into actual error.

In this paper, however, we'll go off automatic pilot, and by resolutely demanding answers to questions like what is really equal to what we'll arrive at a remarkable conclusion, which is that *the concept of equality alone can express all of mathematics!*

We'll leave fractions for now, but we'll come back to them, since they supply the pattern for a crucial step in the journey to this remarkable conclusion.

### Equality and identity

**Equality defined.** An *equality* is a two-place predicate that is reflexive, symmetric and transitive, i.e.

- 1)  $x=x$
- 2) If  $x=y$  then  $y=x$
- 3) If  $x=y$  and  $y=z$  then  $x=z$ .

**Identity defined.** Within a particular domain of discourse, an equality will be called an *identity* if it satisfies the principle of *substitutivity*, which says that substituting equals for equals does not change truth-values, or, to put it more formally:

**The principle of substitutivity:** Let  $S$  and  $S'$  be two sentences in which  $y$  is not a bound variable, and that are the same except for  $S'$  having  $y$  in place of the free variable  $x$  of  $S$ ; then  $x=y \Rightarrow (S \Rightarrow S')$ .

It can be shown<sup>1</sup> that if two equalities both satisfy substitutivity in a formal axiom system they are logically equivalent, so any axiom system has at most one identity.

In our fractions example we are implicitly dealing with two equalities, one for fractions and the other for rational numbers. Which of these is the identity? Remember, there can be only one. More exactly, there can be only one in a given axiom system. What we do in practice is to shift back and forth between what are in effect *two* axiom systems, one for rationals and the other for fractions, each with its own identity. In the former, an arithmetic operator such as addition acts on two whole-number pairs to give another pair, e.g.  $2/3 + 3/4 = 17/12$ . In the latter an arithmetic operator acts on two rationals to give another rational, so “ $2/3 + 3/4 = 17/12$ ” would be interpreted as saying that the rational 2 divided by the rational three plus the rational 3 divided by the rational 4 is the rational 17 divided by the rational 12.

Of course the axiom systems for fractions and rationals are usually seen as embedded in a single more encompassing system that has its own “global” identity. However, our ability to shift from this to “local” identities like fraction equality is an important aspect of mathematical practice. This raises the general question of how the interrelation of “local” identities is related to mathematical structure in the usual sense.

If the identity of a system is given as a *conjunction* of equalities, we’ll call it a *compound identity*, and we’ll speak of its components as *partial identities*. To put the above question in a different way, how might the practice of mathematics be affected by taking such decomposition seriously? What might be gained by thinking of identity as a *compound* rather than as an irreducible singular?

This raises the more limited question of how much of mathematical business can be “offloaded” to partial identities, so-to-speak. In particular, what can compound identity do by itself, without help from other kinds of predication? We’ll now see that it can do a great deal, and is in fact strong enough to express all of (mainstream) mathematics. Our main theorem says that there is a three-component compound identity system having the expressive power of ZF set theory. More exactly:

**Expressiveness theorem.** Consider an axiom system whose only primitive predicates are three equalities, written  $R(x=y)$ ,  $C(x=y)$  and  $V(x=y)$ . It is possible to define a predicate  $x=y$  in terms of these three equalities such that, if we take  $V(x=y)$  to be set-theoretic identity, we can assume the axioms of ZF set theory for  $x=y$  and  $V(x=y)$  without contradicting the nine axioms that characterize these three primitives as equalities.

We have chosen ZF set theory because it is generally regarded as a complete foundation for mainstream mathematics, and no one has yet seriously challenged its consistency.

This is not to say that other set theories wouldn't do as well, nor that mainstream mathematics is the last word. In fact our proof makes very little use of the particulars of ZF; all we really need is its ability to define ordered pairs, together with certain minor features that it shares with many other systems. However, it's best to start with something definite.

This paper will present a short and relatively informal but, I hope, convincing proof of the expressiveness theorem, the idea being to make the truth of what this theorem asserts as accessible and as intuitively clear as possible while also providing insights that go beyond what is stated by the theorem alone.

## Homomorphisms

One way to describe the relationship between fractions and rationals is to use the algebraic concept of homomorphism. We start by treating them as elements of distinct algebras, each with its own addition and multiplication. We then create a many-one mapping of fractions onto rationals, call it  $\text{Val}(f)$ , which preserves plus and times, i.e.  $\text{Val}(f + g) = \text{Val}(f) + \text{Val}(g)$  and  $\text{Val}(fg) = \text{Val}(f)\text{Val}(g)$ .  $\text{Val}$ , so defined, is called a *homomorphism*. So far we haven't mentioned equality, leaving "=" in its traditional role as the symbol for complete or *absolute* identity. However, we can introduce the equality of fractions, as we first encountered it in the example of  $2/3 = 4/6$ , to mean  $\text{Val}(f) = \text{Val}(g)$ , i.e. two fractions are equal if they have the same *values* as ratios. We'll write fraction equality as  $F(f=g)$  so as not to confuse it with absolute identity,  $F(2/3=4/6)$ , for instance, is *true* but  $2/3 = 4/6$  is now *false*.

Let's write  $F(x+y)$  and  $F(xy)$  for fraction sum and product. We now have two parallel languages, one based on the primitive expressions  $x+y$ ,  $xy$  and  $x=y$ , and the other on the corresponding primitive expressions  $F(x+y)$ ,  $F(xy)$  and  $F(x=y)$ . How do sentences in one of these languages relate to the corresponding sentences in the other? The answer is very simple: *they make the same statements*. By substituting the equality  $F(x=y)$  for the identity  $x=y$ , we in effect discard all information about fractions except for their values, and when we say things about fractions that depend only on their values, we are saying things about these values themselves.

This is so obvious that it ordinarily goes without saying; it's built into our "automatic pilot". And yet by taking the trouble to say it we learn something that's not so obvious, which is that treating an equality as an identity can turn a homomorphism between two languages into an *isomorphism*. We also get a hint of something more fundamental, which is that the concepts of homomorphism and isomorphism don't really belong to algebra but to the logical syntax of formal languages.

## Cells and sets

We'll begin our proof of the expressiveness theorem by applying these lessons to Zermelo-Fraenkel set theory<sup>2</sup>, abbreviated ZF.

The first step is to define certain entities called *cells* that are to sets what fractions are to rational numbers.

**Cells defined.** A cell is an ordered triple  $\langle x,y,n \rangle$  such that  $x \neq y$ , and  $n$  is either 1 or 2.

An ordered triple is defined in ZF as an ordered pair whose first member is an ordered pair, where the ordered pair  $\langle a,b \rangle$  is defined as the set  $\{\{a\},\{a,b\}\}$ . In saying that  $n$  is 1 or 2, all we really care about is that  $n$  is one of two definite sets that we decide to label "1" and "2"; these could be  $\{\}$  and  $\{\{\}\}$ , for instance. As mentioned, any of a wide range of axiom systems could take the place of ZF. Whatever that system, however, cells must be defined as objects within it.

The word *cell*, in the language of data tables, refers to the intersection of a row and column. If we think of all ordered pairs in which  $x \neq y$  as the *rows* in a two column *membership table*, then a cell in our present sense literally specifies a cell in this table, since  $x$  and  $y$  specify the row and  $n$  specifies the column. Here, for instance, are three sets:  $P = \{\}$ ,  $Q = \{P\} = \{\{\}\}$ ,  $R = \{P,Q\} = \{\{\},\{\}\}$ , and here is their membership table:

P	Q
P	R
Q	R

And here are the six cells  $c_1 \dots c_6$  of that membership table:

<table style="border-collapse: collapse;"><tr><td style="border: 1px solid black; padding: 2px;">P</td><td>Q</td></tr><tr><td>P</td><td>R</td></tr><tr><td>Q</td><td>R</td></tr></table>	P	Q	P	R	Q	R	<table style="border-collapse: collapse;"><tr><td>P</td><td style="border: 1px solid black; padding: 2px;">Q</td></tr><tr><td>P</td><td>R</td></tr><tr><td>Q</td><td>R</td></tr></table>	P	Q	P	R	Q	R	<table style="border-collapse: collapse;"><tr><td>P</td><td>Q</td></tr><tr><td style="border: 1px solid black; padding: 2px;">P</td><td>R</td></tr><tr><td>Q</td><td>R</td></tr></table>	P	Q	P	R	Q	R	<table style="border-collapse: collapse;"><tr><td>P</td><td>Q</td></tr><tr><td>P</td><td style="border: 1px solid black; padding: 2px;">R</td></tr><tr><td>Q</td><td>R</td></tr></table>	P	Q	P	R	Q	R	<table style="border-collapse: collapse;"><tr><td>P</td><td>Q</td></tr><tr><td>P</td><td>R</td></tr><tr><td style="border: 1px solid black; padding: 2px;">Q</td><td>R</td></tr></table>	P	Q	P	R	Q	R	<table style="border-collapse: collapse;"><tr><td>P</td><td>Q</td></tr><tr><td>P</td><td>R</td></tr><tr><td>Q</td><td style="border: 1px solid black; padding: 2px;">R</td></tr></table>	P	Q	P	R	Q	R
P	Q																																								
P	R																																								
Q	R																																								
P	Q																																								
P	R																																								
Q	R																																								
P	Q																																								
P	R																																								
Q	R																																								
P	Q																																								
P	R																																								
Q	R																																								
P	Q																																								
P	R																																								
Q	R																																								
P	Q																																								
P	R																																								
Q	R																																								
$\langle P,Q,1 \rangle$	$\langle P,Q,2 \rangle$	$\langle P,R,1 \rangle$	$\langle P,R,2 \rangle$	$\langle Q,R,1 \rangle$	$\langle Q,R,2 \rangle$																																				
$c_1$	$c_2$	$c_3$	$c_4$	$c_5$	$c_6$																																				

We'll now proceed to define a homomorphism on our new "fractions". We'll again call it Val. Val( $c$ ) maps cells onto sets in general according to the following rule:

**Cell value defined.** Let  $c = \langle x,y,n \rangle$ . Then  $\text{Val}(c) = x$  if  $n=1$ , otherwise  $\text{Val}(c) = y$ .

The cell values in our simple table are shown in the square boxes above.

**Value equality defined.** Define  $V(c=d)$  for cells to mean  $\text{Val}(c) = \text{Val}(d)$ .

The V-equal cells above are  $V(c_1=c_3)$ ,  $V(c_2=c_5)$ , and  $V(c_4=c_6)$

In what sense is Val a homomorphism? In order to justify that term, there must be a relation of membership among cells, call it “cEd”, that is mapped onto set membership by Val, i.e. cEd if and only if  $\text{Val}(c) \in \text{Val}(d)$ .

**Cell membership defined.** The predicate  $xEy$  is defined for cells as meaning that  $\text{Val}(x) \in \text{Val}(y)$ .

In other words, we simply use our homomorphism to *define what we mean* by cell membership.

Here are the *membership* pairs, according to our new definition, among the cells above:  $c_1 \in c_2$ ,  $c_1 \in c_4$ ,  $c_2 \in c_4$ ,  $c_2 \in c_6$ ,  $c_3 \in c_2$ ,  $c_3 \in c_4$ ,  $c_5 \in c_4$ . Notice that there are seven membership pairs rather than four.

We now ask the same question as before: how do sentences in the predicate pair  $xEy$  and  $V(x=y)$  relate to corresponding sentences in  $x \in y$  and  $x=y$ ? The answer is the same: they are logically equivalent. And for the same reason: By taking the weaker equality predicate  $V(x=y)$  as our identity in cell language, we factor out the extra structure that cells have as “representations” of sets, leaving us with statements about the sets themselves. It follows that the theorems that can be stated about cells in terms of  $xEy$  and  $V(x=y)$  exactly correspond to the theorems (including axioms) that can be stated in terms of  $x \in y$  and  $x=y$ , i.e. the theorems of ZF. In other words, our cell language based on E and V is simply the language of ZF in different notation.

The reader is perhaps asking, so what? Why bother to make a copy of ZF that merely adds irrelevant structure to each set? The reason is, as in the case of fractions, that this “irrelevant” structure gives us handles on the ZF sets to grasp them in useful new ways. That’s what we’ll now proceed to do, and it will take us quickly to our main conclusion.

## Row and column equality

Having defined *value* equality, we’ll now define two more cell equalities called *row* equality and *column* equality. We’ll refer to these three equalities together as the RCV equalities.

**Row equality defined.**  $R(c=c')$  for cells  $c = \langle x, y, n \rangle$  and  $c' = \langle x', y', n' \rangle$  means that  $x=x'$  and  $y=y'$ .

**Column equality defined.**  $C(c=c')$  for cells  $c = \langle x, y, n \rangle$  and  $c' = \langle x', y', n' \rangle$  means that  $n=n'$ .

Recall that in the cell  $\langle x,y,n \rangle$ ,  $x \neq y$  and  $n$  is 1 or 2. Thus if we think of this cell as the intersection of the  $n$ 'th column and the  $\langle x,y \rangle$  row in the membership table, the names row and column equality are literally accurate. Value equality then refers to the value of the entry in a row and column. Since row, column and value taken together define a cell, we see that the conjunction of the RCV equalities is the *identity* for cells, i.e. if  $c$  and  $d$  are cells then  $(R(c=d) \ \& \ C(c=d) \ \& \ V(c=d)) \Rightarrow c=d$ .

**Define First(c)** to mean that cell  $c$  is in the first column, i.e. its  $n$  is 1.

The first column of the membership table contains every set, since every set is a member of some other set. There is one set missing from the second column, however, which is the null set, since it has no members. Thus a cell is in the first column if and only if for every cell  $d$  there is a cell in the same column as  $c$  that has the same value as  $d$ . In symbols:

**Theorem 1.**  $\text{First}(c)$  iff  $\forall d \exists e (V(e=d) \ \& \ C(e=c))$

Notice that this defines  $\text{First}(c)$  in terms of the RCV equalities. This brings us to the key step in our proof, which is to define  $cEd$  in terms of the RCV equalities.

Recall that  $cEd$  means that the set that is the value of  $c$  is a member of the set that is the value of  $d$ . If  $x$  is the value of  $c$  and  $y$  the value of  $d$ , then  $cEd$  if and only if there exist cells  $\langle x,y,1 \rangle$  and  $\langle x,y,2 \rangle$ . What this says is that there exist two cells, call them  $e$  and  $f$ , such that  $e$  and  $f$  are in the same row (their  $x$ 's and  $y$ 's are identical), and  $c$  is in the first column and has the same value as  $e$ , and  $d$  is in the second column and has the same value as  $f$ . In symbols:

**Theorem 2.**  $cEd$  if and only if  $\exists e,f (R(e=f) \ \& \ \text{First}(e) \ \& \ V(c=e) \ \& \ \sim \text{First}(f) \ \& \ V(d=f))$

Combining Theorem 2 with Theorem 1 translates  $cEd$  into the language of  $R$ ,  $C$  and  $V$ .

## The consistency of RCV set theory

We saw above that the homomorphism  $\text{Val}(c)$  produces an isomorphism between the language of sentences about cells constructed from  $cEd$  and  $V(c=d)$  and the language of sentences in ZF constructed from  $x \neq y$  and  $x=y$ . This result has nothing to do with the nature of ZF in particular, but follows only from the fact that  $cEd$  and  $V(c=d)$  are defined by using  $\text{Val}$  to “boost”  $x \neq y$  and  $x=y$  into the domain of its argument. This is exactly the same situation that we encountered with fractions and rationals. There is a further analogy, which is that in each case we used the extra structure of the “upper” language to define the boosted predicates in a new way. Had we begun with this new way, we might have questioned its consistency, but if we believe that the lower language is consistent, then its isomorphism to the upper shows that our new scheme of definitions must be consistent too.

Define RCV set theory to be the upper language in ZF abstracted from its interpretation in ZF. It is then based on the three equalities R, C and V. Its axioms are the equality axioms for R, C and V plus the ZF axioms for the defined predicate cEd. But are these axioms consistent? If ZF is consistent, they must be, since when we interpret the abstract R, C and V as the defined R, C and V we constructed in ZF, the abstract axioms turn into theorems of ZF.

This completes our proof of the expressiveness theorem.