# SINGLE AXIOMS FOR GROUPS

by

Kenneth Kunen

Computer Sciences Technical Report #1076

February 1992

# Single Axioms for Groups

Kenneth Kunen[1]
Computer Sciences Department
University of Wisconsin
Madison, WI 53706, U.S.A.
kunen@cs.wisc.edu
February 10, 1992

## ABSTRACT

We study equations of the form $(\alpha = x)$ which are single axioms for group theory. Earlier examples of such were found by Neumann and McCune. We prove some lower bounds on the complexity of such $\alpha$, showing that McCune's examples are the shortest possible. We also show that no such $\alpha$ can have only two distinct variables. We do produce an $\alpha$ with only three distinct variables, refuting a conjecture of Neumann. Automated reasoning techniques are used both positively (searching for and verifying single axioms) and negatively (proving that various candidate $(\alpha = x)$ hold in some non-group and are hence not single axioms).

**§0. Introduction.** A *group* is a model for the following set of five axioms:

G1. $t(x, i(x)) = e$
G2. $t(i(x), x) = e$
G3. $t(x, e) = x$
G4. $t(e, x) = x$
G5. $t(x, t(y, z)) = t(t(x, y), z)$

Here, $t$ (times) is a 2-place function symbol, $i$ (inverse) is a 1-place function symbol, and $e$ (identity) is a constant. The variables $x, y, z$ are understood to be universally quantified. As is well-known, these axioms are redundant, in that either of the subsets, $\{G1, G3, G5\}$ or $\{G2, G4, G5\}$, suffices to derive all the axioms. It is easy to verify that no 2-element subset of $\{G1, G2, G3, G4, G5\}$ suffices, although there are pairs of (universally quantified) equations in $t, i, e$ which are equivalent to the group axioms; for example, such a pair is given by axiom G1 together with

S1. $t(w, i(t(t(i(t(i(y), t(i(w), x))), z), i(t(y, z))))) = x$ ;

the reason why is explained below.

It is thus natural to ask whether any single equation in $t, i, e$ is equivalent to the group axioms. The answer, however, is "no", as was announced without proof by Tarski [5]; a proof may be found in B. H. Neumann [4]; see also §2. However, if we consider the basic symbols to be just $t, i$, then there are single axioms – an example of such, also due to Neumann [4] is S1 above. This paper studies such axioms further, and gives a fairly precise answer to how "small" such a single axiom can be. We use automated techniques both to generate small

[1] This research was supported by NSF Grant DMS-9100665.

single axioms and to prove, via exhaustive searches, that there are no smaller single axioms. We do not consider further the question of axiom pairs in $t, i, e$, except to remark that we trivially get such a pair if we add any single axiom in $t, i$, such as S1, to the axiom G1.

In general, we shall call a *single group axiom* any equation of the form $(\alpha = \beta)$, where $\alpha$ and $\beta$ are terms in $t, i$ and variables, such that $(\alpha = \beta)$ is valid in all groups, and such that, from $(\alpha = \beta)$, one may derive G5 along with

G1'. $t(x, i(x)) = t(y, i(y))$

G3'. $t(x, t(y, i(y))) = x$

So, in any model for $(\alpha = \beta)$, $t(x, i(x))$ will be a constant, $e$, for which G1,G3,G5 (and hence G2,G4) hold. Equivalently, $(\alpha = \beta)$ is a single axiom for groups iff $(\alpha = \beta)$ is valid in all groups, and, from $(\alpha = \beta)$, one may derive G5 along with

G2'. $t(i(x), x) = t(i(y), y)$

G4'. $t(t(i(y), y), x) = x$

A proof that S1 is a single axiom for groups was given by Neumann [4]. A proof may also easily generated using the automated reasoning program OTTER, developed by McCune [1,2]; see §4. McCune [3] also found some single group axioms shorter than S1 and used OTTER to verify them. We discuss this further below, but first make some preliminary remarks on the form that such an axiom must take.

Neumann [4] said that it was already "well-known" that $(\alpha = \beta)$ cannot be a single group axiom unless one of $\alpha, \beta$ is a variable. To see this, let $G$ be any set containing 0 and at least one other element. On $G$, define $t(x, y) = 0$ and $i(x) = 0$. Then, $G$ is not a group, but satisfies all equations of the form $(\alpha = \beta)$ such that neither $\alpha$ nor $\beta$ is a variable.

So, in the following, we shall, without loss of generality, consider only candidate single axioms of the form $(\alpha = x)$, where $\alpha$ is a term in $t, i, x$ and other variables. We may then focus on $\alpha$.

As a first approximation to its complexity, let us say that $\alpha$ is *of type* $(N, D)$ iff $\alpha$ has $N$ variable occurrences and $D$ distinct variables. Thus, in Neumann's S1 above, the $\alpha$ is of type $(7, 4)$.

Now, suppose $\alpha$ is of type $(N, D)$. It is easy to see that if $(\alpha = x)$ is valid in all groups, then $N$ must be odd. We shall show below (Theorem 3.1) that if $(\alpha = x)$ is a single group axiom, then $N$ must be at least 7. Neumann [4] conjectured that $D$ must be at least 4, but this is false, since, for example,

S2. $t(i(t(y, i(y))), t(t(i(y), z), i(t(i(t(y, x)), z)))) = x$

is a single group axiom with $\alpha$ of type $(7, 3)$. Again, this may be easily verified on OTTER (see §4).

It is true (see Theorem 1.1) that $D$ must be at least 3. Thus, in terms of the *type* measure, our $\alpha$ of type $(7, 3)$ is best possible. However, McCune [3] found a number of single axioms, such as

S3. $t(t(w, t(i(t(i(x), w)), z)), t(i(t(y, z)), y)) = x$

The $\alpha$ here has type $(7, 4)$, but is shorter, having 3 occurrences of $i$, whereas the term in S2 has 5 occurrences of $i$. We do not know if there is a single axiom $(\alpha = x)$ with $\alpha$ of type $(7, 3)$ and with only 3 occurrences of $i$.

We shall show in §2 that if $(\alpha = x)$ is a single group axiom, then $\alpha$ must have an odd number of occurrences of $i$ and at least one $i$ within an $i$ – that is, $\alpha$ has a subterm of form $i(\beta)$, where $i$ occurs in $\beta$. In particular, $i$ must occur at least 3 times in $\alpha$.

It now follows that in terms of length, S3 is the shortest single axiom possible. More precisely, let $wt(\alpha)$ be the number of symbols in $\alpha$, excluding commas and parentheses (this is the default weight function on OTTER). So, the $\alpha$ in S3 has weight 16: 7 variable occurrences, 3 occurrences of $i$, and 6 occurrences of $t$. Now, let $(\alpha = x)$ be any single axiom; say $\alpha$ is of type $(N, D)$. Then $\alpha$ must have exactly $N - 1$ occurrences of $t$. Since $\alpha$ has at least 3 occurrences of $i$ and $N \geq 7$, $wt(\alpha) \geq 7 + (7 - 1) + 3 = 16$.

§5 describes the search method by which S2 was found. Roughly, it is the same principle as the proof that $N \geq 7$. Thus, once we have shown (Theorem 1.1) that $D \geq 3$, the only possibility for $N < 7$ would be of type $(5, 3)$, and we refute these by an exhaustive search, producing a non-group model for each one. We then attempted to refute type $(7, 3)$ by the same techniques; this failed, but led to a list of candidate $(\alpha = x)$ of this type for which we could not find a counter-model. The list was short enough that we could run OTTER on each candidate, resulting in a few, such as S2, from which we could derive the group axioms.

Finally, we remark that single axioms for *Abelian* groups have less complexity than single axioms for groups. McCune [3] discovered such single axioms of the form $(\alpha = x)$, where $\alpha$ is, for example, $t(t(t(y, x), z), i(t(y, z)))$. This $\alpha$ has type $(5, 3)$ and $wt(\alpha) = 10$. It is easily seen that no smaller weight is possible.

**§1. The two-variable model.** We show here, as claimed in the Introduction, that there are no single axioms for groups of type $(N, D)$ with $D < 3$. That is, if $(\alpha = x)$ is valid in all groups, where $\alpha$ is built from $t, i$ and variables $x, y$, then $(\alpha = x)$ is valid in some non-group, $\mathcal{G}$. Actually, we prove a stronger result. First, we show that the same $\mathcal{G}$ works for all such $\alpha$. Second, $\mathcal{G}$ also satisfies all 2-variable equations true in all Boolean groups. Here, a *Boolean* group is an Abelian group satisfying the equation $i(x) = x$ (that is, every element is of order 2). Third, $\alpha$ may involve the identity, $e$ as well.

**1.1 Theorem.** There is a structure $\mathcal{G} = (G; t_G, i_G, e_G)$ for the language of group theory such that

1. $t_G$ is not associative (so $\mathcal{G}$ is not a group).
2. If $(\alpha = \beta)$ is any equation valid in all Boolean groups, where $\alpha, \beta$ are built from $t, i, e, x, y$, then $(\alpha = \beta)$ is valid in $\mathcal{G}$.

We begin with two lemmas. The first shows that any relevant $(\alpha = \beta)$ can be derived from the following five equations:

B1. $t(x, y) = t(y, x)$
B2. $i(x) = x$
B3. $t(x, e) = x$
B4. $t(x, x) = e$
B5. $t(x, t(x, y)) = y$

**1.2 Lemma.** If $(\alpha = \beta)$ is any equation valid in all Boolean groups, where $\alpha, \beta$ are built from $t, i, e, x, y$, then $(\alpha = \beta)$ is derivable from B1,B2,B3,B4,B5.

**Proof.** Let $\gamma$ be $t(\alpha, \beta)$. Then $(\gamma = e)$ is valid in all Boolean groups, and $(\alpha = \beta)$ is derivable from $(\gamma = e)$ using B3 and B5. It is thus sufficient to prove that whenever $(\gamma = e)$ is valid in all Boolean groups and $\gamma$ is built from $t, i, e, x, y$, then $(\gamma = e)$ is derivable from B1,B2,B3,B4,B5. In view of B2, we may assume that $i$ does not occur in $\gamma$. We may now simply proceed by induction on the number of occurrences of $t$ in $\gamma$. ∎

The second lemma gives a general form for all models of B1,B2,B3,B4,B5. If $I$ is any set, we use the Erdös notation $[I]^k$ for the set of all subsets of $I$ with exactly $k$ elements. Let us call a *premodel* on $I$ any family $\mathcal{F} \subseteq [I]^3$ with the property that for each $A \in [I]^2$, there is precisely one $B \in \mathcal{F}$ with $A \subset B$. For example, if $G$ is a Boolean group and $I$ is the set of all elements of $G$ other than the identity, a premodel is given by

$$\mathcal{F} = \{\{x, y, z\} \in [I]^3 : t(x, y) = z\}.$$

Turning this around, given *any* premodel $\mathcal{F}$ on $I$, we may define a structure $\mathcal{G} = \mathcal{G}_{\mathcal{F},I}$ by choosing an element $\epsilon \notin I$, setting $G = I \cup \{\epsilon\}$, defining $i_G$ to be the identity function, setting $e_g = \epsilon$, and defining $t_G$ as follows: Let $t_G(\epsilon, x) = t_G(x, \epsilon) = x$, $t_G(x, x) = \epsilon$, and, for $x, y$ any *distinct* members of $I$, let $t_G(x, y)$ be the (unique) $z \in I$ such that $\{x, y, z\} \in \mathcal{F}$.

**1.3. Lemma.** Let $\mathcal{F}$ on $I$ be any premodel. Let $(\alpha = \beta)$ be any equation valid in all Boolean groups, where $\alpha, \beta$ are built from $t, i, e, x, y$. Then $(\alpha = \beta)$ is valid in $\mathcal{G}_{\mathcal{F},I}$.

**Proof.** One easily verifies B1,B2,B3,B4,B5. Then apply Lemma 1.2. ∎

**Proof of Theorem.** Let $I$ be the set of natural numbers. Let $\mathcal{F}_0$ be the set of 4 triples,

$$\{\{1, 2, 3\}, \{0, 3, 4\}, \{0, 1, 5\}, \{2, 5, 6\}\} \quad .$$

It is easy to construct, by induction, a premodel, $\mathcal{F}$ on $I$ with $\mathcal{F}_0 \subset \mathcal{F}$. For this $\mathcal{G}_{\mathcal{F},I}$, $t$ is not associative, since $t(0, t(1, 2)) = t(0, 3) = 4$ and $t(t(0, 1), 2) = t(5, 2) = 6$. ∎

§2. **More models.** Suppose now that $(\alpha = x)$ is an equation valid in all groups, where $\alpha$ is built from $t, i, x$ plus other variables, and we wish to prove that $(\alpha = x)$ is not a single group axiom. So, we need to produce a non-group in which $(\alpha = x)$ is valid. Of course, if $\alpha$ uses only one variable besides $x$, the model of §1 will work. In this section, we describe some other models which work for some more complex $\alpha$. These will be sufficient to prove that $(\alpha = x)$ cannot be a single group axiom if $\alpha$ has fewer than 7 variable occurrences.

We begin with some restrictions on the occurrences of $i$ in $\alpha$, proved by considering a few special models, and then proceed to describe a general class of models, the *ring models.*

**2.1 Theorem.** If $(\alpha = x)$ is a single group axiom, then $\alpha$ has an odd number of occurrences of $i$.

**Proof.** Consider the model whose domain of discourse is $Z_2 = \{0, 1\}$, in which $t$ is interpreted as addition (mod 2), and $i(x) = x + 1 \pmod 2$. Although $t$ is a group operation, the correct $i(x)$ to make this a group would be $x$, not $x + 1$. Thus, this model is not a group. If $(\alpha = x)$ is valid in all groups and $\alpha$ had $n$ occurrences of $i$, then the value of $\alpha$ in this model is $(n + x) \pmod 2$. So, if $n$ is even, $(\alpha = x)$ is valid in this non-group. ∎

Another way of viewing this model is to consider $\{0,1\}$ to be a Boolean algebra, whence $t$ is XOR and $i$ is NOT. Any other Boolean algebra could have been used as well.

We can use a different model to exclude the possibility that $\alpha$ has exactly 1 occurrence of $i$.

**2.2 Theorem.** If $(\alpha = x)$ is a single group axiom, then $\alpha$ must have at least 3 occurrences of $i$.

**Proof.** Theorem 2.1 refutes 0 or 2 occurrences. If $\alpha$ has 1 occurrence of $i$ and $(\alpha = x)$ is valid in all groups, then either the left-most or the right-most variable in $\alpha$ must be $x$. If $x$ is left-most, then $(\alpha = x)$ is valid in any model for $[i(x) = x \wedge t(x,y) = x]$. Similarly when $x$ is right-most. ∎

In addition, $\alpha$ must have a nested $i$ occurrence – that is,

**2.3 Theorem.** If $(\alpha = x)$ is a single group axiom, then $\alpha$ has a subterm (possibly $\alpha$ itself) of the form $i(\beta)$, where $i$ occurs in $\beta$.

**Proof.** Let $n$ be the number of occurrences of $i$ in $\alpha$. By Theorem 2.2, we may assume that $n \geq 3$. In the ring $Z_n$, interpret $t$ as the usual addition (mod $n$), and let $i(x) = -x + 1$ (mod n). If $(\alpha = x)$ is valid in all groups and $\alpha$ has no nested occurrence of $i$, then in this model, $\alpha = x + n = x$. ∎

An $\alpha$ with 3 occurrences of $i$ is possible, such as McCune's S3 in §0. Such $\alpha$ are restricted by:

**2.4 Theorem.** If $(\alpha = x)$ is a single group axiom and $\alpha$ has exactly 3 occurrences of $i$, then $\alpha$ cannot have a subterm of the form $i(i(\beta))$.

**Proof.** If $\alpha$ has 3 occurrence of $i$, $(\alpha = x)$ is valid in all groups, and $\alpha$ contains an $i(i(\beta))$, then, replacing this by $\beta$, we see that either the left-most or the right-most variable in $\alpha$ must be $x$. We then refute $\alpha$ as in Theorem 2.2. ∎

The models used in these proofs may be generalized by the following class of models. Let $(R, +, \cdot)$ be a ring. On $R$, we may interpret $i$ and $t$ as linear functions. That is, we may set $i(x) = m \cdot x + b$ and $t(x,y) = h \cdot x + k \cdot y + c$, where with $h, k, m, b, c$ are fixed elements of $R$. Of course, one must make sure to choose $R, h, k, m, b, c$ so that the resulting model is not a group. The models used in Theorems 2.1 - 2.4 are clearly of this form; for example in Theorem 2.2, $R$ is any ring with a unit, $b = c = k = 0$, and $m = h = 1$. Also, the proof in Neumann [4] that there is no single axiom in $t, i, e$ was a special case of this, with $m = h = k = 1$ and $R = Z_n$; given $(\alpha = x)$ in $t, i, e$ which is valid in all groups, one can always choose $n, b, c, e$ to provide a non-group model of $(\alpha = x)$; the additional freedom of being able to choose $e$ made this possible.

Aside from the above models, our purposes will be served by a somewhat more restricted class, using $Z_n$ as the ring and taking $b = c = 0$.

**2.5 Definition.** If $n, h, k, m$ are integers with $n \geq 2$ and $0 \leq h, k, m < n$, then $\mathcal{R}(h, k, m, n)$ is the structure whose domain of discourse is $Z_n$, where $i, t$ are interpreted as $i(x) = m \cdot x$ and $t(x,y) = h \cdot x + k \cdot y$.

This is a group only in the trivial case in which it reduces to the usual additive group on $Z_n$.

**2.6 Lemma.** If $\mathcal{R}(h,k,m,n)$ is a group then $m = n-1$ and $h = k = 1$.

**Proof.** Assume it is a group. Then the value of $t(x,i(x))$ is independent of $x$; setting $x = 1,0$, we get $h + k \cdot m = 0$; so $t(x,i(x)) = 0$ for all $x$. Then, by $t(y,t(x,i(x))) = t(t(x,i(x)),y) = y$, we get $h \cdot y = k \cdot y = y$ for all y; setting $y = 1$ yields $h = k = 1$. Then $1 + 1 \cdot m = 0$ implies $m = n-1$. ∎

Actually, the same proof would work if we replaced $Z_n$ by any ring with a unit, 1; we would conclude that $h = k = 1$ and that $m$ was the $-1$ of the ring. Also, the proof only needed that $\mathcal{R}(h,k,m,n)$ satisfied all the 2-variable consequences of the group axioms, so the fact, proved in §1, that these axioms do not imply all the group axioms required a different kind of model.

Now, suppose we wish to prove that $(\alpha = x)$ is not a single group axiom by using an $\mathcal{R}(h,k,m,n)$. We may at first leave $h,k,m$ as undetermined parameters. Then $(\alpha = x)$ yields a set of algebraic equations in $h,k,m$. We may then try to find a solution of these (other than $h = k = 1$; $m = n-1$) in some $Z_n$. If successful, we know we have a counter-model for $(\alpha = x)$.

In solving the equations, we have found it helpful to just assume that $h,k,m$ are invertible whenever this seemed convenient. This will always be true if $n$ is prime and $h,k,m$ are non-zero.

For a specific example, consider

A1. $t(z,t(i(t(y,z)),t(i(t(y,i(t(y,x)))),y))) = x$

This seemed hopeful as a single group axiom, since, as one may easily verify on OTTER, it has groupish consequences, such as $(t(i(x),x) = t(i(y),y))$, $(i(t(i(x),x)) = t(i(x),x))$ and $(t(x,t(i(y),y)) = x)$. Setting $i(x) = mx$ and $t(x,y) = hx + ky$, and expanding, we get

$$(hk^4m^2)x + (h^2km + h^2k^2m + h^2k^3m^2 + k^3)y + (h + hk^2m)z \quad = \quad x \ .$$

This will be valid if the coefficients of $y$ and $z$ are 0 and the coefficient of $x$ is 1. The coefficient of $z$ yields $h + hk^2m = 0$, or $m = -k^{-2}$. Substituting this in the coefficient of $x$ yields $h = 1$. Then, expressing the coefficient of $y$ in terms just of $k$, we get $-k^{-1} - 1 + k^{-1} + k^3 = 0$, or $k^3 = 1$. To solve $k^3 = 1$ in $Z_n$ with $k \neq 1$, we can use any prime $n$ such that $n-1$ is divisible by 3. Specifically, we may choose $n = 7$ and $k = 2$, whence $m = -1/4 = 5$. So, $(\alpha = x)$ is valid in the non-group $\mathcal{R}(1,2,5,7)$.

Of course, in general there is no guarantee that a solution other than $h = k = 1$; $m = n-1$ will be found. Even in the above example, $h$ was forced to be 1. Obviously, if we start with a single group axiom $(\alpha = x)$, then our equations will force $h = k = 1$; $m = n-1$, but this could happen even if $(\alpha = x)$ fails to be a single group axiom. However, the ring models $\mathcal{R}(n,h,k,m)$ will be sufficient to prove the theorems in this paper.

One might automate the entire search for a ring model, although we have not found it necessary to do so. We did write two simple Prolog programs. One program runs through a file of candidate $\alpha$ in the 3 variables, $x,y,z$, and extracts the 3 equations that $h,k,m$ must satisfy. The output file consists of each candidate followed by its corresponding equations

(represented as a Prolog term). It is then an easy matter to look at a few of these equations by hand to see which $h, k, m, n$ solve them. The second program takes a list of quadruples, $(h, k, m, n)$, and runs through the output file of the first program, deleting those (candidate, equations) pairs which are satisfied by a quadruple on the list. For small $n$, it is feasible to run through all possibilities for $h, k, m$; this lets us delete many candidates without looking at their equations at all. We used Prolog because its syntax is compatible with OTTER's, saving us the trouble of writing a parser. Speed was never a problem here.

§3. **Five-variable terms.** If $(\alpha = x)$ is valid in all groups, then it is easily seen that $\alpha$ has an odd number of variable occurrences. In this section, we prove that this number must be at least 7 if $(\alpha = x)$ is a single group axiom.

Roughly, the proof is via an exhaustive search. We generate all $\alpha$ with fewer than 7 variable occurrences such that $(\alpha = x)$ is valid in all groups, and verify that each $(\alpha = x)$ is also valid in one of the non-groups discussed in §§1,2. By Theorem 1.1, we need only consider $\alpha$ with at least 3 distinct variables. Any variable other than $x$ in $\alpha$ must occur an even number of times. Thus, we need only consider $\alpha$ with 5 variable occurrences, in which variables $y, z$ occur twice and $x$ occurs once. However, there are still infinitely many such $\alpha$, since there is no a-priori upper bound to the number of occurrences of $i$ in $\alpha$. So, we shall reduce the infinite search to a finite one by proving a stronger theorem.

**3.1 Theorem.** Suppose $(\alpha = x)$ is valid in all groups, where $\alpha$ has 5 variable occurrences. Then $(\alpha = x)$ is valid in some non-group which also satisfies $(i(i(x)) = x)$.

Now, of course, we need only consider $\alpha$ with no subterms of the form $i(i(\beta))$, and there are only finitely many of these (up to variable renaming). We shall eventually refute these by using the models in §§1,2. In the case of the ring models, $\mathcal{R}(h, k, m, n)$, we shall only use $m = 1$ and $m = n - 1$, so that they will satisfy $(i(i(x)) = x)$. The results of §§1,2 yield:

**3.2 Lemma.** Suppose that $(\alpha = x)$ is valid in all groups, and that all group axioms are derivable from $(\alpha = x)$ plus $(i(i(x)) = x)$. Then:

1. $(\alpha = x)$ is not derivable from the set of all equations $(\beta = \gamma)$ such that $(\beta = \gamma)$ contains only 2 variables and is valid in all groups.
2. The number of occurrences of $i$ in $\alpha$ is odd and at least 3.
3. Neither the left-most nor the right-most variable in $\alpha$ is $x$.

**Proof.** We may use the counter-models described in the proofs of Theorems 1.1, 2,1, and 2.3, all of which satisfy $(i(i(x)) = x)$. ∎

We remark that the equation A1 in §2 is a minimal example of an $(\alpha = x)$ satisfying the hypothesis of Lemma 3.2; one may easily verify on OTTER that it plus $(i(i(x)) = x)$ yields all the group axioms. This $\alpha$ has 7 variable occurrences, 3 distinct variables, and 3 occurrences of $i$. None of these three numbers can be reduced, as we see by Theorem 3.1, Lemma 3.2.1, and Lemma 3.2.2. As we showed in §2, A1 alone is not a single group axiom.

Given the material in §§1,2, it is now a simple matter to do a computer search to prove Theorem 3.1, using just a few minutes of cpu time, since the number of candidate $\alpha$ is not that large. In view of Lemma 3.2, we need only consider $\alpha$ with 1 occurrence of $x$, 2 occurrences of $y$ and of $z$, and no subterms of the form $i(i(\beta))$; there are only 8960 of these such that

$(\alpha = x)$ is valid in all groups (see below). This number is small enough, and the number of counter-models is small enough, that it is quite feasible to run through them all. Our original proof did exactly that. However, when we tried to apply this method to terms with 7 variable occurrences, we had 9461760 candidates, and some optimizations were required. These optimizations, applied to Theorem 3.1, resulted in the proof given below, which even a human can understand.

We begin with a definition regarding the structure of $\alpha$.

**3.3 Definition.** Let $\alpha$ be any term in $t, i$ plus variables. Then:

$\alpha$ is *ii-free* iff $\alpha$ has no subterms of the form $i(i(\delta))$.

$\alpha$ is in *basic form* iff $\alpha$ is *ii*-free and $i$ applies only to variables in $\alpha$ – that is, $\alpha$ has no subterms of the form $i(t(\gamma, \delta))$.

$\alpha$ is in *right associated basic form* iff $\alpha$ is in basic form and $t$ is right associated – that is, $\alpha$ has no subterms of the form $t(t(\beta, \gamma), \delta)$.

Given any $\alpha$, one may convert it to basic form or right associated basic form in a canonical way. Formally,

**3.4 Definition.** If $\alpha$ is any term in $t, i$ and variables, define $BF(\alpha)$ recursively by:

1. $BF(\alpha)$ is $\alpha$ if $\alpha$ is $V$ or $i(V)$ for some variable $V$.
2. If $\alpha$ is $t(\beta, \gamma)$, then $BF(\alpha)$ is $t(BF(\beta), BF(\gamma))$.
3. If $\alpha$ is $i(t(\beta, \gamma))$, then $BF(\alpha)$ is $t(BF(i(\gamma)), BF(i(\beta)))$.
4. If $\alpha$ is $i(i(\beta))$, then $BF(\alpha)$ is $BF(\beta)$.

Clearly, $BF(\alpha)$ is in basic form and is the same as $\alpha$ iff $\alpha$ is already in basic form. Furthermore, the equation $(\alpha = BF(\alpha))$ is valid in all groups.

**3.5 Definition.** If $\alpha$ is in basic form, define $RA(\alpha)$ recursively by:

1. $RA(\alpha)$ is $\alpha$ if $\alpha$ is $V$ or $i(V)$ for some variable $V$.
2. If $\alpha$ is $t(\beta, \gamma)$, let $\beta'$ be $RA(\beta)$. If $\beta'$ is $t(\delta, \zeta)$, then $RA(\alpha)$ is $t(\delta, RA(t(\zeta, \gamma)))$. Otherwise, $RA(\alpha)$ is $t(\beta', RA(\gamma))$.

If $\alpha$ is in basic form, $RA(\alpha)$ is in right associated basic form and is the same as $\alpha$ iff $\alpha$ is already in right associated basic form. Furthermore, the equation $(\alpha = RA(\alpha))$ is valid in all groups.

Finally,

**3.6 Definition.** If $\alpha$ is any term in $t, i$ and variables, define $RABF(\alpha)$ to be $RA(BF(\alpha))$.

Again, for any $\alpha$ $RABF(\alpha)$ is in right associated basic form and is the same as $\alpha$ iff $\alpha$ is already in right associated basic form. Furthermore, the equation $(\alpha = BF(\alpha))$ is valid in all groups.

As an example, if we take $\alpha$ from A1 of §2, then we have:

$$\begin{aligned} \alpha: &\quad t(z, t(i(t(y, z)), t(i(t(y, i(t(y, x)))), y))) \\ BF(\alpha): &\quad t(z, t(t(i(z), i(y)), t(t(t(y, x), i(y)), y))) \\ RABF(\alpha): &\quad t(z, t(i(z), t(i(y), t(y, t(x, t(i(y), y)))))) \end{aligned}$$

A convenient way to generate all candidate $\alpha$ for the proof of Theorem 1 is to work backwards from $RABF(\alpha)$ as follows:

*Phase 1*: Generate all $\gamma$ in $t, i, x, y, z$ with 1 occurrence of $x$ and 2 occurrences each of $y$ and of $z$, such that $\gamma$ is in right associated basic form and $(\gamma = x)$ is valid in all groups.

*Phase 2*: For each $\gamma$ generated in Phase 1, generate all basic form $\beta$ such that $RA(\beta)$ is $\gamma$.

*Phase 3*: For each $\beta$ generated in Phase 2, generate all $ii$-free $\alpha$ such that $BF(\alpha)$ is $\beta$.

*Phase 4*: For each $\alpha$ generated in Phase 3, verify that it is true in some non-group ring model.

It is easy to compute the number of $\alpha$ generated. In Phase 1, there are 8 $\gamma$ of form $\tau_1\tau_2 x\tau_3\tau_4$, and 16 each of forms $x\tau_1\tau_2\tau_3\tau_4$ and $\tau_1\tau_2\tau_3\tau_4 x$, making 40 in all. In general, there are 14 ways to associate a product of 5 factors, so for such $\gamma$, there are 14 corresponding $\beta$ generated in Phase 2. Each $\beta$ has 4 occurrences of $t$, and in Phase 3, each of those occurrences may or may not be preceded by an $i$, making for $2^4 = 16$ corresponding $\alpha$. Thus, we have $40 \cdot 14 \cdot 16 = 8960$ candidates for $\alpha$.

We now describe three optimizations used in these phases, and then return to discuss the phases in more detail.

*Two-variable exclusion*: We have already used this implicitly in Phase 1 to tell us that we need only consider $\gamma$ in which $y$ and $z$ both actually occur. Note, however, that this may exclude further candidates. There are many $\alpha$, such as $t(t(t(y, i(y)), t(x, t(i(z), z))))$, which use 3 variables but such that $(\alpha = x)$ is derivable from the set of all valid 2-variable equations. Such $\alpha$ may be deleted by Lemma 3.2.1.

*$y/z$ symmetry*: Note that if $\alpha^*$ is obtained from $\alpha$ by interchanging $y$ and $z$, then $[(\alpha = x) \wedge (i(i(x)) = x)]$ is equivalent to the group axioms iff $[(\alpha^* = x) \wedge (i(i(x)) = x)]$ is. We may arrange our search to consider only one of them.

*$i(V)/V$ symmetry*: Suppose that $\alpha$ is $ii$-free and $V$ is any variable. Let $flip(\alpha, V)$ be obtained by replacing all occurrences of $V$ in $\alpha$ by $i(V)$ and then replacing all $i(i(V))$ by $V$. For example, $flip(t(x, t(i(z), z)),\ z)$ is $t(x, t(z, i(z)))$. Let $\beta$ be $flip(\alpha, V)$. If $V$ is $y$ or $z$, then $[(\alpha = x) \wedge (i(i(x)) = x)]$ is equivalent to the group axioms iff $[(\beta = x) \wedge (i(i(x)) = x)]$ is. For $V$ being $x$ itself, $[(\alpha = x) \wedge (i(i(x)) = x)]$ is equivalent to the group axioms iff $[(i(\beta) = x) \wedge (i(i(x)) = x)]$ is. Since any subset of $\{x, y, z\}$ can be flipped, this will eventually reduce the number of candidates by a factor of 8.

We now return to our three phases, describing them in detail, and thereby proving Theorem 3.1. We present this as a standard mathematical proof, without regard to automation; the reader will find it straightforward, although a bit tedious, to verify all the steps. Automation will be discussed in §5, where we take up 7-variable terms. The techniques there can also be used to make the verification of Theorem 3.1 less painful.

*Phase 1*: Generate all 40 $\gamma$ as described above. But, at this stage, we can already implement $y/z$ symmetry, $i(y)/y$ symmetry, and $i(z)/z$ symmetry. That is, looking ahead, we shall be considering all $ii$-free $\alpha$ such that $RABF(\alpha)$ is $\gamma$. Note that $RABF(\alpha^*)$ is $\gamma^*$ and $RABF(flip(\alpha, V))$ is $flip(\gamma, V)$. So, at Phase 1, we need only keep $\gamma$ in which the left-most occurrence of $y$ is left of the left-most occurrence of $z$, and for $V$ both $y$ and $z$, the left-most

occurrence of $V$ is as $i(V)$. This reduces the number of such $\gamma$ by a factor of 8, to the following 5:

1. $t(i(y), t(y, t(x, t(i(z), z))))$
2. $t(x, t(i(y), t(y, t(i(z), z))))$
3. $t(x, t(i(y), t(i(z), t(z, y))))$
4. $t(i(y), t(y, t(i(z), t(z, x))))$
5. $t(i(y), t(i(z), t(z, t(y, x))))$

*Phase 2*: For each of the $\gamma$ generated in Phase 1, generate all basic form $\beta$ such that $RA(\beta)$ is $\gamma$. As explained above, each $\gamma$ yields 14 $\beta$. But, we may at this point apply the *two-variable exclusion* to delete all $\beta$ such that $(\beta = x)$ is derivable from all valid 2-variable equations. The reason is that, looking ahead, we shall consider all $\alpha$ such that $BF(\alpha)$ is $\beta$. But for such an $\alpha$, the equation $(\alpha = \beta)$ is derivable from the valid 2-variable equations (as can easily be verified from the definition of $BF$), so the same holds for $(\alpha = x)$. Thus, we can delete $\beta$. By applying this deletion to the $5 \cdot 14 = 90$ $\gamma$ obtained in Phase 1, only 8 remain, namely:

1.1. $t(i(y), t(t(y, t(x, i(z))), z))$
1.2. $t(t(i(y), t(t(y, x), i(z))), z)$
2.1. $t(t(t(x, i(y)), t(y, i(z))), z)$
3.1. $t(t(t(x, i(y)), i(z)), t(z, y))$
3.2. $t(t(t(x, t(i(y), i(z))), z), y)$
4.1. $t(i(y), t(t(y, i(z)), t(z, x)))$
5.1. $t(i(y), t(i(z), t(t(z, y), x)))$
5.2. $t(t(i(y), i(z)), t(z, t(y, x)))$

In verifying that these 8 are the only survivors, it is helpful to realize that we may delete any $\beta$ which has a subterm $\zeta$ such that for some $\eta$ with fewer variables than $\zeta$, $(\zeta = \eta)$ is provable from the 2-variable validities. The reason is that if we form $\beta'$ from $\beta$ by replacing $\zeta$ by $\eta$, then $\beta'$ will only use 2 variables, so, from only 2-variable validities, it follows that $\beta = \beta' = x$. This is illustrated in the first example below, arising from $\gamma$ number 3 from Stage 1; the second example illustrates a somewhat more tricky deletion. On the basis of 2-variable validities,

$$t(t(x,\ t(t(i(y), i(z)), z)\ ), y) = t(t(x, i(y)), y) = x$$
$$t(t(x, t(\ t(i(y), i(z))\ )),\ t(z, y)\ ) = t(t(x, t(\ i(t(z, y))\ )),\ t(z, y)\ ) = x$$

so the left-hand sides of these equations may be deleted.

*Phase 3*: For each of the $\beta$ generated in Phase 1, generate all $ii$-free $\alpha$ such that $BF(\alpha)$ is $\beta$. As explained above, each $\beta$ yields 16 $\alpha$. But, we may at this point apply the $i(x)/x$ *symmetry*, and consider only $\alpha$ which begin with $t$ – that is, of the form $t(\zeta, \eta)$. The reason is that any $ii$-free $\alpha$ which does not begin with $t$ will be of the form $i(flip(\alpha', x))$, where $\alpha'$ begins with $t$; if $[(\alpha = x) \wedge (i(i(x)) = x)]$ were equivalent to the group axioms the same would hold of $[(\alpha' = x) \wedge (i(i(x)) = x)]$. Now, each $\beta$ yields only 8 $\alpha$, so we have $8 \cdot 8 = 64$ candidates to consider. By Lemma 3.2, we may delete from these 64 any $\alpha$ which has $x$ as its left-most or right-most variable, or which has an even number of occurrences of $i$. Only 26 remain.

*Phase 4*:

**Proof of Theorem 3.1.** If some $\alpha$ were a counter-example, then there must be a counter-example among the 26 found at Phase 3. Each of these 26 $\alpha$ is listed below, followed by a ring model, $\mathcal{R}(h,k,m,n)$, in which $(\alpha = x)$ is valid; the reader may easily verify this validity by verifying that the corresponding algebraic equations in $h,k,m$ hold in $Z_n$, as explained in §2. Observe that for each of these, $m$ is either 1 or $n-1$, and $h,k$ are not both 1. Thus, these models are non-groups and satisfy $(i(i(x)) = x)$. ∎

| | |
|---|---|
| 1.1.1. $t(i(y), i(t(i(z), i(t(y, t(x, i(z))))))$ | $\mathcal{R}(2,2,1,5)$ |
| 1.1.2. $t(i(y), i(t(i(z), t(t(z, i(x)), i(y)))))$ | $\mathcal{R}(2,2,1,5)$ |
| 1.1.3. $t(i(y), t(i(t(i(t(x, i(z))), i(y))), z))$ | $\mathcal{R}(2,2,1,5)$ |
| 1.1.4. $t(i(y), t(t(y, i(t(z, i(x)))), z))$ | $\mathcal{R}(2,2,1,5)$ |
| 1.2.1. $t(i(t(i(t(t(y, x), i(z))), y)), z)$ | $\mathcal{R}(2,2,1,5)$ |
| 1.2.2. $t(i(t(t(z, t(i(x), i(y))), y)), z)$ | $\mathcal{R}(2,2,1,5)$ |
| 1.2.3. $t(t(i(y), i(t(z, i(t(y, x))))), z)$ | $\mathcal{R}(2,2,1,5)$ |
| 1.2.4. $t(t(i(y), t(i(t(i(x), i(y))), i(z))), z)$ | $\mathcal{R}(2,2,1,5)$ |
| 2.1.1. $t(i(t(i(t(y, i(z))), i(t(x, i(y))))), z)$ | $\mathcal{R}(2,4,1,5)$ |
| 2.1.2. $t(i(t(t(z, i(y)), t(y, i(x)))), z)$ | $\mathcal{R}(23,16,28,29)$ |
| 2.1.3. $t(t(i(t(y, i(x))), t(y, i(z))), z)$ | $\mathcal{R}(2,1,1,3)$ |
| 3.1.1. $t(i(t(z, i(t(x, i(y))))), t(z, y))$ | $\mathcal{R}(2,1,1,3)$ |
| 3.1.2. $t(i(t(z, t(y, i(x)))), i(t(i(y), i(z))))$ | $\mathcal{R}(4,2,1,5)$ |
| 3.1.3. $t(t(i(t(y, i(x))), i(z)), t(z, y))$ | $\mathcal{R}(16,23,28,29)$ |
| 3.2.1. $t(i(t(i(z), i(t(x, t(i(y), i(z)))))), y)$ | $\mathcal{R}(16,23,28,29)$ |
| 3.2.2. $t(i(t(i(z), t(t(z, y), i(x)))), y)$ | $\mathcal{R}(1,2,1,3)$ |
| 3.2.3. $t(t(i(t(i(t(i(y), i(z))), i(x))), z), y)$ | $\mathcal{R}(2,4,1,5)$ |
| 4.1.1. $t(i(y), i(t(i(t(z, x)), i(t(y, i(z))))))$ | $\mathcal{R}(4,2,1,5)$ |
| 4.1.2. $t(i(y), i(t(t(i(x), i(z)), t(z, i(y)))))$ | $\mathcal{R}(16,23,28,29)$ |
| 4.1.3. $t(i(y), t(t(y, i(z)), i(t(i(x), i(z)))))$ | $\mathcal{R}(1,2,1,3)$ |
| 5.1.1. $t(i(y), i(t(i(t(t(z, y), x)), z)))$ | $\mathcal{R}(23,16,28,29)$ |
| 5.1.2. $t(i(y), i(t(t(i(x), t(i(y), i(z))), z)))$ | $\mathcal{R}(2,1,1,3)$ |
| 5.1.3. $t(i(y), t(i(z), i(t(i(x), i(t(z, y))))))$ | $\mathcal{R}(4,2,1,5)$ |
| 5.2.1. $t(i(t(z, y)), i(t(t(i(x), i(y)), i(z))))$ | $\mathcal{R}(2,4,1,5)$ |
| 5.2.2. $t(t(i(y), i(z)), i(t(i(t(y, x)), i(z))))$ | $\mathcal{R}(1,2,1,3)$ |
| 5.2.3. $t(t(i(y), i(z)), t(z, i(t(i(x), i(y)))))$ | $\mathcal{R}(23,16,28,29)$ |

We remark that our proof could have been made somewhat more efficient, in that at Phase 2, we could have deleted terms 1.1 and 1.2. The reason is that for these two $\beta$, $(\beta = x)$ is valid in $\mathcal{R}(2,2,1,5)$. For any $\alpha$ such that $BF(\alpha)$ is $\beta$, the equations needed to prove $(\alpha = \beta)$ are valid in $\mathcal{R}(h,k,m,n)$ whenever $h = k$ and $m^2 = 1$. Thus, we could already have seen at Phase 2 that for any $\alpha$ arising from these two $\beta$, $(\alpha = x)$ would hold in $\mathcal{R}(2,2,1,5)$.

§4. **Verifying single axioms.** This paper makes a number of claims that either $(\alpha = x)$ or $[(\alpha = x) \wedge (i(i(x)) = x)]$ implies all the group axioms, for various terms $\alpha$. These claims can all be verified on OTTER. We see no point in presenting OTTER's proofs here, since they are usually not very instructive and readers can easily reproduce such proofs themselves if desired. However, we make a few remarks in this section on how we set OTTER's switches.

To verify any specific claim made in this paper, it is easy enough to play around with these settings until OTTER gets a proof. But, if one wishes to go through a long list of candidate $\alpha$, running OTTER on each one, a few remarks on efficiency might be useful.

The most obvious way to verify an axiom would be to simply put it in the `sos` and let it run until enough group axioms appear. As explained in §0, it is enough to get G5, together with either G1′, G3′ or G2′, G4′. Say we do this with the S2 of §0. We tried running this on a DECstation5000, putting S2 in the `sos`, letting the `usable` list contain just $(x = x)$, setting `para_into`, `para_from`, `dynamic_demod`, and `order_eq`, and setting `max_weight` to 50, and `pick_given_ratio` to 3. Then G1′ appeared in about 15 seconds, as clause number 839, but the other axioms did not appear within the first 5 minutes. Of course, the success of the run may depend on how the switches are set, and we didn't try every possible combination. Rather than trying to modify the switches to get success in one run, we simply started a second OTTER run, this time adding in $(t(x, i(x)) = e)$ as a demodulator and in the set of support; this is justified, since the first run proved that $(t(x, i(x))$ is a constant. In this run, we just tried to prove G3, since we found in practice that associativity, G5, is often the hardest to derive, so we simply added $(t(p, e) \neq p)$ into the `sos` list, and ran OTTER until a contradiction was found. In this run, we set `max_weight` to 40 and `reduce_weight_limit` to 6020, since the additional demodulator should reduce the size of clauses needed. This produced a proof in about 82 seconds, at clause number 3139. Finally, the third run, we proved associativity; we added $(t(x, e) = x)$ as a demodulator and in the set of support, added $(t(p, t(q, r)) \neq t(t(p, q), r))$ into the `sos`, and found a contradiction in about 7 seconds at clause number 628.

In summary, we can verify an axiom by three OTTER runs, the first proving that $i$ is a right inverse, the second proving that $e$ is a right identity, and the third proving associativity. For the first run, we now simply put $(t(p, i(p)) \neq t(q, i(q)))$ in the `sos`, so that OTTER will stop when it has found a proof.

Now, if we have a file consisting of many equations in the format of S2, it is a simple matter to write a UNIX [1] shell script which invokes OTTER on each one. Our OTTER input files have a time cutoff – say 1 or 2 minutes – after which OTTER will stop if a proof is not found. Success or failure after this time can be determined in the shell script by passing the output file through `fgrep 'UNIT CONFLICT'`. For each equation, $\phi$, our script does the following: First, try to verify that $i$ is a right inverse; if this succeeds, go on to try to prove that $e$ is a right identity; if this succeeds, go on to try to prove associativity. Then, $\phi$ is echoed, along with either `success` or `failure`.

Of course, failure of $\phi$ does not prove that $\phi$ is not a single group axiom, but this technique is useful in discovering single axioms.

We also can run our candidates through a shell script which checks for left inverse and left identity. Mathematically, the two tests are equivalent, but because of the time cutoff, sometimes one will succeed and the other will fail. Thus, we discover more single axioms by using a pair of shell scripts.

A similar method is used to prove that an equation, such as A1 of §2, generates all the group axioms if $(i(i(x)) = x)$ is added. Now, $(i(i(x)) = x)$ is always in the set of support

[1] UNIX is a trademark of AT&T

and the demodulator list. Under $(i(i(x)) = x)$, the two equations, $(t(x, i(x)) = e)$ and $(t(i(x), x) = e)$, are equivalent. Thus, as soon as we verify one we can add the other, and, in running through a list of candidates, we only need one shell script.

**§5. Seven-variable terms.** After proving Theorem 3.1, we conjectured that the same result held for terms with 7 variables – that is, if the type (see §0) of $\alpha$ is $(7, 3)$ and $(\alpha = x)$ is valid in all groups, then it is valid in some non-group which also satisfies $(i(i(x)) = x)$. We already knew of Neumann's and McCune's single axioms of type $(7, 4)$, and we had, by a different method, found a single axiom of type $(9, 3)$.

We set out to prove this conjecture by applying the proof of Theorem 3.1 to 7-variable terms. The outcome, however, was a counter-example, rather than a proof. In fact, we didn't even need the $(i(i(x)) = x)$. We found single group axioms of type $(7, 3)$, such as equation S2 of §0, and an even longer list of equations, such as A1 of §2, which were not single axioms, but which, when added to $(i(i(x)) = x)$, proved all the group axiom.

Of course, counter-examples may simply be listed, without any comment, and the reader may simply verify them on OTTER. However, we shall describe in this section some further details on the organization of the search. This may be useful if the reader wishes to find more such examples. Also, we were not successful in determining whether there is a single axiom of type $(7, 3)$ with only 3 occurrences of $i$. We suspect that this could be settled by the methods described here, perhaps with more patience or computer time. The methods described here can also be used (as we did ourselves) to verify the more tedious parts in the proof of Theorem 3.1.

First, some general remarks on automation. The syntax of OTTER output files is compatible with Prolog, as well as with the UNIX tools `awk` and `grep`. We found it useful to store and manipulate candidate $\alpha$ in the form of literals, $p(\alpha)$. Thus, the output from an OTTER run which is generating candidates in right associated basic form may have many lines which look like:

```
** KEPT: 221 [para_into,27,8,demod,14,14]  p(t(x,t(y,t(i(y),t(i(x),t(x,t(z,i(z))))))).
```

This may be passed through `fgrep KEPT` and then `awk '{print $5;}'` to just keep the

```
p(t(x,t(y,t(i(y),t(i(x),t(x,t(z,i(z))))))).
```

from these lines. These lines are now in a convenient format to be processed by Prolog programs, such as, for example, the ones described in §2 for deleting candidates true in ring models. Or, if it is desired to just keep the terms in which the left-most $y$ is left of the left-most $z$, we may pass the file through `grep '[^z]*y'`

We may repeat the four phases described in §3, now working with seven-variable terms. It is easy to see that proceeding naively here would generate too many terms. In Phase 1, we generate all $\gamma$ in $t, i, x, y, z$ with 7 variable occurrences in which $x, y, z$ all actually appear, such that $\gamma$ is in right associated basic form and $(\gamma = x)$ is valid in all groups. There are 1120 of these. In Phase 2, we would, for each such $\gamma$, generate all basic form $\beta$ such that $RA(\beta)$ is $\gamma$. Since there are 132 ways to associate a product of 7 factors, we would have $132 \cdot 1120 = 147840$ of these $\beta$. Then, in Phase 3, we would, for each such $\beta$, generate all basic $\alpha$ such that $BF(\alpha)$ is $\beta$. Each $\beta$ has 6 occurrences of $t$, and each of those occurrences may or may not be preceded by an $i$, making for $2^6 = 64$ corresponding $\alpha$. Thus, we have $64 \cdot 147840 = 9461760$ candidates for $\alpha$, and the optimizations described in §3 seem to be

more essential. We now proceed to describe how these optimizations work out and how they are automated.

In Phase 1, we used paramodulation and demodulation to generate all relevant $\gamma$ on OTTER, in the form $p(\gamma)$. We set the switch `prolog_style_variables`, which causes OTTER to regard $x, y, z$ as constants, and upper case letters as variables. The `sos` consists of just `p(x)`. The `usable` list contains 12 equations such as `(V = t(t(i(x),x), V) )`; the `t(i(x),x)` can also be `t(x,i(x))`, and can also occur on the right of `V`, and the `x` can also be `y` or `z`. The `demodulator` list contains just `(t(t(U,V),W) = t(U,t(V,W)))`; this causes all generated equations to be right-associated. We set the maximum weight to 7, and weight terms so that any term containing an $i(i(\beta))$ is weighted high, and for other terms, the weight is just the number of occurrences of $x, y, z$. This makes the search finite, terminating with $p(\gamma)$ being generated whenever $\gamma$ uses $x, y, z$, $\gamma$ has 7 or fewer variable occurrences, $\gamma$ has no subterms of form $i(i(\beta))$, $\gamma$ is in right-associated basic form, and $(\gamma = x)$ is valid in all groups. We then used `awk` and `grep` as described above to build a file with just the 1120 candidates. This number may be reduced by a factor of 8 to 140, by using $y/z$ symmetry, $i(y)/y$ symmetry, and $i(z)/z$ symmetry, although we proceed slightly differently than in the 5 variable case. Call $\gamma$ of *form* $\langle XYZ \rangle$ if it has $X$ occurrences of $x$, $Y$ occurrences of $y$, and $Z$ occurrences of $z$. Of the 1120, 560 are of form $\langle 322 \rangle$, 280 of form $\langle 142 \rangle$, and 280 of form $\langle 124 \rangle$. For the form $\langle 322 \rangle$, we implement $y/z$ symmetry exactly as in the 5 variable case, reducing the number to 280. For forms $\langle 142 \rangle$ and $\langle 124 \rangle$, we implement $y/z$ symmetry by simply deleting all $\gamma$ of form $\langle 124 \rangle$, keeping the original 280 of form $\langle 142 \rangle$. Now, $i(y)/y$ symmetry, and $i(z)/z$ symmetry are implemented as before, reducing what is left by a factor of 4 to 70 of form $\langle 322 \rangle$ and 70 of form $\langle 142 \rangle$.

In Phase 2, we generated all candidate $\beta$ by a similar use of paramodulation, and then deleted all $\beta$ such that $(\beta = x)$ is a consequence of 2-variable facts. This resulted in 2153 of form $\langle 142 \rangle$ and 1994 of form $\langle 322 \rangle$.

Phases 3 and 4 are as in the 5-variable case, except that the ring models described there do not now eliminate all the candidates. After trying more ring models – in particular $\mathcal{R}(h, k, m, n)$ with $m^2 = 1$, $n = 4, 5, 7$, and all possibilities for $h, k$ – we were still left with 1692 of form $\langle 322 \rangle$ and 5943 of form $\langle 142 \rangle$, making 7635 in all. Looking these over by hand, it appeared that in many (not all) cases, the candidates could not be refuted by any ring model. However, the number remaining was small enough that it was now feasible to spend a few minutes on each one, so we went on to:

*Phase 5*: Run each of the 7635 remaining candidates through a shell script as described in §4, to see if it, together with $(i(i(x)) = x)$, generated the group axioms. This resulted in 55 which did. Some examples, besides A1 above, are

A2. $(t(i(t(i(y), i(t(t(x, i(t(y, z))), t(y, i(y)))))), z) = x)$

A3. $(t(t(t(i(y), y), y), i(t(i(t(z, x)), t(z, y)))) = x)$

All 55 were of form $\langle 142 \rangle$, and we do not know if there are any at all of form $\langle 322 \rangle$.

*Phase 6*: Try to see if any of these 55 generated the group axioms by itself, without the $(i(i(x)) = x)$. This was done using the "left" and "right" shell scripts, as described in §4. All 55 failed. *However*, once we drop $(i(i(x)) = x)$, the 8 variants formed using $i(V)/V$ symmetry are no longer equivalent. So, from each of the 55 candidates, we produced all its variants using

a simple Prolog program, and then we ran the same shell scripts on all 440. This produced the following single axioms besides S2 from §0:

S4. $(t(t(i(t(z,i(t(x,y)))),t(z,i(y))),i(t(i(y),y))) = x)$
S5. $(t(i(t(y,i(y))),t(t(i(y),i(z)),i(t(i(t(y,x)),i(z))))) = x)$
S6. $(t(t(i(t(i(z),i(t(x,y)))),t(i(z),i(y))),i(t(i(y),y))) = x)$
S7. $(i(t(i(t(z,i(t(i(x),i(t(y,i(t(i(y),y))))))),t(z,y))) = x)$
S8. $(i(t(t(y,z),i(t(i(t(i(t(i(t(y,i(y))),y)),i(x))),z)))) = x)$
S9. $(i(t(i(t(i(z),i(t(i(x),i(t(y,i(t(i(y),y))))))),t(i(z),y))) = x)$
S10. $(i(t(t(y,i(z)),i(t(i(t(i(t(i(t(y,i(y))),y)),i(x))),i(z))))) = x)$

**§6. Conclusion.** The following three questions are left open.

1. Is there a single group axiom $(\alpha = x)$ of type $(7,3)$ with only 3 occurrences of $i$?
2. Is it decidable whether an equation $(\alpha = x)$ is a single group axiom?
3. Is it true that if $(\alpha = x)$ is valid in all groups and is not a single group axiom, then $(\alpha = x)$ fails to be valid in some *finite* non-group?

We conjecture that the answers to all three are "no". It is likely that (1) could be settled by an exhaustive search, using methods described in this paper. Answers to questions (2) and (3) would involve other concepts.

If the answer to (3) turns out to be "yes", that would imply a "yes" answer to (2) as well, although the algorithm this yields (a parallel search for a proof and a counter-model) would not be feasible to implement.

A "yes" answer to (2) via a very efficient algorithm would make most of the results in this paper obsolete.

## References


[1] McCune, W. W., OTTER 2.0 Users Guide, Technical Report ANL-90/9, Argonne National Laboratory, 1990.

[2] McCune, W. W., What's New in OTTER 2.2, Technical Memo ANL/MCS-TM-153, Mathematics and Computer Science Division, Argonne National Laboratory, 1991.

[3] McCune, W. W., Single Axioms for Groups and Abelian Groups with Various Operations, Preprint MCS-P270-1091, Mathematics and Computer Science Division, Argonne National Laboratory, 1991.

[4] Neumann, B. H., Another Single Law for Groups, *Bull. Australian Math. Soc.*, 23:81-102, 1981.

[5] Tarski, A., Equational Logic and Equational Theories of Algebras, in *Proceedings of the Logic Colloquium, Hannover 1966*, H. A. Schmidt, K. Schütte, and H.-J. Thiele, eds., North-Holland, 1968, pp. 275-288.