Single Axioms for Groups and Abelian Groups with Various Operations*

William W. McCune
Mathematics and Computer Science Division
Argonne National Laboratory
Argonne, Illinois 60439-4844
U.S.A.
e-mail: mccune@mcs.anl.gov

March 30, 1995

Abstract

This paper summarizes the results of an investigation into single axioms for groups, both ordinary and Abelian, with each of following six sets of operations: {product, inverse}, {division}, {double division, identity}, {double division, inverse}, {division, identity}, and {division, inverse}. In all but two of the twelve corresponding theories, we present either the first single axioms known to us or single axioms shorter than those previously known to us. The automated theorem-proving program OTTER was used extensively to construct sets of candidate axioms and to search for and find proofs that given candidate axioms are in fact single axioms.

1 Introduction

A single axiom for an equational theory is an equality from which the entire theory can be derived. For example, each of the equalities

$$(x/((((x/x)/y)/z)/(((x/x)/x)/z))) = y, \tag{1.1}$$
$$(x \cdot (((y^{-1} \cdot (x^{-1} \cdot z))^{-1} \cdot u) \cdot (y \cdot u)^{-1})^{-1}) = z \tag{1.2}$$

is a single axiom for (ordinary) groups. Equation (1.1), in terms of division, $\alpha/\beta = \alpha \cdot \beta^{-1}$, was shown to be a single axiom by G. Higman and B. H. Neumann in [1], and (1.2) was given by Neumann in [13]. Each of (1.1) and (1.2) axiomatizes groups in the sense that each generates a theory definitionally equivalent to standard axiomatizations, for example, the triple

$$(e \cdot x) = x,$$
$$(x^{-1} \cdot x) = e,$$
$$((x \cdot y) \cdot z) = (x \cdot (y \cdot z)),$$

where e is the identity.

*This work was supported by the Applied Mathematical Sciences subprogram of the Office of Energy Research, U.S. Department of Energy, under Contract W-31-109-Eng-38.

The investigation summarized in this paper focused on searching for simple single axioms for groups and for Abelian groups, each in terms of each of the six sets of operations {product, inverse}, {division}, {double division, identity}, {double division, inverse}, {division, identity}, and {division, inverse}. (There is no single axiom in terms of {product, inverse, identity} [17, 13].) New single axioms were found for each of the twelve corresponding theories. In seven of the theories, no single axioms were previously known to us; in three of the theories, the new single axioms are shorter than those previously known to us; and in the remaining two cases, the new single axioms are the same size as the ones previously known.

Operations. Throughout the paper, we use $\alpha \cdot \beta$ for product, α^{-1} for inverse, e for the identity element, α/β for division $\alpha \cdot \beta^{-1}$, and $\alpha \parallel \beta$ for double division $\alpha^{-1} \cdot \beta^{-1}$. Given a single axiom in one set of operations, it may seem trivial to obtain a single axiom in other operations by applying a simple transformation. For example, given $(x/(y/(z/(x/y)))) = z$, which is a single axiom for Abelian groups, and making the obvious transformation, say $\alpha/\beta \rightarrow f(\alpha, g(\beta))$, one obtains a single axiom in the sense that it is definitionally equivalent to all other axiomatizations; however, f is not product, and g is not inverse.

Mirror Images. The mirror image of an equality with respect to a binary operator is obtained by reversing the arguments of all occurrences of the operator. The mirror image of a single axiom in terms of product and inverse or in terms of double division is also a single axiom, and the mirror image of a single axiom in terms of (right) division is a single axiom in terms of left division $\alpha^{-1} \cdot \beta$.

Axiom Type. We considered length, number of variable occurrences, and number of distinct variables as measures when searching for simple single axioms. It is known that in a single axiom, say $\alpha = \beta$, for any variety of groups, either α or β must be a variable [13]. Assuming β is the variable, we say that a single axiom $\alpha = \beta$ has type $\langle L, N, D \rangle$, if L is the number of variable and operator occurrences in α, N is the number of variable occurrences in α, and D is the number of distinct variables in α. (Kunen [6] classifies axioms by just $\langle N, D \rangle$.

The OTTER [8] automated theorem-proving program was used extensively in two distinct ways (Section 4) during the investigation: (1) as a symbolic calculator, to construct sets of candidate axioms, and (2) to search for proofs that given candidates are single axioms. Theorem-proving programs have been used in the past to verify known single axioms for groups [3] and to search for and find new single axioms for nonequality theories of groups [10, 12]. Kunen's goal, in his recent study of single axioms for groups [6], was to find precisely how small a single axiom for (ordinary) groups, in terms of product and inverse, can be. By giving non-group models of all candidates, he showed that no single axiom of type $\langle x, 5, 3 \rangle$ exists. When trying to show that there are no single axioms of type $\langle 18, 7, 3 \rangle$, he found (with help from OTTER) several of that type (e.g., (2.1) below).

2 Previously Known Single Axioms

As far as we know, the following are the simplest previously known single axioms for groups and Abelian groups. The type and reference are given for each.

Ordinary Groups:

$$(x/((((x/x)/y)/z)/(((x/x)/x)/z))) = y \qquad \langle 17, 9, 3 \rangle \quad [1] \qquad (1.1)$$

$$(((z \cdot (x \cdot y)^{-1})^{-1} \cdot (z \cdot y^{-1})) \cdot (y^{-1} \cdot y)^{-1}) = x \qquad \langle 18, 7, 3 \rangle \quad [6] \qquad (2.1)$$

$$(((x \parallel (y \parallel e)) \parallel ((z \parallel (u \parallel (u \parallel e))) \parallel (x \parallel e))) \parallel y) = z \quad \langle 19,7,4 \rangle \quad [14] \tag{2.2}$$

Abelian Groups:

$$(x/(y/(z/(x/y)))) = z \qquad \langle 9,5,3 \rangle \quad [16] \quad (2.3)$$
$$((((x \cdot y)^{-1} \cdot (y \cdot x))^{-1} \cdot ((z \cdot u)^{-1} \cdot (z \cdot ((v \cdot w^{-1}) \cdot u^{-1})^{-1})))^{-1} \cdot w) = v \quad \langle 28,11,5 \rangle [13] \quad (2.4)$$

The preceding equalities, except (2.4), can be shown to be single axioms by the methods presented in Section 4.1. Kunen verified (2.4) by using OTTER with a nonstandard strategy [5].

Neumann claims in [14] that

$$((x \parallel ((y \parallel z) \parallel (y \parallel (u^{-1} \parallel z^{-1}))^{-1})) \parallel x)^{-1} = u \tag{2.5}$$

is a single axiom for ordinary groups, but a two-element model of (2.5), $a \parallel a = a$, $b \parallel b = a$, $a \parallel b = b$, $b \parallel a = b$, $a^{-1} = b$, $b^{-1} = a$, shows that it is not, because there is no element e for which $e^{-1} = e$. The counterexample was found by J. Slaney's program FINDER [15].

Prior to the investigation, we did not know of any single axioms for the remaining theories. Tarski states in [17, p. 278] that single axioms exist for {division, identity} and {division, inverse}, but none is given there. Neumann states [14, p. 300] that it should be "quite feasible" to find single axioms for ordinary groups in terms of {division, identity} and in terms of {division, inverse}, and for Abelian groups in terms of {double division, identity}.

Neumann also conjectured [13] that the simplest single axiom for ordinary groups in terms of product and inverse has type $\langle 18,7,4 \rangle$. However, Kunen's axiom (2.1) has type $\langle 18,7,3 \rangle$, and we present one of type $\langle 16,7,4 \rangle$ in the following section.

3 New Single Axioms

Tables 1 and 2 contain representatives of the single axioms that were found by the methods summarized in Section 4. Proofs for axioms (3.1) and (3.7) are given in Section 5. Proofs for the other single axioms listed in this section can be found in [9].

Table 1: New Single Axioms for Ordinary Groups

Operators	Axiom	Type	Ref.
$\cdot$ and $^{-1}$	$(x \cdot (y \cdot (((z \cdot z^{-1}) \cdot (u \cdot y)^{-1}) \cdot x))^{-1}) = u$	$\langle 16,7,4 \rangle$	(3.1)
$/$	$(x/((((y/y)/y)/z)/(((y/y)/x)/z))) = y$	$\langle 17,9,3 \rangle$	(3.2)
$/$ and e	$((e/(x/(y/(((x/x)/x)/z))))/z) = y$	$\langle 15,7,3 \rangle$	(3.3)
$/$ and $^{-1}$	$((x/x)/(y/((z/(u/y))/u^{-1}))) = z$	$\langle 14,7,4 \rangle$	(3.4)
$\parallel$ and e	$((x \parallel (((x \parallel y) \parallel z) \parallel (y \parallel e))) \parallel (e \parallel e)) = z$	$\langle 15,5,3 \rangle$	(3.5)
$\parallel$ and $^{-1}$	$(x^{-1} \parallel ((x \parallel (y \parallel z))^{-1} \parallel (u \parallel (y \parallel u)))^{-1}) = z$	$\langle 16,7,4 \rangle$	(3.6)

Table 2: New Single Axioms for Abelian Groups

Operators	Axiom	Type	Ref.
$\cdot$ and $^{-1}$	$(((x \cdot y) \cdot z) \cdot (x \cdot z)^{-1}) = y$	$\langle 10,5,3 \rangle$	(3.7)
/	$(x/((x/y)/(z/y))) = z$	$\langle 9,5,3 \rangle$	(3.8)
/ and e	$((e/(((x/y)/z)/x))/z) = y$	$\langle 11,5,3 \rangle$	(3.9)
/ and $^{-1}$	$((x/(y/(x/z))^{-1})/z) = y$	$\langle 10,5,3 \rangle$	(3.10)
$\parallel$ and e	$((x \parallel ((z \parallel (x \parallel y)) \parallel (e \parallel y))) \parallel (e \parallel e)) = z$	$\langle 15,5,3 \rangle$	(3.11)
$\parallel$ and $^{-1}$	$(x \parallel (((x \parallel y) \parallel z^{-1})^{-1} \parallel y)^{-1}) = z$	$\langle 12,5,3 \rangle$	(3.12)

The axioms in division alone, (3.2) and (3.8), are the same type as those previously known. The remaining axioms in Tables 1 and 2 are either the first known to us or simpler than those previously known to us.

4 Methodology

OTTER [8] is a computer program that searches for proofs of conjectures stated in first-order logic with equality. The user specifies inference rules, search strategies, and the way that derived formulas are to be processed. Inference rules are of two types: resolution rules, which are based on a generalization of modus ponens, and paramodulation rules, which generalize equality substitution. Search strategies include restricting application of the inference rules and methods for selecting the next formula on which to focus. Processing of derived formulas includes methods for discarding them and methods for turning derived equalities into simplification rules to be applied to subsequently and/or previously derived formulas.

4.1 Trying to Prove That a Candidate Is a Single Axiom

OTTER can be directed to perform a search based on the Knuth-Bendix completion procedure for equational theories [4]. (Briefly, the Knuth-Bendix procedure attempts to convert a set of equalities into a terminating and confluent set of rewrite rules which is a decision procedure for the word problem for the theory. The procedure derives new equalities by a restricted form of paramodulation, using a user-supplied ordering on terms to orient new equalities into rewrite rules, and keeps everything fully simplified with respect to the set of rewrite rules. Success occurs if every derived equality can be oriented and the procedure terminates.) We used two well-known extensions to the procedure [7, 2]: (1) turning it into a proof (refutation) search by including denials of known axiomatizations in the input, and (2) allowing nonorientable equalities to enter the search. The extended procedure is useful even in cases when it does not terminate.

We typically started searches with a candidate and with denials of all single axioms known to us. In addition, we input denials of other properties such as associativity of product and the existence of an identity. OTTER was directed to output all proofs that it found within a specified time. Although the precise settings of the OTTER parameters varied for the different theories we explored, we remark on the general OTTER 2.2 [8, 11] strategies we used.

(1) We set the `kunth_bendix` flag which automatically sets several paramodulation, demodulation, and ordering parameters.

(2) We used the lexicographic recursive path ordering; the ordering on operators was typically ($^{-1} \succ \cdot$), ($/ \succ e$), ($/ \succ {}^{-1}$), ($\| \succ e$), and ($^{-1} \succ \|$), with $\cdot$ and $\|$ having left-to-right status.

(3) We set an initial maximum of 50 or 60 on the weight (symbol count) of inferred clauses, then reduced the limit to to 25 after 25 given clauses.

(4) When more than one property was required to show that a candidate is a single axiom, we input the denials as unit clauses rather than as a multiliteral clause and marked success with multiple proofs rather than with a single proof (the reasons are fairly technical). It is sound to do so in this case, because paramodulation and demodulation alone will not cause the unit denials to interact with one another.

4.2 Constructing and Testing Sets of Candidates

Aside from automated theorem proving, OTTER can also serve as a symbolic calculator, for which the user "programs" his or her task with formulas and equalities that have a procedural rather than a declarative interpretation. Examples of four types of task are (1) given a set of equalities, decide which are true in all groups, (2) given a string of symbols, generate all binary associations of the symbols, (3) given a set of equalities, insert (in a well-formed way) specified terms into each, and (4) given a set of equalities, apply paramodulation with specified equalities in a very constrained way. OTTER was used in this "programmed" mode to construct sets of prospective single axioms.

The practical limit on the size of candidate sets was about 10,000 members, and most candidate sets we used had fewer than 5,000 members. (That way we could run a set overnight or over a long weekend and allow 20–30 seconds for each candidate.) Given a set of candidates, we ran a simple program that initiates a separate OTTER search with each candidate. The search strategy and the list of denials (of known single axioms and other key properties) were fixed for the sequence of runs. The time limit for each search varied from 10 to 60 seconds, depending on the size of the set. Any proofs that were found were collected in a file.

Groups in terms of product and inverse. Neumann's axiom (1.2) has type $\langle 18, 7, 4\rangle$. We built the set of identities of type $\langle x, 7, 4\rangle$, for $x = 14, 15, 16, 17$ (corresponding to $1, 2, 3, 4$ occurrences of inverse). (At that time we were not aware of Neumann's theorem that all single axioms have an odd number of occurrences of inverse [13], which eliminates lengths 15 and 17.) The set has 120,736 members. Looking to Neumann's single axioms [13] for guidance, we decided to consider candidates without inverse at the outermost level and with inverse applied to product in at least two places. No single axioms were found for length 17, but many were found for length 16. We later found others of the same type with inverse at the outermost level. A total of 107 single axioms of type $\langle 16, 7, 4\rangle$, excluding mirror images, were found. We list here five representatives:

$$
\begin{aligned}
&(x \cdot (y \cdot (((z \cdot z^{-1}) \cdot (u \cdot y)^{-1}) \cdot x))^{-1}) = u, \\
&((((x \cdot y) \cdot z)^{-1} \cdot x) \cdot y) \cdot (u \cdot u^{-1}))^{-1} = z, \\
&(x \cdot (y \cdot (z \cdot ((z^{-1} \cdot (u \cdot y)^{-1}) \cdot x)))^{-1}) = u, \\
&(x \cdot (y \cdot ((y^{-1} \cdot z) \cdot (u \cdot (x \cdot z))^{-1})))^{-1} = u, \\
&(x \cdot (y \cdot ((z \cdot z^{-1}) \cdot (u \cdot (x \cdot y))^{-1})))^{-1} = u.
\end{aligned}
\tag{3.1}
$$

We then tried, without success, to find axioms of type $\langle 16,7,3\rangle$, by taking instances of the 107 axioms. All other attempts at finding simpler axioms failed. Kunen [6] later showed that the only possibility for a simpler axiom is $\langle 16,7,3\rangle$.

Abelian groups in terms of product and inverse. Neumann's axiom (2.4) has type $\langle 28,11,5\rangle$. The first approach was to take axioms of type $\langle 16,7,4\rangle$ for ordinary groups and commute products in all possible ways. This led to many single axioms of type $\langle 16,7,4\rangle$. (Of the $2^6 = 64$ commuted variants of just the first of the 107 axioms, 28 were found to be single axioms for Abelian groups.) To search for simpler axioms, we extracted the identities of type $\langle x,5,3\rangle$, for $x = 10,11,12,13,14$, from the 120,736-member set mentioned in the preceding paragraph, and obtained all commuted variants of those. This approach led to three single axioms, excluding mirror images, of type $\langle 10,5,3\rangle$:

$$\begin{aligned}&(((x\cdot y)\cdot z)\cdot(x\cdot z)^{-1}) = y,\\ &(x\cdot((y\cdot z)\cdot(x\cdot z)^{-1})) = y,\\ &(x\cdot(((x\cdot y)^{-1}\cdot z)\cdot y)) = z.\end{aligned}\tag{3.7}$$

Note that simpler single axioms are impossible, because three variables [5, 6] and at least one occurrence of inverse are required.

Groups in terms of division. Higman and Neumann's axiom (1.1) has type $\langle 17,9,3\rangle$. We first considered identities of types $\langle 9,5,3\rangle$, $\langle 13,7,4\rangle$, and $\langle 17,9,5\rangle$ and found 29 single axioms of type $\langle 17,9,5\rangle$. We then examined three-variable instances of the 29 axioms, and found the following two new axioms of type $\langle 17,9,3\rangle$:

$$\begin{aligned}&(x/((((y/y)/y)/z)/(((y/y)/x)/z))) = y,\\ &(((x/x)/(x/(y/(((x/x)/x)/z))))/z) = y.\end{aligned}\tag{3.2}$$

Abelian groups in terms of division. Two single axioms of type $\langle 9,5,3\rangle$, were previously known to us: Tarski's (2.3), and Higman and Neumann's $(x/((y/z)/(y/x))) = z$ [1]. No simpler axiom is possible, because three variables are required. We examined identities of the same type and found the following four additional single axioms:

$$\begin{aligned}&(x/((x/y)/(z/y))) = z,\\ &((x/(y/z))/(x/y)) = z,\\ &((x/((x/y)/z))/y) = z,\\ &((x/y)/((x/z)/y)) = z.\end{aligned}\tag{3.8}$$

Groups in terms of division and identity. No single axioms were previously known to us. We first considered, without success, identities of type $\langle 15,5,3\rangle$ (three occurrences of identity). We then took the single axioms in division alone (type $\langle 17,9,3\rangle$); each has two occurrences of α/α, for variable α. Considering the six candidates of type $\langle 15,7,3\rangle$ obtained from those by replacing one occurrence of α/α, with the identity, we found the following four single axioms:

$$\begin{aligned}&((e/(x/(y/(((x/x)/x)/z))))/z) = y,\\ &(((x/x)/(x/(y/((e/x)/z))))/z) = y,\\ &(x/(((e/y)/z)/(((x/x)/x)/z))) = y,\\ &(x/((((x/x)/y)/z)/((e/x)/z))) = y.\end{aligned}\tag{3.3}$$

We note that by replacing (x/x) with e in (3.3), a single axiom for groups is obtained, with (e/e) as the identity (shown by OTTER), but e is *not* the identity (shown by FINDER).

Abelian groups in terms of division and identity. No single axioms were previously known to us. We started with the four single axioms for ordinary groups in terms of division and identity, and applied limited paramodulation with the Abelian identities $x/(x/y) = y$ and $(x/y)/z = (x/z)/y$ to obtain a set of 48 candidates of various types. Several single axioms were found, the simplest being the following three of type $\langle 11, 5, 3 \rangle$:

$$\begin{aligned} &((e/(((x/y)/z)/x))/z) = y, \\ &((e/(x/y))/((y/z)/x)) = z, \\ &((e/x)/(((y/x)/z)/y)) = z. \end{aligned} \tag{3.9}$$

Groups in terms of division and inverse. No single axioms were previously known to us. We took the 29+3 single axioms in division alone, and applied paramodulation from the definition of inverse, $(y/y)/x = x^{-1}$, one time at each possible position, obtaining 200 candidates of various type. The simplest single axioms discovered were fifteen of type $\langle 14, 7, 4 \rangle$. We list five representatives here:

$$\begin{aligned} &((x/x)/(y/((z/(u/y))/u^{-1}))) = z, \\ &((x/(y/(z/u)))^{-1}/((u/z)/x)) = y, \\ &(((x/y)^{-1}/((z/u)/x))/(u/z)) = y, \\ &((((x/y)/z)/(u/z))^{-1}/(y/x)) = u, \\ &((((x/x)/y)/(z/(y/u)))^{-1}/u) = z. \end{aligned} \tag{3.4}$$

Abelian groups in terms of division and inverse. No single axioms were previously known to us. We first took the 15 single axioms from the preceding paragraph and applied paramodulation with the Abelian identity $x/(x/y) = y$, obtaining 106 candidates. In that set, fourteen single axioms were found, all of type $\langle 14, 7, 4 \rangle$. We then turned to an exhaustive search of the $\langle 10, 5, 3 \rangle$ candidates. The following three single axioms of that type were found.

$$\begin{aligned} &((x/(y/(x/z))^{-1})/z) = y, \\ &(x/((y/z)/(x/z))^{-1}) = y, \\ &(((x/y^{-1})/z)/(x/z)) = y. \end{aligned} \tag{3.10}$$

Groups in terms of double division and identity. The only single axiom known to us was Neumann's (2.2) of type $\langle 19, 7, 4 \rangle$. We tried all candidates of type $\langle 15, 5, 3 \rangle$ (three occurrences of identity) and discovered 208 single axioms. These axioms are noteworthy because they are the simplest, in terms of variable occurrences and distinct variables, of all known single axioms for ordinary groups. We list here five representatives:

$$\begin{aligned} &((x \parallel (((x \parallel y) \parallel z) \parallel (y \parallel e))) \parallel (e \parallel e)) = z, \\ &(x \parallel (((e \parallel ((x \parallel e) \parallel (y \parallel z))) \parallel y) \parallel e)) = z, \\ &((e \parallel x) \parallel (e \parallel (((x \parallel y) \parallel e) \parallel (z \parallel y)))) = z, \\ &((e \parallel x) \parallel (((y \parallel z) \parallel (e \parallel e)) \parallel (x \parallel z))) = y, \\ &((e \parallel (x \parallel (y \parallel e))) \parallel ((y \parallel (z \parallel x)) \parallel e)) = z. \end{aligned} \tag{3.5}$$

Abelian groups in terms of double division and identity. No single axioms were previously known to us. We took the single axiom (3.5) for ordinary groups, applied commutativity of $\parallel$ in all combinations, and deleted mirror images, obtaining 32 candidates. Eleven of those, also of type $\langle 15, 5, 3 \rangle$, were found to be single axioms. We list here five representatives:

$$
\begin{array}{l}
((x \parallel ((y \parallel (x \parallel z)) \parallel (e \parallel z))) \parallel (e \parallel e)) = y, \\
((x \parallel ((y \parallel (x \parallel z)) \parallel (z \parallel e))) \parallel (e \parallel e)) = y, \\
((x \parallel ((y \parallel (z \parallel x)) \parallel (z \parallel e))) \parallel (e \parallel e)) = y, \\
((x \parallel (((y \parallel x) \parallel z) \parallel (y \parallel e))) \parallel (e \parallel e)) = z, \\
((x \parallel ((e \parallel y) \parallel (z \parallel (y \parallel x)))) \parallel (e \parallel e)) = z.
\end{array} \tag{3.11}
$$

This case, double division and identity, is noteworthy because it is the only case in which the currently known single axioms for Abelian groups are not simpler than the single axioms for ordinary groups.

Groups in terms of double division and inverse. No single axioms were previously known to us. We first considered, without success, all identities of type $\langle x, 5, 3\rangle$, for $x = 12, 13, 14$ (corresponding to three, four, and five occurrences of inverse). We then considered identities of type $\langle 16, 7, 4\rangle$, without occurrences of $(\alpha \parallel \alpha^{-1})$ or $(\alpha^{-1} \parallel \alpha)$, for variable α, and discovered two single axioms:

$$
\begin{array}{l}
(x^{-1} \parallel ((x \parallel (y \parallel z))^{-1} \parallel (u \parallel (y \parallel u)))^{-1}) = z, \\
((x \parallel (y \parallel z)^{-1}) \parallel (y^{-1} \parallel (u \parallel (x \parallel u))^{-1})) = z.
\end{array} \tag{3.6}
$$

Abelian groups in terms of double division and inverse. No single axioms were previously known to us. We first took the first single axiom for ordinary groups and applied commutativity of $\parallel$ in all combinations. Six of the resulting 32 candidates (type $\langle 16, 7, 4\rangle$), were found to be single axioms. We then considered all identities of types $\langle 10, 5, 3\rangle$ and $\langle 12, 5, 3\rangle$ (one and three occurrences of inverse) and found the following eight single axioms of type $\langle 12, 5, 3\rangle$:

$$
\begin{array}{l}
(x \parallel (((x \parallel y) \parallel z^{-1})^{-1} \parallel y)^{-1}) = z, \\
(((x \parallel y) \parallel (x \parallel z^{-1})^{-1})^{-1} \parallel y) = z, \\
((x \parallel y) \parallel (x \parallel (z \parallel y)^{-1})^{-1})^{-1} = z, \\
((x \parallel y) \parallel (x \parallel (z^{-1} \parallel y)^{-1})^{-1}) = z, \\
((x \parallel (y \parallel (x \parallel z))^{-1})^{-1} \parallel z)^{-1} = y, \\
((x \parallel (y^{-1} \parallel (x \parallel z))^{-1})^{-1} \parallel z) = y, \\
(((x \parallel y)^{-1} \parallel z)^{-1} \parallel (x \parallel z))^{-1} = y, \\
(((x \parallel y^{-1})^{-1} \parallel z)^{-1} \parallel (x \parallel z)) = y.
\end{array} \tag{3.12}
$$

5 Proofs for Product/Inverse Axioms (3.1) and (3.7)

This section contains OTTER's proofs that (3.1) and (3.7) are single axioms, in terms of product and inverse, for groups and Abelian groups, respectively. Proofs found by our most successful OTTER strategies usually are more complex than necessary, and the following proofs are the result of several tricks to coerce OTTER into finding shorter proofs.

The justification $m \rightarrow n$ indicates paramodulation from n into n (substitution of an instance of the left side of m for an instance of a term in the left side of n), and $: i, j, \cdots$ indicates simplification with $i, j, \cdots$. The numbering of the equalities reflects the sequence of equalities retained by the program.

THEOREM 1. *The theory of groups can be defined by the single axiom*

$$(x \cdot (y \cdot (((z \cdot z^{-1}) \cdot (u \cdot y)^{-1}) \cdot x))^{-1}) = u. \tag{3.1}$$

Proof. First, Eq. (3.1) holds in groups, a fact that can be checked by straightforward calculation. Next, consider the following derivation, starting with (3.1).

5	$(x \cdot (y \cdot (((z \cdot z^{-1}) \cdot (u \cdot y)^{-1}) \cdot x))^{-1}) = u$	[(3.1)]
7	$(x \cdot ((((y \cdot y^{-1}) \cdot (z \cdot u)^{-1}) \cdot (v \cdot v^{-1})) \cdot (z \cdot x))^{-1}) = u$	[5→5]
9	$(x \cdot ((y \cdot (z \cdot z^{-1})) \cdot (u \cdot x))^{-1}) = (((v \cdot v^{-1}) \cdot (y \cdot u)^{-1}) \cdot (w \cdot w^{-1}))$	[5→7]
10	$(((y \cdot y^{-1}) \cdot (((z \cdot z^{-1}) \cdot (u \cdot x)^{-1}) \cdot u)^{-1}) \cdot (v \cdot v^{-1})) = x$	[7→9]
12	$(((x \cdot x^{-1}) \cdot y^{-1-1}) \cdot (z \cdot z^{-1})) = y$	[10→10]
14	$((x \cdot x^{-1}) \cdot (y \cdot z)^{-1}) = ((u \cdot u^{-1}) \cdot (y \cdot z)^{-1})$	[10→5]
15	$((x \cdot x^{-1}) \cdot y^{-1}) = ((z \cdot z^{-1}) \cdot y^{-1})$	[12→14:12]
17	$(u \cdot u^{-1}) = (v \cdot v^{-1})$	[15→5:5]
19	$(x \cdot x^{-1}) = ((y \cdot y^{-1}) \cdot (z \cdot z^{-1})^{-1})$	[17→15]
20	$(((x \cdot x^{-1}) \cdot ((y \cdot y^{-1}) \cdot z)^{-1}) \cdot (u \cdot u^{-1})) = z^{-1}$	[17→10]
22	$(x \cdot (y^{-1} \cdot ((z \cdot z^{-1}) \cdot x))^{-1}) = y$	[17→5]
25	$(x \cdot ((u \cdot u^{-1})^{-1-1} \cdot (w \cdot x))^{-1}) = w^{-1}$	[19→7:20]
32	$((x \cdot x^{-1})^{-1} \cdot (y^{-1} \cdot (z \cdot z^{-1}))^{-1}) = y$	[17→22]
34	$(x^{-1} \cdot ((y \cdot y^{-1})^{-1-1} \cdot (z \cdot z^{-1}))^{-1}) = x^{-1}$	[17→25]
36	$((y \cdot y^{-1}) \cdot (x \cdot (z \cdot z^{-1})^{-1-1})^{-1})^{-1} = x$	[5→25]
44	$(x \cdot ((y \cdot y^{-1})^{-1-1} \cdot (z \cdot z^{-1}))^{-1}) = x$	[36→34:36]
48	$((x \cdot x^{-1})^{-1-1} \cdot (y \cdot y^{-1})) = (z \cdot z^{-1})$	[44→17]
52	$(x \cdot (y \cdot y^{-1})^{-1}) = x$	[48→44]
57	$((z \cdot z^{-1})^{-1} \cdot u)^{-1-1} = u$	[52→10:20]
62	$(x^{-1} \cdot (y \cdot y^{-1}))^{-1} = x^{-1-1}$	[32→57]
65	$(y \cdot ((z \cdot z^{-1}) \cdot (x \cdot y)^{-1}))^{-1} = x^{-1-1}$	[5→57:52]
76	$(x \cdot (y \cdot y^{-1}))^{-1} = x^{-1}$	[57→62:57]
88	$((x \cdot x^{-1})^{-1} \cdot y^{-1-1}) = y$	[65→32]
92	$((u \cdot u^{-1}) \cdot y^{-1})^{-1} = y$	[65→20:12,76]
116	$(y \cdot (u \cdot u^{-1})) = y$	[76→32:76,88]
126	$((y \cdot z) \cdot z^{-1}) = y$	[76→5:92]
201	$(x \cdot y^{-1-1}) = (x \cdot y)$	[126→126]
207	$((x \cdot x^{-1}) \cdot z) = z$	[19→126:52,201]
215	$(x \cdot (y \cdot ((x \cdot y)^{-1} \cdot u))) = u$	[5→126:207,201]
227	$y^{-1-1} = y$	[126→36:207,52]
229	$(z \cdot x)^{-1} = (x^{-1} \cdot z^{-1})$	[126→25:227,207]
239	$(x \cdot ((x^{-1} \cdot u) \cdot y)) = (u \cdot y)$	[126→5:207,229,229,227,227]
260	$((x \cdot y) \cdot z) = (x \cdot (y \cdot z))$	[215→215:229,229,229,227,227,239]

By 17, there exists a unique element e such that for all x, $(x \cdot x^{-1}) = e$; it follows from 116 that e is a right identity; and 260 shows the associativity of product. ∎

THEOREM 2. *The theory of Abelian groups can be defined by the single axiom*

$$(((x \cdot y) \cdot z) \cdot (x \cdot z)^{-1}) = y. \tag{3.7}$$

Proof. First, Eq. (3.7) holds in Abelian groups, a fact that can be checked by straightforward calculation. Next, consider the following derivation, starting with (3.7).

8	$(((x \cdot y) \cdot z) \cdot (x \cdot z)^{-1}) = y$	[(3.7)]
10	$((x \cdot y) \cdot (((z \cdot x) \cdot u) \cdot y)^{-1}) = (z \cdot u)^{-1}$	[8→8]
12	$(x \cdot ((y \cdot x) \cdot (y \cdot z)^{-1})^{-1}) = z$	[8→8]
16	$((x \cdot (y \cdot z)^{-1}) \cdot x^{-1}) = (y \cdot z)^{-1}$	[8→10]
18	$(y \cdot (z \cdot ((y \cdot z) \cdot x)^{-1}))^{-1} = x$	[12→10]
23	$((x \cdot y) \cdot (x \cdot (y \cdot z))^{-1})^{-1} = z$	[10→18]
37	$((x \cdot y) \cdot x^{-1}) = y$	[23→16:23]
39	$((z \cdot y) \cdot (z \cdot x)^{-1})^{-1} = (x \cdot y^{-1})$	[12→16]
41	$(x \cdot ((y \cdot x) \cdot z)^{-1}) = (y \cdot z)^{-1}$	[8→16]
43	$(x \cdot (z \cdot x^{-1})) = z$	[12:39]
51	$(x \cdot (x \cdot z)^{-1})^{-1} = z$	[18:41]
53	$(x \cdot (y \cdot x)^{-1}) = y^{-1}$	[37→37]
55	$(y \cdot z)^{-1} = (y^{-1} \cdot z^{-1})$	[37→10:53]
58	$((((x \cdot y) \cdot z) \cdot x^{-1}) \cdot y^{-1}) = z$	[37→8]
60	$(x \cdot (y^{-1} \cdot y^{-1-1})) = x$	[37→8:55]
64	$(x^{-1} \cdot (x^{-1-1} \cdot y^{-1-1})) = y$	[51:55,55,55]
85	$x^{-1-1} = x$	[43→64]
92	$(x^{-1} \cdot (x \cdot y)) = y$	[64:85,85]
94	$(x \cdot (y^{-1} \cdot y)) = x$	[60:85]
101	$(x \cdot (x^{-1} \cdot y)) = y$	[85→92]
108	$(x \cdot y) = (y \cdot x)$	[92→37:85]
114	$(x \cdot (y \cdot y^{-1})) = x$	[85→94]
136	$(x \cdot x^{-1}) = (y \cdot y^{-1})$	[114→101]
172	$(((z \cdot x) \cdot y) \cdot z^{-1}) = (x \cdot y)$	[58→43]
184	$((x \cdot y) \cdot z) = ((z \cdot x) \cdot y)$	[92→172:85]
244	$((x \cdot y) \cdot z) = (x \cdot (y \cdot z))$	[184→108]

By 136, there exists a unique element e such that for all x, $(x \cdot x^{-1}) = e$; it follows from 114 that e is a right identity; and 108 and 244, respectively, show the commutativity and associativity of product. ∎

6 Conclusion

The remaining question is whether there exist single axioms simpler than the ones listed in Tables 1 and 2. Our focus has been on finding short axioms rather than on finding ones with few variables. The two cases that currently use four variables are {division, inverse} and {double division, inverse} for ordinary groups ((3.4) and (3.6) in Table 1). Are there single axioms for these cases with just three variables?

With our type criteria, there is currently no simplest-known single axiom for groups in terms of product and inverse; the ones given here have type $\langle 16, 7, 4 \rangle$, and Kunen's [6] have type $\langle 18, 7, 3 \rangle$. The only possibility for a simpler single axiom is $\langle 16, 7, 3 \rangle$, because a

single axiom must have an odd number ≥ 3 of occurrences of inverse, at least seven variable occurrences, and at least three variables [6].

The goal of the work reported here was to find simple single axioms. We made occasional use of FINDER [15] to search for small counterexamples when we had a promising candidate that OTTER could not prove to be a single axiom. However, further work in this area will most likely benefit from extensive model searches, for both simple models with a program like FINDER, and for more complex models as in Kunen's methods [6].

References

[1] G. Higman and B. H. Neumann. Groups as groupoids with one law. *Publicationes Mathematicae Debrecen*, 2:215–227, 1952.

[2] J. Hsiang and M. Rusinowitch. On word problems in equational theories. In T. Ottmann, editor, *Proceedings of 14th ICALP, Lecture Notes in Computer Science, Vol. 267*. Springer-Verlag, 1987.

[3] D. Kapur and H. Zhang. Proving equivalence of different axiomatizations of free groups. *Journal of Automated Reasoning*, 4(3):331–352, 1988.

[4] D. Knuth and P. Bendix. Simple word problems in universal algebras. In J. Leech, editor, *Computational Problems in Abstract Algebras*. Pergamon Press, 1970.

[5] K. Kunen, Sept.–Oct. 1991. Correspondence by electronic mail.

[6] K. Kunen. Single axioms for groups. Tech. Report 1076, Computer Sciences Dept., University of Wisconsin-Madison, February 1992. To appear in *J. Automated Reasoning*.

[7] D. Lankford. Canonical inference. Tech. Report ATP-32, Dept. of Computer Sciences, University of Texas, Austin, TX, 1975.

[8] W. McCune. OTTER 2.0 Users Guide. Tech. Report ANL-90/9, Argonne National Laboratory, Argonne, IL, March 1990.

[9] W. McCune. Proofs for group and Abelian group single axioms. Tech. Memo ANL/MCS-TM-156, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL, October 1991.

[10] W. McCune. Single axioms for the left group and right group calculi. Preprint MCS-P219-0391, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL, 1991. To appear in *Notre Dame J. Formal Logic*.

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

[12] W. McCune. Automated discovery of new axiomatizations of the left group and right group calculi. *Journal of Automated Reasoning*, 9(1):1–24, 1992.

[13] B. H. Neumann. Another single law for groups. *Bull. Australian Math. Soc.*, 23:81–102, 1981.

[14] B. H. Neumann. Yet another single law for groups. *Illinois Journal of Mathematics*, 30(2):295–300, 1986.

[15] J. Slaney. FINDER, finite domain enumerator: Version 1.0 notes and guide. Tech. Report TR-ARP-10/91, Automated Reasoning Project, Australian National University, Canberra, Australia, 1991.

[16] A. Tarski. Ein Beitrag zur Axiomatik der Abelschen Gruppen. *Fundamenta Mathematicae*, 30:253–256, 1938.

[17] A. Tarski. Equational logic and equational theories of algebras. In K. Schütte, editor, *Contributions to Mathematical Logic*, pages 275–288. North-Holland, 1968.