Single Axioms for Odd Exponent Groups

Joan Hart[1] and Kenneth Kunen[1]
University of Wisconsin
Madison, WI 53706, U.S.A.
jhart@math.wisc.edu and kunen@cs.wisc.edu
October 24, 1994

ABSTRACT

With the aid of automated reasoning techniques, we show that all previously known short single axioms for odd exponent groups are special cases of one general schema. We also demonstrate how to convert the proofs generated by an automated reasoning system into proofs understandable by a human.

§**0. Introduction.** There are two eras in the history of single axioms for groups and varieties of groups. The early results, by Neumann and others [7], often produced single axioms which were larger than the minimal possible size, but which were constructed via some scheme which made them easy to verify by hand. Although not optimal, these results had the virtue that a person could conceptually grasp their proofs. The second era began with the advent of McCune's automated reasoning system OTTER [4]; now one could produce shorter and simpler single axioms, which often required much more complex verifications. Short single axioms for groups and some varieties of groups were found by McCune and Wos [5,6], and by Kunen [2,3]; in many cases, these axioms were shown to be of optimal size. The results in these latter four papers had the defect that no insight was given into *why* the single axiom worked. The proofs often consisted of instructions on how to set up the OTTER input, and the reason given for considering a particular axiom was often that it survived an exhaustive computer search.

In this paper, we have our cake and eat it too – at least in the case of single axioms for odd exponent groups. We produce a large class of such axioms of minimal size, and we give conceptual proofs that these axioms are correct. We, too, used OTTER as a reasoning assistant, as advocated by Larry Wos, but found that by examining the output from our assistant, we could provide conceptual proofs which a human could also understand. This conceptual understanding, in turn, led us to discover more axioms.

We present most of our results in their final polished form, as theorems and proofs which can easily be checked by the reader without the aid of a computer. However, at the end of §3, we shall give one specific detailed example explaining the translation of OTTER output into this form.

We begin with our notation. We shall use i for the group inverse operation and e or 1 for a group identity. We shall use symbols such as $*$ or # to denote product operations, written in infix as usual, with products associating to the right, and we often omit the product symbol. We use exponentiation as a further abbreviation, with x^1 abbreviating x

[1] Authors supported by NSF Grant DMS-9100665.

and x^{n+1} abbreviating $x * x^n$. Thus, for example, x^3, $x * x * x$, and xxx all abbreviate the term $x * (x * x)$.

If $n \geq 1$ is an integer, a *group of exponent* n is a group which satisfies the equation $x^n = e$. We do not require that n be the smallest exponent of the group; so, for example, every group of exponent 3 is also a group of exponent 6. For groups of a fixed finite exponent, inverse and identity can be equationally defined in terms of product, so one may axiomatize such groups by equations using product only. We shall study here single axioms in product alone, and in product plus identity. In many cases, we can create an axiom with identity from one without identity by simply inserting an e in the correct place (see Theorem 1.8).

If α is a term constructed from $*$ and variables, then we say that the equation $(\alpha = y)$ is a *single axiom* for groups of exponent n iff $(\alpha = y)$ is valid in all groups of exponent n and every model for $(\alpha = y)$ is a group of exponent n. For example,

$$x * (x * (x * y) * z) * z * z = y \quad , \tag{A.3.1}$$

discovered by McCune and Wos (equation 4.3 of [6]), is a single axiom for groups of exponent 3.

If α is a term constructed from $*$, e, and variables, then we say that the equation $(\alpha = y)$ is a *single axiom* for groups of exponent n iff $(\alpha = y)$ is valid in all groups of exponent n (interpreting e as the identity), and every model for $(\alpha = y)$ is a group of exponent n in which e is the identity. An example, also taken from [6] (equation 4.10) is the following single axiom for groups of exponent 3:

$$x * (x * (x * y) * z) * e * z * z = y \quad . \tag{B.3.1}$$

However, we do not call

$$x * (x * (x * y) * z) * (e * e * e) * z * z = y$$

a single axiom for groups of exponent 3, because although every model for this axiom is a group of exponent 3, e can be interpreted as any constant in the model (since the cube of every element is the identity). If α contains only one occurrence of e, then in every model for $(\alpha = y)$ in which $*$ is a group operation, e must be the identity, as can be seen by setting all variables in α equal to the group identity.

One might also consider axioms in product and inverse, but we do not do that here. There are no single axioms for any variety of groups in product, identity, and inverse together (see Theorem 5.1).

The general form of the equations $A.3.1$ and $B.3.1$, as associative variants of $x^3yz^3 = y$, perhaps with an e inserted somewhere, is no accident. These are of the minimal possible size, and any single axiom of that minimal size must be of this general shape. More formally, let $V(\alpha)$ be the number of variable occurrences in α. Suppose $(\alpha = y)$ is a single axiom for groups of exponent $n > 1$. Then $V(\alpha) \geq 2n + 1$. So, for example, for $n = 3$, the minimal $V(\alpha)$, 7, is displayed by $A.3.1$ and $B.3.1$. Furthermore, if $n > 2$ and $V(\alpha) = 2n + 1$, then α must be some associative variant of $x^n yz^n$, with zero or more occurrences of e inserted. This is proved in Theorem 5.5.

We confine ourselves in this paper to such axioms of minimal possible size. The existence of arbitrarily long single axioms for groups of exponent n is immediate by a general result of Neumann [7]; see also [3]. For even $n > 2$, short single axioms are known only in the case of exponent 4, and the axioms with e [6] do not bear much resemblance to the axioms without e [3].

For small odd exponents, a number of such axioms, with and without e, were described by McCune and Wos [6]. For the most part, these axioms seemed unrelated, although McCune and Wos detected a few patterns in axioms for exponents 3 and 5 and extended the patterns to a sequence of axioms for odd exponents. They discovered their axioms by testing associative variants of $x^3yz^3 = y$ on OTTER. In analyzing their results, we discovered that all their axioms, with and without e, are in fact part of one meta-pattern. We also discovered a conceptual proof that the pattern provides axioms for groups of odd exponent.

Now, equation $A.3.1$ generalizes in three ways. First, as noticed by McCune and Wos [6], the axiom extends to larger odd exponents, producing axiom $A.n.1$ for every odd $n \geq 3$. For example, the exponent 7 axiom is

$$xxx(xxx(xy)z)z^6 = y \quad . \tag{A.7.1}$$

Second, replacing the z^6 by some particular other associative variants of z^6 produces still more axioms. One such axiom is

$$xxx(xxx(xy)z)(zz)(zz)(zz) = y \quad . \tag{C.7.1}$$

As before, there is also a corresponding $C.n.1$ for every odd $n \geq 3$. Third, by the notion of *cycling*, defined in §1, each of these axioms generates a family of 9 equations. For example, $A.7.1$ generates the family:

$$\begin{aligned}
xxx(xxx(xy)z)z^6 &= y && (A.7.1)\\
xx(xxx(xxy)z)z^6 &= y && (A.7.2)\\
x(xxx(xxxy)z)z^6 &= y && (A.7.3)\\
(xxx(xxxxy)z)z^6 &= y && (A.7.4)\\
xxx(xxxxyz^6)z &= y && (A.7.5)\\
xx(xxxx(xy)z^6)z &= y && (A.7.6)\\
x(xxxx(xxy)z^6)z &= y && (A.7.7)\\
(xxxx(xxxy)z^6)z &= y && (A.7.8)\\
xxxx(xxxyz)z^6 &= y && (A.7.9)
\end{aligned}$$

Cycle A.7

Equation $A.7.5$ is equation 4.7 from [6], and McCune and Wos verified that this pattern extends to all odd exponents. They also conjectured that pattern $A.7.1$ generalizes, which we verify here. In fact, we show (Theorem 1.4) that the members of such a family are all equivalent except (possibly) for $A.7.4$ and $A.7.9$. We do not know about $A.7.4$ and $A.7.9$, although they are equivalent to the others in all finite models.

To express our axioms for an arbitrary odd exponent, we use the following notation for repeated products:

Definition. Let $f_0(x, y)$ be y and let $f_{j+1}(x, y)$ be $x * f_j(x, y)$.

Thus, for example, $f_3(x, y)$ denotes $xxxy$, whereas x^3y denotes $(xxx)y$.

The form which generalizes $A.7.1$ and $C.7.1$, for odd exponent, $n = 2m + 1$ is

$$f_m(x, f_m(x, (x * y) * z) * g(z)) = y \quad , \qquad (G.n.1)$$

where $g(z)$ is some associative variant of z^{2m}, perhaps with an e inserted. By Theorem 1.4, for any such $g(z)$, $G.n.1$ is one of a collection of n equivalent equations.

Definition. If $g(z)$ is a term constructed from $*$, exactly $2m$ occurrences of the variable z, and zero or more occurrences of the constant e, we say that $g(z)$ *works* iff $G.n.1$ with that $g(z)$ is a single axiom for groups of exponent n.

Note that the form of $g(z)$ implies that $G.n.1$ will be valid in all groups of exponent n, so $g(z)$ works iff $G.n.1$ implies that $*$ is a group operation and, if e occurs in $g(z)$, that e is the identity. The "exponent n" part is then trivial by setting $y = z = e$ in $G.n.1$.

We do not have an algorithm to decide whether a given $g(z)$ works, but we have verified a number of general patterns. For example, $g(z) = z^{2m}$ (right associated) does work, as does $g(z) = (zz)^m$ (the form of $C.7.1$ above), as does $g(z) = z^{m+1} * z^{m-1}$. In exponent 5 without e, this gives us three $g(z)$ which do work: $zzzz$, $(zz)(zz)$, and $(zzz)z$. The other two associative variants of z^4, $((zz)z)z$ and $z(zz)z$, do not work.

Each single axiom without e yields a single axiom with e, since if $g(z)$ has no e in it, and works, then so does $g(z) * e$ (Theorem 1.8). However, $e * g(z)$ could fail; for example, in exponent 5, $e * (zz)(zz)$ fails. However, $g(z) = e * z^{2m}$ does work, as was conjectured by McCune and Wos [6], who, with the help of OTTER, verified it up to exponent 19.

Sections 1 and 2 contain some consequences of $G.n.1$, which hold for all $g(z)$. In particular, in §2, we show that $g(z)$ working is equivalent to a statement about automorphisms of groups. Proofs for the $g(z)$ which work are given in §3, and countermodels for some $g(z)$ which do not work are given in §4. In §5, we prove some facts about single axioms in general. In §6, we show that our meta-pattern includes all single axioms for groups of exponent 3, but we also demonstrate there a single axiom for groups of exponent 5 which the pattern omits.

§1. Cycles. We begin with the following elementary observation. Consider the two equations:

$$\forall y(k(h(y)) = y) \qquad (1)$$

$$\forall y(h(k(y)) = y) \qquad (2)$$

Now, (1) and (2) are not in general equivalent, but they are equivalent statements if k and h are bijections. Generalizing this idea, we shall see that under an assumption of injectivity or surjectivity, we can establish the equivalence of some equations of apparently different form. In this way, each single axiom for groups will immediately give rise to a number of equivalent clones.

Suppose that γ and π are terms in variables y, $x_1, \ldots x_n$. Let $\gamma(\tau), \pi(\tau)$ denote the result of substituting the term τ for all occurrences of y in γ, π. So $\gamma(y), \pi(y)$ are the same as γ, π. Now, consider the equations:

$$\forall y, x_1, \ldots x_n \left(\pi(\gamma(y)) = y \right) \tag{1}$$

$$\forall y, x_1, \ldots x_n \left(\pi(\gamma(\pi(y))) = \pi(y) \right) \tag{1.5}$$

$$\forall y, x_1, \ldots x_n \left(\gamma(\pi(y)) = y \right) \tag{2}$$

Clearly, (1) $\Rightarrow$ (1.5) and (2) $\Rightarrow$ (1.5). But also (1) $\Rightarrow$ (2) under the injectivity assumption

$$\forall u1, u2, x_1, \ldots x_n (\pi(u1) = \pi(u2) \Rightarrow u1 = u2) \quad ,$$

since that yields (1.5) $\Rightarrow$ (2); similarly, (2) $\Rightarrow$ (1) under the surjectivity assumption

$$\forall v, x_1, \ldots x_n \exists u (\pi(u) = v) \quad ,$$

since that yields (1.5) $\Rightarrow$ (1).

We shall use this only in the case that $\pi(y)$ is a product of the form $y * \delta$ or $\delta * y$, whence $\pi(\gamma(y))$ is $\gamma(y) * \delta$ or $\delta * \gamma(y)$, and $\gamma(\pi(y))$ is $\gamma(y * \delta)$ or $\gamma(\delta * y)$. Then, a somewhat simpler notion of surjectivity and injectivity will suffice for our purpose:

Definition. A binary function $*$ is called
left injective or *left cancellative* iff $\forall u1, u2, x \, (x * u1 = x * u2 \Rightarrow u1 = u2)$
left surjective iff $\forall v, x \exists u (x * u = v)$
left bijective iff it is both left injective and left surjective
right injective or *right cancellative* iff $\forall u1, u2, x \, (u1 * x = u2 * x \Rightarrow u1 = u2)$
right surjective iff $\forall v, x \exists u (u * x = v)$
right bijective iff it is both right injective and right surjective

Thus, for example, left surjective says that if we fix any x, multiplication on the left by x ($u \mapsto x * u$) is a surjection.

Definition. Σ is the set of all terms in $*$, constants, and variables, which have exactly one occurrence of y. A map $T : \Sigma \to \Sigma$ is defined as follows: $T(y)$ is y. If α is of the form $\delta * \gamma(y)$, where δ does not contain y, we say that *y is on the right* in α, and we let $T(\alpha)$ be $\gamma(\delta * y)$. If α is of the form $\gamma(y) * \delta$, where δ does not contain y, we say that *y is on the left* in α, and we let $T(\alpha)$ be $\gamma(y * \delta)$.

1.1 Lemma. *T is a bijection from Σ onto Σ. For each $\alpha \in \Sigma$, there is a finite n such that $T^n(\alpha)$ is α.*

Thus, each $\alpha \in \Sigma$ is part of a finite *cycle*, $\alpha, T(\alpha), T^2(\alpha), \ldots, \alpha$. An example of a cycle of length 9 is cycle $A.7$ in the Introduction. As examples of the computation of T: In $A.7.1$, y is on the right; we write α as $x * xx(xxx(x \ y \ )z)z^6$, and $T(\alpha)$ is $xx(xxx(x \ (x * y) \ )z)z^6$, which is $A.7.2$. In $A.7.4$, y is on the left; we write this α as $[xxx(xxxx\ y)\ z] * z^6$, and $T(\alpha)$ is $[xxx(xxxx\ (y * z^6))\ z]$, which is $A.7.5$.

In any model in which $*$ is left and right bijective, all axioms in a cycle are equivalent. More precisely,

1.2 Lemma. Suppose α is a term in Σ.

a. If y is on the right in α, then every left injective model for $(\alpha = y)$ is a model for $(T(\alpha) = y)$

b. If y is on the right in α, then every left surjective model for $(T(\alpha) = y)$ is a model for $(\alpha = y)$

c. If y is on the left in α, then every right injective model for $(\alpha = y)$ is a model for $(T(\alpha) = y)$

d. If y is on the left in α, then every right surjective model for $(T(\alpha) = y)$ is a model for $(\alpha = y)$

Proof. For (a,b), α is $\delta * \gamma(y)$, and the π in (1)(1.5)(2) above is just $\delta * y$. For (c,d), α is $\gamma(y) * \delta$, and the π in (1)(1.5)(2) above is just $y * \delta$. ∎

Obviously, we could extend our cycles to the case of terms with i, where $T(i(\gamma(y))) = \gamma(i(y))$, and going around the cycle would require injectivity or surjectivity of i. In fact, $T(\alpha)$ could be defined for terms with exactly one y in any language.

Many of the equations that we meet in studying single axioms for groups imply the needed injectivity or surjectivity. In some cases, this implication is immediate by the following:

1.3 Lemma. Let $\delta(y)$ be a term.

a. Every model for $(\delta(x * y) = y)$ satisfies left injectivity.

b. Every model for $(x * \delta = y)$ satisfies left surjectivity.

c. Every model for $(\delta(y * x) = y)$ satisfies right injectivity.

d. Every model for $(\delta * x = y)$ satisfies right surjectivity.

We remark that the Lemma does not require that y occur exactly once in δ, although y does occur exactly once in our intended applications.

As an example of the Lemma: In Cycle $A.7$, equation $A.7.1$ is of the form $\ldots(xy)\ldots = y$, and hence implies left injectivity (by 1.3a). Thus, since y is on the right, $A.7.1$ implies $A.7.2$ in any model (by 1.2a). Also, equation $A.7.2$ is of the form $x * \ldots = y$, and hence implies left surjectivity (1.3b); so $A.7.2$ implies $A.7.1$ in any model (1.2b).

Likewise, since y is on the right in $A.7.7$, $A.7.7$ implies $A.7.8$ in any model satisfying left injectivity, and $A.7.8$ implies $A.7.7$ in any model satisfying left surjectivity. Now $A.7.7$ is of the form $\ldots(xy)\ldots = y$, and hence implies left injectivity, but $A.7.8$ is of the form $\ldots * z = y$, which implies *right* surjectivity; so it is not immediately clear that $A.7.8$ implies $A.7.7$ in every model. It does, however, as we show by studying the cycle more carefully. We turn to a proof of this now, in general form.

In general, we consider equation $G.n.1$ of the Introduction, and study its cycle, which has length $n + 2$.

In the following display, to make the pattern clear, we sometimes write an axiom twice, rewriting an xy as $f_1(x, y)$.

$$\left.\begin{array}{r} f_m(x, f_m(x, (x * y) * z) * g(z)) = y \\ f_m(x, f_m(x, f_1(x, y) * z) * g(z)) = y \end{array}\right\rangle \qquad (G.n.1)$$

$$f_{m-1}(x, f_m(x, f_2(x, y) * z) * g(z)) = y \qquad (G.n.2)$$

$$\circ \circ \circ \circ \circ \circ \circ \circ \circ$$

$$\left.\begin{array}{r} f_1(x, f_m(x, f_m(x, y) * z) * g(z)) = y \\ x * f_m(x, f_m(x, y) * z) * g(z) = y \end{array}\right\rangle \qquad (G.n.m)$$

$$f_m(x, f_{m+1}(x, y) * z) * g(z) = y \qquad ?(G.n.m + 1)$$

$$f_m(x, f_{m+1}(x, y * g(z)) * z) = y \qquad (G.n.m + 2)$$

$$\left.\begin{array}{r} f_{m-1}(x, f_{m+1}(x, (x * y) * g(z)) * z) = y \\ f_{m-1}(x, f_{m+1}(x, f_1(x, y) * g(z)) * z) = y \end{array}\right\rangle \qquad (G.n.m + 3)$$

$$\circ \circ \circ \circ \circ \circ \circ \circ \circ$$

$$\left.\begin{array}{r} f_1(x, f_{m+1}(x, f_{m-1}(x, y) * g(z)) * z) = y \\ x * f_{m+1}(x, f_{m-1}(x, y) * g(z)) * z = y \end{array}\right\rangle \qquad (G.n.2m + 1)$$

$$f_{m+1}(x, f_m(x, y) * g(z)) * z = y \qquad (G.n.2m + 2)$$

$$f_{m+1}(x, f_m(x, y * z) * g(z)) = y \qquad ?(G.n.2m + 3)$$

Cycle G.n $\quad n = 2m + 1$

The symbol $g(z)$ has a dual meaning. Our original intent was that it stand for some associative variant of z^{2m}, perhaps with an e inserted. But, the basic results of this section hold if $g(z)$ is *any* function of z – that is, we can consider g to be a new function symbol of the language. In this generality, we can prove a number of results which come *close* to saying that $*$ is an exponent n group operation and g is the group inverse operation. Then, in §3 and §4, when we replace $g(z)$ by a specific term, it will often be easy to see whether or not the resultant equation really is a single axiom for groups of exponent n.

However, $f_j(x, u)$ *always* stands for one specific term, as defined in the Introduction. Observe, in going down the cycle, that $f_j(x, u)$ is the same term as $x * f_{j-1}(x, u)$; since we are right associating, any expression beginning as $f_j(x, \ldots) \ldots$ is really of the form $x * \ldots$, with y on the right.

This display emphasizes the structure of the cycle for large n; for $n = 3, 5$, the equation labels overlap somewhat; for example, for $n = 5, m = 2$: $G.n.m + 3$ and $G.n.2m + 1$ are the same.

For any n and $g(z)$, all the members of the cycle are equivalent except (possibly) the two marked with a ?.

1.4. Theorem. In cycle $G.n$, with $n = 2m + 1$, if $g(z)$ is any function, then each of the equations $G.n.i$ except (possibly) $G.n.m + 1$ and $G.n.2m + 3$ implies all the other equations in the cycle, together with left and right bijectivity. Every *finite* model for either $G.n.m + 1$ or $G.n.2m + 3$ satisfies all the equations in cycle $G.n$.

Proof. We make frequent use of Lemmas 1.2 and 1.3, plus some additional arguments. $G.n.1$ immediately implies left surjectivity and left injectivity. By left surjectivity, it implies $G.n.2m+3$, which implies right injectivity. Thus, any model for $G.n.1$ is left and right injective, and thus satisfies $G.n.2, G.n.3, \ldots$; that is, $G.n.1$ implies all the other equations in the cycle. Since $G.n.2m+2$ implies right surjectivity, $G.n.1$ implies left and right bijectivity. So, it is sufficient now to show that each of the equations except (possibly) $G.n.m+1$ and $G.n.2m+3$ implies $G.n.1$.

Each of $G.n.2$ through $G.n.m$ implies left surjectivity, and hence $G.n.1$.

Equation $G.n.m+2$ implies $G.n.1$ by the following longer argument. Let us use f for f_m, and note that $f_{m+1}(x,u) = x * f(x,u)$. Writing $G.n.m+2$ twice:

$$
\begin{array}{lllllll}
f(x,[x* & f(x, & y & * & g(z)) &]*z) = y & \\
 & f(u, & [u*f(u,v*g(w))] & * & w) & = v & ,
\end{array}
$$

and matching $(w \to g(z) \quad x \to u \quad y \to u * f(u, v * g(g(z))))$, we get $f(u,(u*v)*z) = u * f(u, v * g(g(z)))$. Comparing this with $G.n.m+2$:

$$
\begin{array}{lllllllll}
 & f(u,(u*v)*z) = & u*f(& u & , & v & * & g(g(z))) & \\
f(u, & & u*f(& u & , & v & * & g(w)) & *w) = v \quad ,
\end{array}
$$

matching $(w \to g(z))$, and substituting the first equation into the second, we get $G.n.1$:

$$f(u, f(u,(u*v)*z) * g(z)) = v \quad .$$

Now, each of $G.n.m+3$ through $G.n.2m+1$ implies left surjectivity, and hence $G.n.m+2$, and hence, as we have just seen, $G.n.1$.

Finally, we verify that $G.n.2m+2$ implies left surjectivity (and hence $G.n.2m+1$, and hence $G.n.1$). We again use f for f_m, and now note that $f_{m+1}(x,u) = f(x, x*u)$. Writing $G.n.2m+2$ twice:

$$
\begin{array}{llllll}
f(x,x* & f(x, & y &)* & g(z) &)*z = y \\
 & f(u, & u*f(u,v)*g(w) &)* & w & = v
\end{array}
$$

and matching $(w \to g(z) \quad x \to u \quad y \to u * f(u,v) * g(g(z)))$, we get $f(u, u*v)*z = u * f(u,v) * g(g(z))$. Comparing this with $G.n.2m+2$:

$$
\begin{array}{lllllll}
f(u, & u & * & v &)* & z & = u * f(u,v) * g(g(z)) \\
f(u, & u & * & f(u,y)*g(z) &)* & z & = y
\end{array}
$$

and matching $(v \to f(u,y) * g(z))$ we get

$$u * f(u, f(u,y) * g(z)) * g(g(z)) = y \quad .$$

This is of the form $u * \ldots = y$, and hence implies left surjectivity.

Equation $G.n.m+1$ implies left injectivity, which is equivalent to left surjectivity in any finite model. Since y is on the right in $G.n.m$, every finite model for $G.n.m+1$ satisfies

$G.n.m$, and hence the rest of the cycle. Likewise, in a finite model, $G.n.2m+3$ implies right surjectivity and hence $G.n.2m+2$, and hence the rest of the cycle. ∎

This theorem was discovered through cooperation with OTTER. We could see most of the implications easily enough by hand, but we had trouble showing that $G.n.m+2$ and $G.n.2m+2$ implied the rest of the cycle axioms. For $G.n.2m+2$, we simply ran OTTER with this equation in the `sos`, expressing the equation in terms of $*$, g, and $f = f_m$. We also put $x * f(x,u) = f(x, x * u)$ in the `sos`. We then examined the output for other cycle axioms or for some equation which would yield (via Lemma 1.3) the injectivity or surjectivity needed to imply another cycle axiom. When we found an interesting equation in the output, we ran OTTER again with that equation negated, so that we would get a proof to examine. After a bit of experimentation, we found the reasonably short proof above. We did likewise with $G.n.m+2$.

We tried to do the same for $G.n.m+1$ and $G.n.2m+3$, but failed. Even in the case $n=3$, with $g(z) = z * z$, these do not seem to produce any interesting consequences. We conjecture that these do not imply the rest of the cycle equations, or the group axioms, but we do not have a model to prove this. In [3], the two bad apples in a cycle were refuted by a trivial Knuth-Bendix argument, since they failed to unify with any proper subterms of themselves, but that simple argument does not work here.

Having established Theorem 1.4, we proceeded to see what consequences of the general cycle could be derived for an arbitrary $g(z)$. Presumably, this would make the study of specific $g(z)$ (as in §§3,4) easier. We again ran OTTER, using as axioms those cycle equations which could be expressed in terms of $f = f_m$, together with left and right injectivity. Observe that in view of the definition of f, *left* injectivity for f can be inferred from left injectivity for $*$; this is not true for right injectivity. Thus, we expressed injectivity by putting the following clauses in the `usable` list:

```
x * y != u | x * z != u | y = z.
y * x != u | z * x != u | y = z.
f(x,y) != u | f(x,z) != u | y = z.
```

We set up the run so that only equations were generated. We again examined the output for interesting equations, and then applied the procedure described above to obtain short proofs of them. In particular, the ones in the following theorem seemed especially significant.

1.5. Theorem. In cycle $G.n$, with $n = 2m+1$, if $g(z)$ is any function, then each of the equations $G.n.i$ except (possibly) $G.n.m+1$ and $G.n.2m+3$ implies the following:

a. The expression $f_m(x, f_{m+1}(x,z) * g(z))$ is a constant, which we shall call $\mathbf{1}$.
b. $x * \mathbf{1} = x$.
c. $\mathbf{1} * g(g(y)) = y$.
d. $g(g(\mathbf{1} * x)) = x$.
e. $g(\mathbf{1}) = \mathbf{1}$.
f. $f_n(x,y) = y$.
g. $(x * y) * (\mathbf{1} * z) = x * (y * z)$.
h. $f_j(x, y * z) = f_j(x,y) * f_j(\mathbf{1}, z)$ for every j.
i. $z * f_m(\mathbf{1}, g(z)) = \mathbf{1}$.

Equation (b) says that there is a right identity, which, by injectivity of $*$, must then be unique. Right inverse ($\forall x \exists y (x * y = 1)$) is immediate from left surjectivity. So, by (g), $*$ is a group operation iff 1 is also a left identity. This observation will be useful when we verify specific $g(z)$ in §3. Note that if $*$ is a group operation, then (i) reduces to $z * g(z) = 1$, so g is the group inverse.

Proof of 1.5. By Theorem 1.4, we have all the cycle equations at once. Let us write equation $G.n.m+1$, replacing z by $g(z)$ and y by z, followed by equation $G.n.2m+3$, replacing y by x (and noting that $f_{m+1}(x,u) = x * f_m(x,u) = f_m(x, x*u)$):

$$\begin{array}{llll} & f_m(x, f_{m+1}(x,z) * g(z)) \quad * g(g(z)) & = z & (G.n.m+1) \\ x* & f_m(x, f_{m+1}(x,z) * g(z)) & = x & (G.n.2m+3) \end{array} \quad .$$

The first equation plus right cancellation implies that the value of $f_m(x, f_{m+1}(x,z)*g(z))$ is independent of the value of x, and the second equation plus left cancellation implies that the value of $f_m(x, f_{m+1}(x,z)*g(z))$ is independent of the value of z. Thus, $f_m(x, f_{m+1}(x,z) * g(z))$ is a constant, which we are calling 1, and we have established (a),(b), and (c).

For (d), set $y = 1 * x$ in $(1 * g(g(y)) = y)$, and apply left cancellation.

To establish (e), set $x = y = z = 1$ in equation $G.n.m+1$, and apply $1 * 1 = 1$ to get

$$1 * g(1) = 1 = 1 * 1 \quad ,$$

whence $g(1) = 1$ follows by left cancellation.

To establish (f), set $z = 1$ in equation $G.n.m+1$, and apply the fact that $g(1) = 1$ and 1 is a right identity. We get $f_m(x, f_{m+1}(x,y)) = y$; but $f_m(x, f_{m+1}(x,y))$ is the same as $f_{2m+1}(x,y)$, or $f_n(x,y)$.

For (g), let us write equation $G.n.1$, replacing z by u, followed by equation $G.n.m+2$, replacing z by $g(u)$, (noting that $f_{m+1}(x,w) = f_m(x, x*w)$):

$$\begin{array}{lllll} f_m(x, f_m(x, & (x*y)*u) & *g(u)) & = y & (G.n.1) \\ f_m(x, f_m(x, & x*(y*g(g(u)))) & *g(u)) & = y & (G.n.m+2) \end{array} \quad .$$

Left cancelling x m times, right cancelling $g(u)$, and then left cancelling x m more times, we get $(x*y)*u = x*(y*g(g(u)))$. Now, replacing u by $1*z$ and applying (d), we get (g).

Now, (h) follows from (g) by induction. The case $j = 0$ is trivial and $j = 1$ is just a restatement of (g). Assuming it holds for j, we prove it for $j+1$ by applying (g) again:

$$f_{j+1}(x, y*z) = x*(f_j(x,y)*f_j(1,z)) = (x*f_j(x,y))*(1*f_j(1,z)) = f_{j+1}(x,y)*f_{j+1}(1,z) \quad .$$

For (i), consider the definition of 1 in (a), and apply (h) and (f):

$$\begin{gathered} 1 = f_m(x, f_{m+1}(x,z) * g(z)) = f_m(x, f_{m+1}(x,z)) * f_m(1, g(z)) = \\ f_n(x,z) * f_m(1, g(z)) = z * f_m(1, g(z)) \quad \blacksquare \end{gathered}$$

When using OTTER to verify that a specific $g(z)$ works, one might replace $g(z)$ by its definition in terms of $*$, and use as input all the cycle axioms, together with the consequences of Theorem 1.5, and try to derive $1 * x = x$. In fact, consequences (b)(f)(g)(i) of

Theorem 1.5 are sufficient to imply the cycle axioms, and hence all the other consequences of Theorem 1.5. This is of interest when searching for a proof, since we may argue from assumptions of a much simpler syntactic form, and therefore use a much lower weight bound.

1.6. Theorem. Suppose that g is any function, 1 is a constant, and (b)(f)(g)(i) of Theorem 1.5 all hold. Then $*$ satisfies all the axioms of cycle $G.n$.

Proof. As we noted in the proof of 1.5, (h) follows directly from (g), so we can use (h) also. Applying, (h), (f), (g), (i), then (b), we verify $G.n.2m+3$ as follows:

$$f_{m+1}(x, f_m(x, y*z) * g(z)) = f_{m+1}(x, f_m(x, y*z)) * f_{m+1}(1, g(z)) =$$
$$f_n(x, y*z) * (1 * f_m(1, g(z))) = (y*z) * (1 * f_m(1, g(z))) = y * (z * f_m(1, g(z))) = y * 1 = y \quad .$$

Now, $G.n.1$ follows from $G.n.2m+3$ using left injectivity, which follows from (f). The rest of $G.n$ now follows by Theorem 1.4. ∎

When we replace $g(z)$ by a specific term built from $*$, we must be careful in considering single axioms *with* identity. Here, $g(z)$ is a term constructed from z and one or more occurrences of the constant e. As pointed out in the Introduction, calling the constant "e" is just wishful thinking; we must still *prove* that the axiom forces e to be the same as the identity 1 that we already have. However, by the next theorem, if e occurs just once in $g(z)$, then our wish is always fulfilled:

1.7. Theorem. Suppose that $g(z)$ is composed of $*$, z, and exactly one occurrence of a constant e, and suppose that the cycle axiom $G.n.1$ holds. Then $e = 1$.

Proof. We use Theorem 1.5. First note that, since 1 is a right identity, $\forall x(x1 = 1 \Rightarrow x = 1)$, and using $1 = 11$, plus left cancellation, $\forall x(1x = 1 \Rightarrow x = 1)$. It follows by induction that whenever $\delta(x)$ is a term in 1, $*$, and exactly one occurrence of x, $\forall x(\delta(x) = 1 \Rightarrow x = 1)$. In particular, letting $\delta(x)$ be g and x be e, and using $g(1) = 1$ (by 1.5(e)), we have $e = 1$. ∎

The next result gives us a general way of converting a single axiom without identity to one with identity.

1.8. Theorem. If $g(z)$ is an associative variant of z^{2m} and $g(z)$ works, then so does $g(z) * e$.

Proof. By Theorems 1.5 (b) and 1.7, equation $G.n.1$ using $g(z) * e$ implies that e is a right identity. So $g(z) * e$ reduces to $g(z)$. ∎

The results of the next section might make the results of this section less mysterious.

§**2. Group Models.** Given a group G with product $\#$, we show how to define a new operation $*$ on G. Special cases of this idea were discussed in [2,3] as a way of defeating a candidate $(\alpha = y)$ by constructing a non-group model in which $(\alpha = y)$ is valid. This construction takes on added importance here, since the equations we consider can *only* be defeated by such a model. That is, every model for cycle $G.n$ *is* a group in a natural way, but $*$ need not be the group operation – this depends on $g(z)$.

First, we describe how to build a non-group from a group, and then we explain how to go backwards.

Let G be any group, with group operation $\#$, and suppose φ, ψ are automorphisms of G which commute ($\varphi \circ \psi = \psi \circ \varphi$). We define another operation $*$ on G by

$$x * y = \varphi(x) \# \psi(y) \quad .$$

We use 1 to denote the identity of the group $(G, \#)$.

Observe that $*$ has the following properties:

A. $x * 1 = \varphi(x)$; $1 * y = \psi(y)$.

B. $1 * 1 = 1$.

C. $*$ is left and right bijective.

D. $(x * 1) * (y * z) = (x * y) * (1 * z)$.

(A) and (B) follow from the fact that automorphisms must take 1 to 1. (C) uses the bijectivity of φ and ψ and the left and right bijectivity of $\#$. To prove (D) note that since φ and ψ commute, both the left and the right sides of the equation are equal to $\varphi(\varphi(x)) \# \varphi(\psi(y)) \# \psi(\psi(z))$.

In a group, the identity is the only element which can satisfy equation (B); so by (A), $*$ is a group operation iff φ and ψ are both the identity automorphism.

2.1. Theorem. Assume we have an operation $*$ on a set H and a $1 \in H$, and assume (B),(C),(D) above all hold. Following (A), define

$$\varphi(x) = x * 1 \quad , \quad \psi(y) = 1 * y \quad ;$$

and then define

$$x \# y = \varphi^{-1}(x) * \psi^{-1}(y) \quad .$$

Then $\#$ is a group operation on H with identity 1, φ and ψ are automorphisms of the group $(H, \#)$, $\varphi \circ \psi = \psi \circ \varphi$, and $x * y = \varphi(x) \# \psi(y)$.

Note that the theorem applies to models for most of the equations of cycle $G.n$. By Theorem 1.5 (b)(g) and Theorem 1.4, each of the equations $G.n.i$ except (possibly) $G.n.m+1$ and $G.n.2m+3$ implies (B),(C),(D). For models of these equations, since (B) is strengthened to $x * 1 = x$, φ will be the identity map, and by 1.5(c), $\psi^{-1}(y) = g(g(y))$; so $x \# y = x * g(g(y))$.

We prove the Theorem in the general form to emphasize the symmetry between φ and ψ. Observe that (C) implies that φ, ψ are bijections, so that their inverses, φ^{-1}, ψ^{-1} are defined and are bijections also.

Proof of 2.1. The fact $x * y = \varphi(x) \# \psi(y)$ is immediate from the definition of $\#$. Next, by (B), $\varphi(1) = \psi(1) = 1$; so also $\varphi^{-1}(1) = \psi^{-1}(1) = 1$. Thus

$$x \# 1 = \varphi^{-1}(x) * 1 = \varphi(\varphi^{-1}(x)) = x \quad ,$$

and 1 is a right identity with respect to $\#$. Similarly, 1 is a left identity.

Next, $\#$ is left and right bijective because $*$ is and φ, ψ are bijections. In particular, by left and right surjectivity, there are left and right inverses:

$$\forall x \exists y (x \# y = 1) \quad ; \quad \forall x \exists y (y \# x = 1) \quad ,$$

although it is not clear, until we prove associativity, that the left and right inverses of x are the same.

To see that $\varphi \circ \psi = \psi \circ \varphi$, put $x = z = e$ in (D) ; using (B), we get $1 * (y * 1) = (1 * y) * 1$, or $\psi(\varphi(y)) = \varphi(\psi(y))$.

Next, put $x = 1$ in (D). We get $\psi(y * z) = \psi(y) * \psi(z)$, or, using the fact that ψ, φ commute, $\psi(\varphi(y) \# \psi(z)) = \psi(\varphi(y)) \# \psi(\psi(z))$. Since ψ, φ are bijections, this establishes:

$$\psi(y \# z) = \psi(y) \# \psi(z) \quad .$$

Likewise, putting $z = 1$ in (D) establishes

$$\varphi(x \# y) = \varphi(x) \# \varphi(y) \quad .$$

So, φ, ψ will be group automorphisms if we can show that $\#$ is a group operation, for which all we need prove is associativity. To do this, replace $*$ by its definition in terms of $\#$ in (D), and then use the last two equations. We get

$$\varphi\varphi(x) \# (\psi\varphi(y) \# \psi\psi(z)) = (\varphi\varphi(x) \# \varphi\psi(y)) \# \psi\psi(z) \quad ,$$

which implies

$$x \# (y \# z) = (x \# y) \# z \quad ,$$

because ψ, φ are commuting bijections. ∎

We comment further on the case that φ is the identity automorphism, since that is the situation with our main cycle $G.n$. Note then that

$$f_j(x, y) = x \# \psi(x) \# \ldots \# \psi^{j-1}(x) \# \psi^j(y) \quad , \tag{1}$$

so that

$$f_j(e, y) = \psi^j(y) \quad . \tag{2}$$

We can then express the cycle axioms in terms of requirements on ψ:

2.2. Theorem. Suppose that H is a group, with product $\#$ and identity 1, and g is an arbitrary unary function on H. Suppose that ψ is an automorphism of H, and define $*$ by $x * y = x \# \psi(y)$. Then all the axioms of cycle $G.n$ hold iff

$$x \# \psi(x) \# \ldots \# \psi^{2m}(x) = 1 \tag{3}$$
$$g(z) \# \psi^m(z) = 1 \tag{4}$$

both hold.

Proof. Assume the cycle axioms and apply Theorem 1.5. In particular, by (f), $f_n(x,1) = 1$, from whence we get (3) by applying (1). Next, observe that (3) implies

$$\psi^n(x) = x \quad , \tag{5}$$

since by (3),

$$x\#\psi(1) = x\#\psi(x)\#\ldots\#\psi^{2m+1}(x) = 1\#\psi^{2m+1}(x) \quad ,$$

or $x = \psi^{2m+1}(x)$. Now, by (2) and Theorem 1.5(i), $z\#\psi^{m+1}(g(z)) = 1$, or $\psi^{m+1}(g(z)) = z^{-1}$, or, by (5), $g(z) = \psi^m(z^{-1})$. Now, (4) follows, since ψ is an automorphism.

To prove the converse, assume (3) and (4). By Theorem 1.6, it suffices to derive (b)(f)(g)(i) of Theorem 1.5. But (b) and (g) are trivial, and (f) and (i) follow easily by reversing the above argument. ■

This theorem could also have been proved directly, by expanding one of the cycle axioms in terms of #.

Given a specific g, we can express it explicitly using ψ and #. Then, Theorem 2.2 can be used in two ways. If one can produce a group and a ψ which is not the identity automorphism such that (3) and (4) hold, then we have proved that g does not work. However if we can prove that (3) and (4) imply that ψ is the identity automorphism, then we have proved that g does work.

Thus, the question of whether a specific g works is reduced to the existence of groups with a specific kind of automorphism. We do not know in general whether this question is decidable, but we shall answer it in a number of specific cases in §3 and §4.

Note that (5) says that the automorphism ψ has order n. By (4), $g(z) = (\psi^m(z))^{-1}$, so g is an anti-automorphism: $g(x\#y) = g(y)\#g(x)$; g is an automorphism iff # is commutative. However, $g^2 = \psi^{2m} = \psi^{-1}$ is a group automorphism of order n.

We can now understand what Theorem 1.5 says in terms of #. Parts (b)(f)(g)(i) were just discussed above. (c) and (d) both say again that $\psi^{-1} = g \circ g$. (h) is clear in terms of #, since if we expand out either side of the equation, $f_j(x, y * z)$ or $f_j(x,y) * f_j(1,z)$, we get

$$x\#\psi(x)\#\ldots\#\psi^{j-1}(x)\#\psi^j(y)\#\psi^{j+1}(z) \quad .$$

§3. Some $g(z)$ which work. Using OTTER, we were able to show the four $g(z)$ specified in the Introduction work.

3.1. Theorem. The following $g(z)$ work:

A. $g(z) = z^{2m}$
B. $g(z) = e * z^{2m}$
C. $g(z) = (z^2)^m$
D. $g(z) = z^{m+1} * z^{m-1}$.

That is, if $g(z)$ is given by (A), (B), (C), or (D), then equation $G.n.1$ with that $g(z)$ is a single axiom for groups of exponent n.

By examining the OTTER proof of Theorem 3.1, we were able to construct a fairly short proof, which is easy to verify by hand. We present the short proof first. At the end of this section, we comment more specifically on how we used OTTER.

For the short proof, we rewrite each $g(z)$ in terms of ψ and $\#$. We then use the results of Section 2, showing that ψ must be the identity automorphism to conclude that $g(z)$ works.

First, a lemma:

3.2. Lemma. Let Φ be any function, and suppose that $a \in \mathrm{dom}(\Phi)$ and $\Phi^i(a) = \Phi^j(a) = a$, where i, j are relatively prime positive integers. Then $\Phi(a) = a$.

Proof. Let k be the least positive integer such that $\Phi^k(a) = a$, and note that k must divide both i and j. ∎

Proof of Theorem 3.1. In all four cases, we simply rewrite $g(z)$ in terms of ψ and $\#$, and then insert it into equation (4) of Theorem 2.2. We then use 2.2(3), cancellation, and the automorphism properties of ψ to show either $\forall x(\psi^{m+1}(x) = x)$ or $\forall x(\psi^m(x) = x)$. Since we always have $\forall x(\psi^n(x) = x)$ (see equation (5) of §2), and both m and $m+1$ are relatively prime to n, we may then conclude that $\forall x(\psi(x) = x)$ by Lemma 3.2.

For (A), $g(x) = x\#\psi(x)\#\ldots\#\psi^{2m-1}(x)$. Combining equations (3) and (4) produces

$$x\#\psi(x)\#\ldots\#\psi^{2m-1}(x)\#\psi^{2m}(x) = x\#\psi(x)\#\ldots\#\psi^{2m-1}(x)\#\psi^m(x) \quad .$$

Cancelling, we get $\psi^{2m}(x) = \psi^m(x)$; so $\psi^m(x) = x$, since ψ is an injection..

For (B), note that since e occurs only once in $g(z)$, we may identify it with 1 (by Theorem 1.7); so $g(x) = \psi(x)\#\psi^2(x)\#\ldots\#\psi^{2m}(x)$. Applying ψ to equation (3) and combining the result with equation (4) produces

$$\psi(x)\#\psi^2(x)\#\ldots\#\psi^{2m}(x)\#\psi^{2m+1}(x) = \psi(x)\#\psi^2(x)\#\ldots\#\psi^{2m}(x)\#\psi^m(x) \quad .$$

Cancelling, we get $\psi^{2m+1}(x) = \psi^m(x)$; so $\psi^{m+1}(x) = x$.

For (C), replacing x by x^2 $(x * x)$ in equation (3) and combining the result with equation (4) produces

$$x^2\#\psi(x^2)\#\ldots\#\psi^{2m-1}(x^2)\#\psi^{2m}(x^2) = x^2\#\psi(x^2)\#\ldots\#\psi^{m-1}(x^2)\#\psi^m(x) \quad .$$

Cancelling yields

$$\psi^m(x^2)\#\psi^{m+1}(x^2)\#\ldots\#\psi^{2m}(x^2) = \psi^m(x) \quad ;$$

so

$$x^2\#\psi(x^2)\#\ldots\#\psi^m(x^2) = x \quad .$$

Since x^2 $(x * x)$ is $x\#\psi(x)$, we have

$$x^2\#\psi(x^2)\#\ldots\#\psi^{m-1}(x^2)\#\psi^m(x)\#\psi^{m+1}(x) = x \quad .$$

So by (4) $\psi^{m+1}(x) = x$.

For (D), applying ψ^m to each side of equation (4) and combining the result with equation (3) produces

$$x\#\psi(x)\#\ldots\#\psi^m(x)\#\psi^{m+1}(x)\#\psi^{m+2}(x)\#\ldots\#\psi^{2m}(x) =$$
$$\psi^m(x)\#\psi^{m+1}(x)\#\ldots\#\psi^{2m}(x)\#\psi^{m+1}(x)\#\psi^{m+2}(x)\#\ldots\#\psi^{2m}(x) \quad .$$

Cancelling gives us

$$x\#\psi(x)\#\ldots\#\psi^m(x) = \psi^m(x)\#\psi^{m+1}(x)\#\ldots\#\psi^{2m}(x) \quad . \tag{a}$$

Then combining equations (3) and (4) and cancelling from the left yields

$$\psi^{m+1}(x)\#\psi^{m+2}(x)\#\ldots\#\psi^{2m}(x) = \psi(x)\#\psi^2(x)\#\ldots\#\psi^m(x) \quad .$$

So

$$\psi^m(x)\#\psi^{m+1}(x)\#\ldots\#\psi^{2m-1}(x) = x\#\psi(x)\#\ldots\#\psi^{m-1}(x) \quad . \tag{b}$$

Substituting (b) into (a) we have

$$x\#\psi(x)\#\ldots\#\psi^m(x) = x\#\psi(x)\#\ldots\#\psi^{m-1}(x)\#\psi^{2m}(x) \quad .$$

Hence $\psi^m(x) = \psi^{2m}(x)$, or $x = \psi^m(x)$. ∎

By Theorem 1.8, we may insert e on the right in (A), (C), and (D) to get that $g(z) = z^{2m} * e$, $g(z) = (z^2)^m * e$, and $g(z) = (z^{m+1} * z^{m-1}) * e$ all work. The proof of Theorem 1.8 also shows that $g(z) = f_{2m}(z, e)$, $g(z) = f_m(z^2, e)$, and $g(z) = z^{m+1} * (z^{m-1} * e)$ and $g(z) = (z^{m+1} * e) * z^{m-1}$ all work. In (C) and (D), we cannot insert an e on the left, since in exponent 5, $g(z) = e * (zz)(zz)$ and $e * (zzz)z$ do not work (see Theorem 4.3).

Some more complex $g(z)$, with multiple occurrences of e, can be proved to work by the following theorem.

3.3. Theorem. Suppose $2m = kl$. Consider the following two $g(z)$:

I. $g(z) = z^k * f_{k-1}(e, z^k) * f_{(k-1)2}(e, z^k) * \ldots * f_{(k-1)(l-1)}(e, z^k)$.

II. $g(z) = (e * z^k) * f_{k-1}(e, e * z^k) * f_{(k-1)2}(e, e * z^k) * \ldots * f_{(k-1)(l-1)}(e, e * z^k)$.

For each of these $g(z)$, *if* the cycle axioms with this $g(z)$ imply that $e = 1$, then $g(z)$ works.

Proof. If we can replace e by 1, then expressing $g(z)$ in terms of ψ,we see that in case (I), the expression is the same as in case (A) of 3.1, and in case (II), the expression is the same as in case (B) of 3.1. ∎

3.4. Corollary.

I. $g(z) = z^m * f_{m-1}(e, z^m)$ works iff n is not divisible by 3.

II. $g(z) = (e * z^m) * f_{m-1}(e, e * z^m)$ works.

Proof. By the theorem, $g(z)$ works if the cycle axiom implies that $e = 1$. For (I): Since $g(1) = 1$ and $1^m = 1$, we have $1 * f_{m-1}(e, 1) = 1 = 1 * 1$. By cancellation, $f_{m-1}(e, 1) = 1$. We always have $f_n(e, 1) = 1$ (Theorem 1.5(f)). If n is not divisible by 3, then n and $m - 1$ are relatively prime; so $e = f_1(e, 1) = 1$ (apply Lemma 3.2, with $a = 1$ and $\Phi(x) = e * x$). For (II): Since $g(1) = 1$ and $1^m = 1$, we have $e * f_{m-1}(e, e) = 1$. That is, $f_{m+1}(e, 1) = 1$. Since $f_n(e, 1) = 1$ and $n, m + 1$ are always relatively prime, we have $e = f_1(e, 1) = 1$.

For the converse of (I): If n is divisible by 3, then so is $m - 1$. If we interpret e as the integer $n/3$, then $(\mathbb{Z}_n, +)$ is a model for the axiom in which $+$ is a group operation of exponent n, and e is an element different from 1 (i.e., 0 in this additive group). ∎

We now make some more specific comments on our use of OTTER. The results of this paper were obtained by a combination of mathematics and hacking. In an attempt to prove that the single axioms of McCune and Wos [6] extend to arbitrary odd exponents, we expressed the axioms abstractly in terms of our functions f and g. Then, the "cycle" idea enabled us to consider whole families of these axioms at once.

We used OTTER to derive as much as we could for an arbitrary $g(z)$. This helped us in two ways. First, we built up a whole *library* of general facts, which we kept in a file for use later when we considered a specific $g(z)$. The library facts were expressed using the function symbol $g(z)$, together with the symbol $k(x, y)$ to denote $f_{m-1}(x, y)$. Second, it enabled us to see that in order to prove that a specific $g(z)$ works, it is sufficient to derive $1 * x = x$ (see Theorem 1.5 and following discussion).

Now, we consider in more detail the specific $g(z) = z^{m+1} * z^{m-1}$ in Theorem 3.1 (D), since that was the hardest for us to verify. This $g(z)$ cannot be expressed in terms of k, but can be expressed as $(z * z * j(z, z)) * j(z, z)$, where $j(x, y)$ denotes $f_{m-2}(x, y)$. We can thus rewrite (demodulate) all the library facts to be in terms of j, using $k(x, y) = x * j(x, y)$. For readability, we used the symbol e for the right identity (1) of Theorem 1.5; this will not cause any confusion because the $g(z)$ under consideration does not use e. Our goal is then to prove $e * x = x$, which we input negated as $e * a \neq a$.

At first, we were not successful at getting OTTER to find a proof, although we were able to get proofs for the specific cases of exponents 5, 7, 9, and 11, which convinced us that the general form probably did work. We then looked more closely at the exponent 11 proof to see which library facts were likely to be relevant. We also took some key steps in this proof, re-expressed them in terms of j, and weighted them low in the input file for a general odd exponent, to encourage OTTER to make use of them in the general proof. This resulted in the following successful source file:

```
op(400, xfy, *).
assign(demod_limit, 1000).        assign(max_mem, 20000).
set(ur_res).  set(para_into_units_only).    set(para_from_units_only).
set(para_into).    set(para_from).
set(order_eq).    set(dynamic_demod).    set(back_demod).
assign(pick_given_ratio, 3).        assign(max_distinct_vars, 5).
assign(max_weight, 40).         assign(reduce_weight_limit, 8035).
list(usable).
   (x = x).
   % left and right cancellation for * :
      x * y != u   |   x * z != u   |   y = z.
      y * x != u   |   z * x != u   |   y = z.
   % left cancellation only, for j :
      j(x,y) != u | j(x,z) != u | y = z.
   -p.    % kludge -- more hands-on control than with process_input
end_of_list.
list(passive).
   % Negation of theorem:  e * x = x:
      e * a != a.
end_of_list.
```

```
list(sos).
   % some cycle axioms, in terms of k,g:
      p|x*k(x,(x*k(x,(x*y)*z))*g(z))=y.
      p| (x*k(x,(x*k(x,x*y))*z))*g(z)=y.
      p|x*k(x,x* (x*k(x,y*z))*g(z))=y.
   % Some other useful facts.
      x*e=x.
      (x*y)*e*z=x*y*z.
      p | g(x)*k(e,x)=e.
      p | x*e*k(e,g(x))=e.
      p | x*k(x,k(x,x*x))=e.
      j(y,y)*j(e,z)=y*j(y,z).
end_of_list.
list(demodulators).
   % k and g in terms of j:
      k(x,y) = x*j(x,y).
      g(z) =  (z*z*j(z,z))*j(z,z).
   % cancellation as a demod:
      (x * y = x * z) = (y = z).
      (y * x = z * x) = (y = z).
   % some other equations
   % which seem to be likely demodulators:
      (x*y)*e*z=x*y*z.
      x*e=x.
      x*j(x,e) = j(x,x).
      j(x,x*y) = x * j(x,y).
end_of_list.
% Some key equations for the exponent 11 proof:
weight_list(pick_given).
   weight((e*e*e*j(e,x))* (x*x*j(x,x))*j(x,x)=e,0).
   weight(x*x*j(x,(x*x*j(x,x))*y)=e*e*e*j(e,y),0).
   weight(e*e*e*j(e,x*j(x,x))=x*j(x,x),0).
   weight(e*e*j(e,z*z*j(z,(z*z*j(z,z))*y))=y,0).
   weight(e*e*e*j(e,x)=x,0).
   weight(x*x*j(x,(x*x*j(x,x))*y)=y,0).
   weight(e*e*j(e,y)=y,0).
end_of_list.
```

A remark on our use of the proposition letter p: We had input a number of general facts using the symbols g and k, as explained above. We wanted OTTER to demodulate them in terms of j. The standard way to accomplish this is to set the switch `process_input`. However, this switch causes everything in the input to be processed with all the demodulators, which, we found, frequently led to a much longer proof or to no proof at all. Instead, we input equations in g and k in the form $p \vee (\alpha = \beta)$, and then added the axiom $\neg p$.

Then, when resolution created ($\alpha = \beta$), this particular equation got demodulated. In this way, we could control exactly which equations got processed by the demodulators.

This input generated the following OTTER proof, which has been re-formatted slightly for readability:

```
----- OTTER 2.2xa+, January 1992 -----
----> UNIT CONFLICT at  45.71 sec ----> 1696 [binary,1694,6] $F.
Length of proof is 27.
---------------- PROOF ----------------
1 [] x=x.
2 [] x*y!=u|x*z!=u|y=z.
3 [] y*x!=u|z*x!=u|y=z.
5 [] -p.
6 [] e*a!=a.
7 [] p|x*k(x,(x*k(x,(x*y)*z))*g(z))=y.
8 [] p| (x*k(x,(x*k(x,x*y))*z))*g(z)=y.
10 [] x*e=x.
11 [] (x*y)*e*z=x*y*z.
12 [] p|g(x)*k(e,x)=e.
15 [] j(y,y)*j(e,z)=y*j(y,z).
16 [] k(x,y)=x*j(x,y).
17 [] g(z)= (z*z*j(z,z))*j(z,z).
18 [] (x*y=x*z)= (y=z).
20 [] (x*y)*e*z=x*y*z.
21 [] x*e=x.
22 [] x*j(x,e)=j(x,x).
23 [] j(x,x*y)=x*j(x,y).
24 [ur,7,5,demod,16,17,16]
   x*x*j(x,(x*x*j(x,(x*y)*z))* (z*z*j(z,z))*j(z,z))=y.
26 [ur,12,5,demod,17,16,20] (x*x*j(x,x))*j(x,x)*j(e,x)=e.
30 [ur,8,5,demod,16,23,16,17]
   (x*x*j(x,(x*x*x*j(x,y))*z))* (z*z*j(z,z))*j(z,z)=y.
34 [para_into,11,11,demod,20] (x*y)* (e*z)*u=x* (y*z)*u.
36,35 [ur,15,3,1] j(e,e)=e.
45 [para_into,26,15] (x*x*j(x,x))*x*j(x,x)=e.
47 [para_from,26,11] (y*y*j(y,y))* (j(y,y)*j(e,y))*x=e*e*x.
57 [para_into,24,10,demod,23,36,21,21,36,21,21,23,23,23]
   x*x*x*x*x*x*j(x,j(x,y))=y.
90 [para_into,34,45,demod,21] (x*y)* (e*y*j(y,y))*y*j(y,y)=x.
213 [para_into,57,15] x*x*x*x*x*j(x,x)*j(e,j(x,y))=y.
246 [para_into,30,35,demod,21,21,21,23]
   (e*e*e*j(e,x))* (x*x*j(x,x))*j(x,x)=e.
259 [ur,246,3,30,demod,22] x*x*j(x,(x*x*j(x,x))*y)=e*e*e*j(e,y).
279,278 [para_into,259,45,demod,22] e*e*e*j(e,x*j(x,x))=x*j(x,x).
415 [ur,90,3,1] (x* (e*y*j(y,y))*y*j(y,y))*y=x.
```

```
483 [para_into,47,278,demod,20]
   (x*x*j(x,x))*j(x,x)*j(e,x)*e*j(e,y*j(y,y))=e*y*j(y,y).
490,489 [para_into,47,278,demod,20]
   (x*x*j(x,x))*j(x,x)*j(e,x)*j(e,y*j(y,y))=y*j(y,y).
658 [ur,213,2,1,demod,23] y*y*y*j(y,y)*j(e,y*j(y,x))=x.
768 [ur,658,2,10] x*x*j(x,x)*j(e,x*j(x,x))=e.
770 [ur,658,2,1,demod,23] y*y*j(y,y)*j(e,y*y*j(y,x))=x.
883 [ur,770,2,1,demod,23] y*j(y,y)*j(e,y*y*y*j(y,x))=x.
1132,1131 [ur,883,2,278,demod,36,279,18]
   e*j(e,x*j(x,x))=j(e,x*j(x,x)).
1152,1151 [back_demod,483,demod,1132,490] e*y*j(y,y)=y*j(y,y).
1159,1158 [back_demod,278,demod,1132,1132,1132] j(e,x*j(x,x))=x*j(x,x).
1201 [back_demod,415,demod,1152] (x* (y*j(y,y))*y*j(y,y))*y=x.
1292 [back_demod,768,demod,1159] x*x*j(x,x)*x*j(x,x)=e.
1575 [para_into,1292,11,demod,1152] x* (x*j(x,x))*x*j(x,x)=e.
1694 [para_into,1201,1575] e*x=x.
1696 [binary,1694,6] $F.
------------ end of proof -------------
```

We now decided that a proof in terms of the group operation # might be easier to read, since we could then use associativity of # to drop all parentheses in products. Doing this translation, we saw that many of the lines in the proof simply restated Theorem 2.2 or easy consequences thereof. These lines expressed facts true of an arbitrary $g(z)$. The remaining lines, which were specific to the particular $g(z)$, were simple enough in translation that we could see the key steps emerge for the proof given above for Theorem 3.1 (D).

As an example of a line whose translation restated Theorem 2.2, consider line 883:

$$y * j(y,y) * j(e, y * y * y * j(y,x)) = x.$$

Since $j(x,y) = f_{m-2}(x,y)$, we can rewrite it successively as:

$$\begin{aligned}
y * f_{m-2}(y,y) * f_{m-2}(e, y * y * y * f_{m-2}(y,x)) &= x.\\
y * f_{m-2}(y,y) * f_{m-2}(e, f_{m+1}(y,x)) &= x.\\
y \; * \; (y\#\psi(y)\#\ldots\#\psi^{m-2}(y)) \; * \; \psi^{m-2}(y\#\psi(y)\#\ldots\#\psi^{m}(y)\#\psi^{m+1}(x)) &= x.\\
y \;\#\; \psi(y\#\psi(y)\#\ldots\#\psi^{m-2}(y)) \;\#\; \psi^{m}(y\#\psi(y)\#\ldots\#\psi^{m}(y)\#\psi^{m+1}(x)) &= x.\\
y \;\#\; \psi(y)\#\psi^2(y)\#\ldots\#\psi^{m-1}(y) \;\#\; \psi^{m}(y)\#\psi^{m+1}(y)\#\ldots\#\psi^{2m}(y)\#\psi^{2m+1}(x) &= x.\\
y\#\psi(y)\#\ldots\#\psi^{2m}(y)\#\psi^{2m+1}(x) &= x.
\end{aligned}$$

Since $n = 2m+1$, this last equation is immediate from equations (3) and (5) of §2.

As an example of an equation which seemed to be an important consequence for this particular $g(z)$, consider line 279. Translating this, we get, successively:

$$\begin{aligned}
e * e * e * j(e, x * j(x,x)) &= x * j(x,x).\\
e * e * e * f_{m-2}(e, x * j(x,x)) &= x * j(x,x).\\
f_{m+1}(e, x * j(x,x)) &= x * j(x,x).\\
\psi^{m+1}(x * j(x,x)) &= x * j(x,x).\\
\psi^{m+1}(\alpha) = \alpha \quad ; \quad \alpha &= x\#\psi(x)\#\ldots\#\psi^{m-1}(x).
\end{aligned}$$

So, it seemed to us here that a key step in the proof was to establish that $\psi^{m+1}(\alpha) = \alpha$, or, equivalently, $\psi^m(\alpha) = \alpha$ (since ψ^{2m+1} is the identity). By considerations of this sort, we were led to our proof of Theorem 3.1 (D), where $\psi^m(\alpha) = \alpha$ is equation (b).

§**4. Some $g(z)$ which do not work.** If $g(z)$ fails to work, then, by the results of §2, $g(z)$ may always be refuted by a group model. In many cases, that model may be taken to be a ring model, as in [2,3], where the group is the additive group of a ring. We may find the appropriate ring by studying polynomials, as we describe below.

Definition. If $g(z)$ is a term in $*$, z, and zero or more occurrences of e, the *associated polynomial* for $g(z)$ is the polynomial $Q(k)$ (over $\mathbb{Z}$) obtained by replacing e by 0 and $u * v$ by $u + kv$ in $g(z)$, and reducing the result to $Q(k) \cdot z$.

For example, if $g(z)$ is $e(zz)(zz)$, then, doing the replacement, we get

$$0 + k[(z + kz) + k(z + kz)] = (k^3 + 2k^2 + k)z \quad ,$$

so $Q(k)$ is $k^3 + 2k^2 + k$.

4.1. Lemma. Suppose that $n = 2m + 1$, $g(z)$ is a term in $*$ having exactly $2m$ occurrences of z and zero or more occurrences of e, and $Q(k)$ is the associated polynomial for $g(z)$. Suppose that there is a commutative ring with 1 and a $k \neq 1$ in the ring satisfying the equations $R(k) = S(k) = 0$, where

$$R(k) = 1 + k + k^2 + \cdots k^{2m}$$
$$S(k) = Q(k) + k^m.$$

Then there is a model for the axioms of cycle $G.n$ in which $*$ is not a group operation.

Proof. Multiplying each side of the equation $R(k) = 0$ by $k - 1$ yields $k^n = 1$; so k is a unit of the ring (i.e., has a multiplicative inverse, k^{2m}). So if we let $\psi(x) = kx$, ψ is an automorphism of the additive group of the ring. The result now follows by Theorem 2.2 and the remark preceding Theorem 2.1. ■

The following lemma gives a very simple sufficient condition for the existence of a ring satisfying 4.1.

4.2. Lemma. With the same notation as 4.1, assume that $\gcd(n, S'(1)) > 1$, where S' is the derivative of S. Then there is a model for the axioms of cycle $G.n$ in which $*$ is not a group operation.

Proof. Let p be a prime divisor of n and $S'(1)$, and let $\mathcal{R}$ be the ring of polynomials in one variable, U, over $\mathbb{Z}_p$. Since $Q(k)$ has one term for each occurrence of z in $g(z)$, $R(1) = S(1) = n = 0$ in $\mathbb{Z}_p$. Also, $R'(1) = 1 + 2 + \cdots + 2m = mn$, so $R'(1) = S'(1) = 0$. Thus, $(U - 1)^2$ divides both $R(U)$ and $S(U)$ in $\mathcal{R}$. Let $\mathcal{I}$ be the ideal in $\mathcal{R}$ generated by the polynomial $(U-1)^2$. Then the equations $R(k) = S(k) = 0$ have a solution, $k = U \neq 1$, in the quotient ring $\mathcal{R}/\mathcal{I}$. ■

4.3. Theorem. For exponent 5, none of the following $g(z)$ work:

$$((zz)z)z \qquad z(zz)z \qquad e(zz)(zz) \qquad e(zzz)z \quad .$$

Proof. The four associated polynomials are, respectively,

$$3k+1 \qquad 2k^2+k+1 \qquad k^3+2k^2+k \qquad k^3+2k^2+k \quad .$$

Adding k^2 to get $S(k)$, we see that for all but the second of these, 5 divides $S'(1)$, so we may apply Lemma 4.2. For the second one, we apply Lemma 4.1. We have the equations:

$$k^4+k^3+k^2+k+1 = 3k^2+k+1 = 0 \quad .$$

By $k^5 = 1$, it is natural to look for a solution in a $\mathbb{Z}_p$ with $p-1$ divisible by 5, and we quickly find $k=9$ over $\mathbb{Z}_{11}$. ∎

By the results in §3, we now have analyzed the five associative variants of z^4: $zzzz$, $(zz)(zz)$, and $(zzz)z$, do work, but $((zz)z)z$ and $z(zz)z$ do not. The failure of $e(zz)(zz)$ and $e(zzz)z$ shows that inserting an e before a $g(z)$ which does work may yield one which does not, so that the proof in §3, that $g(z) = e * z^{2m}$ does work, really needed something special about this particular association.

Life is not always so easy, however. Consider the exponent 7 case. Now $g(z) = (zzzz)(zz)$ does work, as we showed in §3, but, we *conjecture* that $g(z) = (zzz)(zzz)$ does not. However, they both have the same associated polynomial, $1+2k+2k^2+k^3$, so it is clear that we cannot refute $(zzz)(zzz)$ by a ring model as in Lemma 4.1. Turning back to groups, we look at the two conditions of Theorem 2.2. The first is, for both $g(z)$,

$$x\#\psi(x)\#\psi^2(x)\#\psi^3(x)\#\psi^4(x)\#\psi^5(x)\#\psi^6(x) = 1 \quad .$$

The second, for $g(z) = (zzzz)(zz)$, is

$$x\#\psi(x)\#\psi^2(x)\#\psi^3(x)\#\psi(x)\#\psi^2(x)\#\psi^3(x) = 1 \quad ,$$

which, as we saw, forced ψ to be the identity, whereas the second, for $g(z) = (zzz)(zzz)$, is

$$x\#\psi(x)\#\psi^2(x)\#\psi(x)\#\psi^2(x)\#\psi^3(x)\#\psi^3(x) = 1 \quad ,$$

which is different if the group is not Abelian.

§**5. Some general limitations.** We prove some results limiting the form of single axioms for varieties of groups in general.

First, no equational variety can be axiomatized by a single equation in product, inverse, and identity. For the variety of all groups, this was pointed out, without proof, by Tarski [8], and a proof was given by Neumann [7]; we simply generalize Neumann's proof here. Of course, we have to omit the trivial variety, consisting of the one element group, which is axiomatized by $(x = y)$.

5.1 Theorem. If $\mathcal{G} = (G; *_\mathcal{G}, i_\mathcal{G}, e_\mathcal{G})$ is any group with more than one element and $(\alpha = y)$ is valid in $\mathcal{G}$, then there is a finite non-group $\mathcal{H} = (H; *_\mathcal{H}, i_\mathcal{H}, e_\mathcal{H})$ such that $(\alpha = y)$ is valid in $\mathcal{H}$.

Note that by $\mathcal{H}$ being a non-group, we mean that it is not the case that $*_{\mathcal{H}}$ is a group operation in which $i_{\mathcal{H}}$ is the inverse operation and $e_{\mathcal{H}}$ is the identity. For example, the following is a minor variant of a single axiom of McCune (see §5 of [2] for a discussion):

$$\big(i(e*z)*x\big) \ * \ i\big(i(e*(z*y))*x\big) = y \quad .$$

If this equation is valid in $\mathcal{H}$, then $*_{\mathcal{H}}$ must be a group operation and $i_{\mathcal{H}}$ must be the group inverse operation; but $e_{\mathcal{H}}$ need not be the group identity. So, this is not a counterexample to Theorem 5.1.

The second result shows that no variety of groups can be axiomatized by any *set* of equations with only two variables. For the variety of all groups, this was shown in [2], but the argument there does not easily generalize to arbitrary varieties. This result is used to limit the candidates for single axioms for groups or varieties of groups; see §6 and [2,3]. Again, the trivial variety, consisting of the one element group, is an exception.

5.2 Theorem. If $\mathcal{G} = (G; *_{\mathcal{G}}, i_{\mathcal{G}}, e_{\mathcal{G}})$ is any group with more than one element, then there is a finite structure $\mathcal{H} = (H; *_{\mathcal{H}}, i_{\mathcal{H}}, e_{\mathcal{H}})$, such that the associative law fails in $\mathcal{H}$ but $\mathcal{H}$ satisfies every equation $(\alpha = \beta)$ such that $(\alpha = \beta)$ contains two or fewer variables and is valid in $\mathcal{G}$.

Let us first reduce the $\mathcal{G}$ in both theorems to an Abelian p-group. Let $\mathbb{Z}_p$ denote the additive group of the integers modulo p. $(\mathbb{Z}_p)^n$ denotes the direct product (or direct sum) of n copies of $\mathbb{Z}_p$.

5.3 Lemma. If $\mathcal{G}$ is any group with more than one element, then there is a prime p such that every equation $(\alpha = \beta)$ valid in $\mathcal{G}$ is valid in $(\mathbb{Z}_p)^n$ for all $n \geq 1$.

Proof. Note that the validity of equations is preserved under products and substructures. Since $\mathbb{Z}_p$ is both a factor and a substructure of $(\mathbb{Z}_p)^n$, both structures satisfy the same equations. Thus, the Lemma holds for $\mathcal{G}$ if $\mathcal{G}$ contains a subgroup isomorphic to $\mathbb{Z}_p$ for some prime p. If not, then $\mathcal{G}$ contains a subgroup isomorphic to $\mathbb{Z}$. Since equations are also preserved under homomorphic images, the conclusion of the Lemma will hold for every p. ∎

Proof of 5.1. By Lemma 5.3, it is sufficient to prove this in the case that $\mathcal{G}$ is $\mathbb{Z}_p$ for some prime p. Then for $\mathcal{H}$, the domain of discourse, H, will be the set $\mathbb{Z}_p$, but $(*_{\mathcal{H}}, i_{\mathcal{H}}, e_{\mathcal{H}})$ will be defined by:

$$x *_{\mathcal{H}} y = x + y + a$$
$$i_{\mathcal{H}}(x) = -x + b$$
$$e_{\mathcal{H}} = c \quad ,$$

where a, b, c are some constants in $\mathbb{Z}_p$. Since $(\alpha = \beta)$ is valid in $\mathbb{Z}_p$, if we replace $(*_{\mathcal{H}}, i_{\mathcal{H}}, e_{\mathcal{H}})$ in $(\alpha = \beta)$ by their definitions, we find $n, m, r \in \mathbb{Z}_p$ such that the linear equation

$$ma + nb + rc = 0$$

is equivalent to the validity of $(\alpha = \beta)$ in $\mathcal{H}$. We need to show that there is some solution to this equation which makes the resultant $\mathcal{H}$ fail to be a group. If $m \neq 0$, let $b = 1$, $c = 0$, and $a = -n/m$; then $\mathcal{H}$ will not satisfy the equation $i(e) = e$, which is true in all groups.

If $m = 0$, let $b = c = 0$ and $a = 1$; then $\mathcal{H}$ will not satisfy the equation $e * e = e$, which is true in all groups. ■

For Theorem 5.2, likewise, it is enough to consider a $\mathbb{Z}_p$. For the case $p = 2$, a 10-element model was constructed in [2] using a Steiner triple system with 9 points (an $S(2;3,9)$ – see, e.g., [1] for notation). For an arbitrary prime p, that proof generalizes to produce a model of size $(p-1)k+1$ from an $S(2;p+1,k)$. However, the following direct proof avoids the use of Steiner systems.

Proof of 5.2. Let F be a field and H a vector space over F. We show how to modify the additive group of H to satisfy the Theorem.

If P is a two dimensional subspace of H, let us call a *radial* map of P any bijection φ from P onto P such that for every one dimensional subspace L of P, there is a non-zero scalar $c \in F$ (depending on L) such that $\varphi(\vec{x}) = c\vec{x}$ for all $\vec{x} \in L$. So, in the plane P, we are just stretching each radial line by a (possibly) different amount. We assume *no* relationship between the c for one line and the c for another line.

Now, choose, for each two dimensional subspace P, some radial map φ_P of P. For each $\vec{x}, \vec{y} \in H$, define $\vec{x} * \vec{y} = \varphi_P^{-1}(\varphi_P(\vec{x}) + \varphi_P(\vec{y}))$ where P is some (*any*) two dimensional subspace containing $\vec{x}, \vec{y}$. This definition of $*$ is unambiguous, because P is unique unless $\vec{x}, \vec{y}$ are linearly dependent, in which case $\vec{x} * \vec{y}$ reduces to $\vec{x} + \vec{y}$ for any P chosen. We interpret inverse as the old inverse operation in H: $i(\vec{x}) = -\vec{x} = \varphi_P^{-1}(-(\varphi_P(\vec{x})))$, and we interpret identity as $\vec{0}$.

This defines the structure $\mathcal{H} = (H; *_{\mathcal{H}}, i_{\mathcal{H}}, e_{\mathcal{H}})$. Observe that for each two dimensional subspace P of the vector space H, the new structure $(*_{\mathcal{H}}, i_{\mathcal{H}}, e_{\mathcal{H}})$ on P is isomorphic to the old additive group structure on P via the bijection φ_P. Thus, our new $\mathcal{H}$ satisfies all the two variable equations valid in the additive group of F^2. If F has characteristic p, these are the same as the two variable equations valid in $\mathbb{Z}_p$.

In view of Lemma 5.3, we are now done if we can show how to choose the φ_P to make associativity fail. We assume here that the vector space H has dimension at least three and that F has more than two elements; so, F can be $\mathbb{Z}_p$ unless $p = 2$, in which case we take F to be some Galois field extending $\mathbb{Z}_2$. F cannot be $\mathbb{Z}_2$ because that would force every radial map to be the identity.

For any linearly independent $\vec{x}, \vec{y} \in H$, let $p(\vec{x}, \vec{y})$ be the two dimensional subspace spanned by $\vec{x}, \vec{y}$. Fix linearly independent $\vec{x}, \vec{y}, \vec{z}$. Fix any $c \in F$ with c different from 0 and 1. Let, for all $\vec{v}$ in the appropriate subspace

$$\begin{aligned}
\varphi_{p(\vec{y},\vec{z})}(\vec{v}) &= \vec{v} \\
\varphi_{p(\vec{x},\vec{y}+\vec{z})}(\vec{v}) &= \vec{v} \\
\varphi_{p(\vec{x},\vec{y})}(\vec{v}) &= \vec{v} \\
\varphi_{p(\vec{x}+\vec{y},\vec{z})}(\vec{z}) &= c\vec{z} \\
\varphi_{p(\vec{x}+\vec{y},\vec{z})}(\vec{x}+\vec{y}) &= \vec{x}+\vec{y} \\
\varphi_{p(\vec{x}+\vec{y},\vec{z})}(\vec{x}+\vec{y}+c\vec{z}) &= \vec{x}+\vec{y}+c\vec{z}
\end{aligned}$$

Note that by linear independence, we are free to make this definition, since the four two dimensional subspaces, $p(\vec{y}, \vec{z})$, $p(\vec{x}, \vec{y}+\vec{z})$, $p(\vec{x}, \vec{y})$, $p(\vec{x}+\vec{y}, \vec{z})$, are all distinct, and within the subspace $p(\vec{x}+\vec{y},\vec{z})$, the three vectors, $\vec{z}$, $\vec{x}+\vec{y}$, $\vec{x}+\vec{y}+c\vec{z}$, lie on different one dimensional subspaces. Then $(\vec{x}*\vec{y})*\vec{z} = \vec{x}+\vec{y}+c\vec{z}$, whereas $\vec{x}*(\vec{y}*\vec{z}) = \vec{x}+\vec{y}+\vec{z}$, so associativity fails. ∎

Associativity is very strong. In the presence of associativity, *any* of the axioms in this paper imply the group axioms. For axioms of the form $x^n * y * z^n = y$, this was shown in [3] Lemma 3.1.

5.4 Theorem. Assume G satisfies associativity and $x^n * y * z^i * e * z^j = y$, where $n > 0$, and $i, j \geq 0$. Then G is a group of exponent n, and e is the identity.

Proof. By $x * (\ldots) = y$, G is left surjective, and by $\ldots(x * y)\ldots = y$, G is left injective (see Lemma 1.3). Setting $z = e$, we have $x^n * y * e^k = y$, where $k = i+j+1$. Since x is arbitrary, $x^n * y * e^k = y = x^{2n} * y * e^k$, so by left injectivity, $y * e^k = x^n * y * e^k = y$. Let $1 = e^k$. Then 1 is a right identity. Right inverse ($\forall x \exists y(xy = 1)$) follows from left surjectivity. Then, setting $x = y = z = 1$ shows that $e = 1$, and setting $y = z = 1$ in the original axiom shows that the group has exponent n. ∎

This last result is less helpful than one might think in practical verification. It is true that to verify $(\alpha = y)$ as a single axiom, it now suffices to insert $(\alpha = y)$ in the `sos` and $a*(b*c) \neq (a*b)*c$ in the `usable` or `passive` list, and let OTTER run; it is not necessary to verify the other group axioms. However, in practice, all the other group axioms get derived quickly anyway *if* associativity appears, and for the harder cases ([3], or §3, or §6), the verification does not succeed unless some other group fact, such as $e * e = e$, is proved first.

Finally, we justify our restriction to associative variants of $x^n y z^n = y$ when considering short single axioms for exponent n groups. For even n, this was done in [3], and now Theorem 5.2 allows us to extend the result for all n. Recall that $V(\alpha)$ is the number of variable occurrences in α.

5.5 Theorem. Suppose that $(\alpha = y)$ is a single axiom for groups of exponent $n > 1$, where α is a term constructed from $*$, variables, and zero or more occurrences of e. Then $V(\alpha) \geq 2n+1$. Furthermore, if $n > 2$ and $V(\alpha) = 2n+1$, then α must be some associative variant of $x^n y z^n$, with zero or more occurrences of e inserted, where x, z are variables distinct from y.

Proof. Since $(\alpha = y)$ is valid in the additive group $\mathbb{Z}_n$, $V(\alpha) = kn + 1$ for some k. Then, since $(\alpha = y)$ implies associativity, α must have at least three distinct variables by Theorem 5.2, so $k \geq 2$; and, furthermore, if $k = 2$, then α must have 1 occurrence of y, and n occurrences each of x, z, where x, z are variables distinct from y. The fact that α is of the claimed form now follows directly from the fact (see, e.g., Lemma 2.2 of [3]) that if $n > 2$ and $0 < i < n$, there is a group of exponent n in which the equation $(x^i y x^{n-i} = y)$ is not valid.

§**6. Other odd exponent axioms.** There are single axioms for odd exponent groups which are not part of cycle $G.n$ at all. For example,

$$(x * x) * ((x * x) * (x * y) * z) * (z * z) * (z * z) = y$$

is a single axiom for groups of exponent 5. This is easily verified on OTTER; in fact, in Version 3.0, set to autonomous mode, if the input consists of this equation and the denial of associativity, then OTTER will set its own switches correctly and quickly find a proof.

This axiom does not seem to be related to the axioms of our cycle $G.5$. Its cycle length is 5, whereas $G.5$ has length 7. Presumably, this too is part of a pattern which extends to other odd exponents, but we have not traced it out.

It is true that in exponent 3 without identity, our cycle $G.3$ yields the only short single axioms. Of course, there is also its mirror, obtained by replacing all $u * v$ by $v * u$. The only possible $g(z)$ here is zz.

6.1. Theorem. Suppose $(\alpha = y)$ is a single axiom for groups of exponent 3, where α is an associative variant of x^3yz^3. Then $(\alpha = y)$ or its mirror is a member of the cycle $G.3$.

Proof. By exhaustive search, as in [3], although the search is a little shorter here. There are only 132 associative variants of x^3yz^3, and it is easy to write a simple Prolog program which generates all of them and eliminates those which are refuted by some simple ring models. In these models, the domain of discourse is some $\mathbb{Z}_r$, and we interpret $x*y$ as $hx + ky$ for some $h, k \in \mathbb{Z}_r$, where h, k are not both equal to 1. All but 40 candidates are eliminated by taking r among $3, 5, 7, 9$. Next, we can eliminate all α such that $(\alpha = y)$ is provable from all two variable facts true in $\mathbb{Z}_3$, since by Theorem 5.2, there is a non-group model for those facts. In exponent 3, this removal is easily accomplished by deleting all terms which contain a subterm of the form $x(xx)$, $(xx)x$, $z(zz)$, or $(zz)z$. After this, only 10 remain; namely, the members of $G.3$ and their mirrors. ∎

§**7. Conclusion.** The use of OTTER to discover new mathematical results is by now standard. We have shown here that by examining OTTER's output, one can construct proofs which a human can understand too. In fact, all the major results in this paper were written in the usual style of theorems and proofs in mathematics.

On the specific subject of single axioms for odd exponent groups, we have produced a large number of such axioms, but are still far from a general description of all of them. We still do not know a decision procedure to test whether a specific equation is a single axiom. We know that our general cycle does not include all such axioms, and even within our cycle we have left two different problems open. First, we do not have a refutation for the cycle members $G.n.m+1$ and $G.n.2m+3$. Second, for the other cycle members, which are all equivalent, we lack a decision procedure for which $g(z)$ work.

Even for the specific $g(z) = (zzz)(zzz)$, we are unable to prove it works or produce a countermodel, although we have reduced the existence of such a model to the existence of a group with a particular kind of automorphism. It is easy to see, by applying the Sylow theorems, that such a model must have size at least 56, so that it would have to be produced by group theoretic techniques, rather than by the model generation techniques from automated reasoning.

References

[1] Beth, T., Jungnickel, D., and Lenz, H., *Design Theory*, Bibliographisches Institut, 1985.

[2] Kunen, K., Single Axioms for Groups, *J. Automated Reasoning*, 9:291 – 308, 1992.

[3] Kunen, K., The Shortest Single Axioms for Groups of Exponent 4, Technical Report UW #1134, University of Wisconsin, 1993; to appear, Computers and Mathematics and Applications.

[4] McCune, W. W., OTTER 3.0 Reference Manual and Guide, Technical Report ANL-94/6, Argonne National Laboratory, 1994.

[5] McCune, W. W., Single Axioms for Groups and Abelian Groups with Various Operations, *J. Automated Reasoning*, 10:1 – 13, 1993.

[6] McCune, W. W. and Wos, L., Applications of Automated Deduction to the Search for Single Axioms for Exponent Groups, in *Logic Programming and Automated Reasoning*, Springer-Verlag, 1992, pp. 131 – 136.

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

[8] 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.