PACIFIC JOURNAL OF MATHEMATICS
Vol. 59, No. 1, 1975

ENDOMORPHISM AND AUTOMORPHISM STRUCTURE OF DIRECT SQUARES OF UNIVERSAL ALGEBRAS

MATTHEW GOULD

Necessary and sufficient conditions are obtained for a given monoid to be representable as the endomorphism monoid of a universal algebra of the form $\mathfrak{A} \times \mathfrak{A}$. These conditions are utilized to prove that every group having an element of order two is representable as the automorphism group of such an algebra.

The *direct square* of a universal algebra $\mathfrak{A}$ is the direct product $\mathfrak{A} \times \mathfrak{A}$ of $\mathfrak{A}$ with itself. Subalgebra lattices of direct squares were characterized by Iskander in [6] and later by Grätzer and Lampe [5] in a simplified proof obviating the axiom of choice. The present note characterizes the endomorphism monoids and automorphism groups of direct squares. The main result (Theorem 2.2) is that the nontrivial automorphism groups of direct squares are (up to isomorphism) all groups containing an element of order two.

Concepts and notations of universal algebra used here and not explicitly defined are taken from Grätzer [4], while semigroup terminology comes from Clifford and Preston [2]. The endomorphism monoid of a universal algebra $\mathfrak{A}$ is denoted End$(\mathfrak{A})$ and its automorphism group Aut$(\mathfrak{A})$. Moreover, the following notations are used with regard to sets of the form $A \times A$.

Given an element x of $A \times A$ its left and right components will be denoted (unless context demands otherwise) x_0 and x_1 respectively. For n a positive integer a function f mapping $(A \times A)^n$ into $A \times A$ will be called a *square function* if there exists a function g, termed the square root of f (notation: $f = g^2$), such that g maps A^n into A and $f(x^0, \cdots, x^{n-1})_i = g(x_i^0, \cdots, x_i^{n-1})$ for all $x^0, \cdots, x^{n-1} \in A \times A$ and $i = 0, 1$. For $n = 0$, a nullary operation f is said to be square if its value x belongs to the diagonal, i.e., if $x_0 = x_1$.

Functions δ_0, δ_1, and τ, all mapping $A \times A$ into itself, are defined by stipulating that for all $x \in A \times A$, τ sends x to the pair $\langle x_1, x_0\rangle$ and δ_i sends x to $\langle x_i, x_i\rangle$.

Given functions α and β mapping $A \times A$ into itself, a third such function $\alpha * \beta$ is defined by setting $x(\alpha * \beta) = \langle (x\alpha)_0, (x\beta)_1\rangle$ for all $x \in A \times A$. Note that $\tau = \delta_1 * \delta_0$. Moreover, if α and β are endomorphisms of a direct square then so is $\alpha * \beta$. In the terminology of Chang, Jónsson, and Tarski [1] the operation $*$ is a decomposition function. For any universal algebra $\mathfrak{A}$ defined on A the system $\langle \mathrm{End}\,(\mathfrak{A} \times \mathfrak{A}); *\rangle$ is in the terminology of Plonka [7] a two-dimensional diagonal algebra, and is therefore isomorphic to a rectangular band (see [7]). If τ is regarded as acting on $\mathrm{End}\,(\mathfrak{A} \times \mathfrak{A})$ by right multiplication (composition), then the system $\langle \mathrm{End}\,(\mathfrak{A} \times \mathfrak{A}); *, \tau\rangle$ is, in the terminology of Fajtlowicz [3], a two-dimensional die.

A further word on notation: in systems having two binary operations of which one is denoted $*$, the other operation will be assumed to take precedence in formulas, e.g., $xy * xz$ means $(xy) * (xz)$.

1. Endomorphism monoids of direct squares.

The following lemma characterizes direct squares in terms of endomorphisms. (A different characterization of direct squares was given by Fajtlowicz [3].) The lemma seems to be well known, but its origin is unclear to the author, who first heard of it in a lecture given by Professor A. Pultr at the Mini-conference in Universal Algebra held at the University of Manitoba in February 1969.

LEMMA 1.1. *Let A be a nonvoid set and $\mathfrak{B}$ a universal algebra defined on $A \times A$. Then $\mathfrak{B}$ is a direct square if and only if δ_0 and δ_1 are endomorphisms of $\mathfrak{B}$.*

Proof. As the converse is evident, suppose $\mathrm{End}\,(\mathfrak{B})$ contains δ_0 and δ_1. Note that the diagonal, which consists of those elements of $A \times A$ on which these two endomorphisms agree, must be a subalgebra of $\mathfrak{B}$. It follows that every nullary operation of $\mathfrak{B}$ is square (since every subalgebra must contain the values of the nullary operations), so let f be an operation having positive rank n. For $i = 0, 1$ define functions $f_i\colon A^n \rightarrow A$ by setting $f_i(a_0, \cdots, a_{n-1}) = f(\langle a_0, a_0\rangle, \cdots, \langle a_{n-1}, a_{n-1}\rangle)_i$ for all $a_0, \cdots, a_{n-1} \in A$. Since the diagonal is a subalgebra, f_0 and f_1 are the same function, g. To see that g is the sequare root of f, let $x^0, \cdots, x^{n-1} \in A \times A$ and compute:

$$\begin{aligned} f(x^0, \cdots, x^{n-1})_i &= (f(x^0, \cdots, x^{n-1})\delta_i)_i = f(x^0\delta_i, \cdots, x^{n-1}\delta_i)_i \\ &= f(\langle x^0_i, x^0_i\rangle, \cdots, \langle x^{n-1}_i, x^{n-1}_i\rangle)_i \\ &= g(x^0_i, \cdots, x^{n-1}_i) \text{ for } i = 0, 1\,, \end{aligned}$$

whereupon the lemma is proved.

LEMMA 1.2. *For every universal algebra $\mathfrak{A}$, $\mathrm{End}\,(\mathfrak{A})$ is isomorphic to the centralizer of $\{\delta_0, \delta_1\}$ in $\mathrm{End}\,(\mathfrak{A} \times \mathfrak{A})$.*

Proof. Let C denote the centralizer of $\{\delta_0, \delta_1\}$ in $\mathrm{End}\,(\mathfrak{A} \times \mathfrak{A})$.

An embedding of $\operatorname{End}(\mathfrak{A})$ into C is given by the correspondence $\alpha \rightarrow \alpha^2$ for all $\alpha \in \operatorname{End}(\mathfrak{A})$. Regarding the members of C as unary operations and applying Lemma 1.1 to the algebra $\langle A \times A; C\rangle$, we see that C must consist of square functions, and it is clear that their square roots are endomorphisms of $\mathfrak{A}$. Thus the embedding is an isomorphism of $\operatorname{End}(\mathfrak{A})$ onto C.

The following theorem characterizes the endomorphism monoids of direct squares and will be instrumental in the characterization of the automorphism groups.

THEOREM 1.3. *A monoid M is isomorphic to the endomorphism monoid of a direct square if and only if there exist elements d_0, d_1 of M and a binary operation $*$ on M satisfying the identities*

(1.3.1) $$d_i d_j = d_i \quad \textit{for } i, j \in \{0, 1\}\ ;$$

(1.3.2) $$xd_0 * xd_1 = x \quad \textit{for all } x \in M\ ;$$

(1.3.3) $$(x * y)d_0 = xd_0 \textit{ and } (x * y)d_1 = yd_1 \quad \textit{for all } x, y \in M\ .$$

Moreover, given a monoid M satisfying these conditions, there exists a multi-unary algebra $\mathfrak{A}$ and an isomorphism φ of M onto $\operatorname{End}(\mathfrak{A} \times \mathfrak{A})$ *such that $d_i\varphi = \delta_i$ for $i \in \{0, 1\}$ and $(x * y)\varphi = x\varphi * y\varphi$ for all $x, y \in M$.*

Proof. For $M = \operatorname{End}(\mathfrak{A} \times \mathfrak{A})$, $d_i = \delta_i$, and $*$ as defined above, verification of the identities is routine.

Let $\langle M; *, d_0, d_1\rangle$ be given satisfying (1.3.1)-(1.3.3). As (1.3.1) implies $Md_0 = Md_1$, set $A = Md_0 = Md_1$. Then (1.3.3) implies $A \times A = \{\langle md_0, md_1\rangle \mid m \in M\}$, and it follows from (1.3.2) that the map $m \rightarrow \langle md_0, md_1\rangle$ gives a bijection of M onto $A \times A$. Hence a monoid isomorphic to M is defined on $A \times A$ by the multiplication

$$\langle md_0, md_1\rangle\langle nd_0, nd_1\rangle = \langle mnd_0, mnd_1\rangle\ .$$

Consider now the multi-unary algebra of left multiplications of this new monoid, that is, the algebra

$$\mathfrak{B} = \langle A \times A; \{f_x \mid x \in A \times A\}\rangle\ ,$$

where $f_x(y) = xy$ for all $y \in A \times A$. As is well known (see, e.g., Theorem 12.3 of [4]), $\operatorname{End}(\mathfrak{B})$ is precisely the monoid of all right multiplications of $A \times A$, hence is isomorphic to $A \times A$ and therefore to M. Specifically, this isomorphism φ of M onto $\operatorname{End}(\mathfrak{B})$ takes each $p \in m$ to $p\varphi = \varphi_p$, where $\langle md_0, md_1\rangle\varphi_p = \langle mpd_0, mpd_1\rangle$ for all

$\langle md_0, md_1\rangle \in A \times A$. Routine calculation shows that $d_i\varphi = d_i$, from which it follows by Lemma 1.1 that $\mathfrak{B}$ is a direct square. Likewise the verification that φ preserves $*$ is routine.

The following corollaries are easy consequences of the above results and their proofs.

COROLLARY 1.4. *Given monoids N and M, there is a universal algebra $\mathfrak{A}$ with* $\operatorname{End}(\mathfrak{A}) \cong N$ *and* $\operatorname{End}(\mathfrak{A} \times \mathfrak{A}) \cong M$, *if and only if M satisfies* (1.3.1)-(1.3.3) *and N is isomorphic to the centralizer of $\{d_0, d_1\}$ in M. Moreover, $\mathfrak{A}$ can be taken to have unary operations only.*

COROLLARY 1.5. *The class of all monoids isomorphic to endomorphism monoids of direct squares is closed under the formation of direct products.*

COROLLARY 1.6. *For every direct square $\mathfrak{B}$ the cardinality of* $\operatorname{End}(\mathfrak{B})$ *is square.*

As the axiom of choice has not been used, it is of interest to note that Corollary 1.6 holds even in a set theory in which not every infinite cardinal is its own square.

2. Automorphism groups of direct squares.

This section will establish the characterization theorem for automorphism groups of direct squares, and the next section will study the question for finite algebras. The algebras constructed in the next three theorems are *rigid*, i.e., their only endomorphisms are the respective identity maps. The following easy lemma will be crucial in establishing rigidity.

LEMMA 2.1. *Let M be a monoid furnished with elements d_0 and d_1 and an operation $*$ such that* (1.3.1)-(1.3.3) *hold. If d_0 is a left zero of M, the algebra given by Theorem* 1.3 *is rigid.*

Proof. Since d_0 is a left zero, so is d_1 in view of (1.3.1). By Lemma 1.2 it suffices to observe that the centralizer in M of $\{d_0, d_1\}$ contains only the identity element 1. But if an element x commutes with both d_0 and d_1 then by (1.3.2), $x = xd_0 * xd_1 = 1d_0 * 1d_1 = 1$ as desired.

The characterization theorem for automorphism groups of direct squares can now be proved after only one more definition. Given sets

A and B, define their *symmetric deleted product* $A \otimes B$ by:

$$A \otimes B = (A \times B) \cup (B \times A) - \{\langle x, x\rangle \mid x \in A \cup B\} .$$

The theorem deals only with nontrivial groups because the one-element group is the automorphism group of the direct square of any one-element algebra, but the direct square of any larger algebra has an automorphism of order two, namely τ.

THEOREM 2.2. *A nontrivial group G is isomorphic to the automorphism group of a direct square if and only if G contains an element of order two. Moreover, given a group G with a specified element t of order two, there exist a rigid multi-unary algebra $\mathfrak{A}$ and an isomorphism φ of G onto* $\mathrm{Aut}(\mathfrak{A} \times \mathfrak{A})$ *such that $t\varphi = \tau$.*

Proof. The converse being evident, let G be a group with an element t of order two. To apply Theorem 1.3 it is necessary to construct a monoid satisfying (for suitable choice of d_0, d_1, and $*$) the identities (1.3.1)-(1.3.3) and having G as its group of invertibles. The last sentence in the statement of Theorem 1.3 will make t correspond to τ provided the additional identity $d_1 * d_0 = t$ is satisfied. The rigidity of the resulting algebra will follow from Lemma 2.1 if d_0 is a left zero.

To build the required monoid, first choose (using the axiom of choice for two-element sets) a subset R of $G - \{1, t\}$ consisting of precisely one element from each set of the form $\{a, ta\}$, $a \in G - \{1, t\}$. The monoid will be defined on the union of the sets given by the following claim. The map ψ defined in the claim will become right-multiplication by t. To avoid unnecessary notational complications, we shall assume at each stage of the following construction that $M_n \cap M_k = \varnothing$ if $k < n$.

Claim 2.2.0. There exist pairwise disjoint sets M_n, $n < \omega$, and *a* function ψ mapping $\bigcup (M_n \mid n < \omega)$ into itself, such that the following conditions are satisfied.

(i) $x \in M_n$ implies $x\psi \in M_n$ and $x\psi\psi = x$.

(ii) $M_0 = G$ and $x\psi = xt$ for all $x \in M_0$.

(iii) For odd n, $M_n = M_{n-1} \otimes \bigcup (M_k \mid k < n, k \text{ even})$, and $x\psi = \langle x_1\psi, x_0\psi\rangle$ for all $x = \langle x_0, x_1\rangle \in M_n$.

(iv) For positive even n, $M_n = S_{n-1} \times R$, where $S_{n-1} = \{x \mid x \in M_{n-1}$ and $x \neq x\psi\}$. For all $\langle x, r\rangle \in M_n$,

$$\langle x, r\rangle\psi = \begin{cases} \langle x, rt\rangle & \text{if } \; rt \in R , \\ \langle x\psi, trt\rangle & \text{if } \; trt \in R . \end{cases}$$

The claim is proved by a routine induction. The only point perhaps not immediately evident is the verification of (iv) and the corresponding case of (i). Given n positive and even, the induction hypothesis allows the definition of M_n as indicated and ensures that $x\psi \in S_{n-1}$ whenever $\langle x, r\rangle \in M_n$, thereby permitting the indicated definition of $\langle x, r\rangle\psi$ as a member of M_n. Note that $r \in R$ implies $rt \in R$ or $trt \in R$. If $rt \in R$ then $\langle x, r\rangle\psi\psi = \langle x, rt\rangle\psi = \langle x, r\rangle$ because $rtt = r \in R$. Finally, if $trt \in R$ then $\langle x, r\rangle\psi\psi = \langle x\psi, trt\rangle\psi = \langle x\psi\psi, r\rangle$ (because $ttrtt = r \in R$), which is just $\langle x, r\rangle$ be the induction hypothesis.

Set $M = \bigcup (M_n \mid n < \omega)$, set $S = \bigcup (S_n \mid n \text{ odd})$, and set $W = \bigcup (M_n - S_n \mid n \text{ odd})$. Before defining operations on M some additional terminology will be convenient.

The *rank* of an element x of M is denoted rank(x) and defined to be the unique n such that $x \in M_n$. The expression "x is odd (even)" will often be used as an alternate way of stating that rank(x) is odd (even). As a notational convenience, the left and right components of an odd element x are denoted x_0 and x_1 respectively; also this notation is extended to even elements x by setting $x_0 = x_1 = x$. Note that x_0 and x_1 are even for all x.

Now define a binary operation $*$ on M as follows. Let $x, y \in M$. If $x = y$, set $x * y = x$. If x and y are distinct, even elements, set $x * y = \langle x, y\rangle$. In all other cases, set $x * y = x_0 * y_1$. It is easy to see that $*$ is a diagonal operation (see [7]), i.e.,

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

for all $x, y, z \in M$. Note that $x = x_0 * x_1$ for all x.

Set $d_0 = \langle 1, t\rangle$ and $d_1 = \langle t, 1\rangle$. Both belong to W, and clearly $d_1 * d_0 = t$ as required.

The next task is the inductive definition of multiplication in M. Let $x, y \in M$ and suppose initially that rank$(y) = 0$. If x also belongs to G, let xy be the product as given in G. If x is odd there are two cases to consider, namely $x \in W$ and $x \in S$. For $x \in W$ set $xy = x$, but for $x \in S$ define

$$xy = \begin{cases} x & \text{if } y = 1\,, \\ x\psi & \text{if } y = t\,, \\ \langle x, y\rangle & \text{if } y \in R\,, \\ \langle x\psi, ty\rangle & \text{if } ty \in R\,. \end{cases}$$

Finally, if x has positive even rank, say $x = \langle x', r \rangle$, set $xy = x'(ry)$.

Now suppose that y has positive rank and that xu has been defined for all u of rank less than rank (y). If rank (y) is odd define $xy = xy_0 * xy_1$, but if $y = \langle y', r \rangle$ has even rank, set $xy = (xy')r$.

Easy calculation shows that $xt = x\psi$ and $x1 = x$ for x of positive even rank (and for all other x by definition). Moreover, an easy induction gives $1x = x$ for all x.

In our present terminology the set W is simply the set of all odd elements satisfying the equation $x = xt$. Obviously no element of G satisfies this equation, but neither does any even element of positive rank. For if $x = \langle x', r \rangle$ satisfied the equation, it would follow that $x = \langle x', rt \rangle$ or $x = \langle x't, trt \rangle$. The first case would yield the contradiction $1 = t$, while the second would imply $x' \in W$, which is impossible because $x' \in S$ by the very definition of elements having positive even rank. Thus $W = \{x \in M \mid x = xt\}$.

The proof that multiplication is associative is somewhat tedious and will be postponed until after the verification of (1.3.1)-(1.3.3). This verification (which will not assume associativity of multiplication) requires three preliminary claims. The first of these immediately implies both (1.3.1) and the fact that d_0 is a left zero.

Claim 2.2.1. Every element of W is a left zero of M.

Fix $x \in W$. For $y \in M_0$ we have $xy = x$ by definition, so let y have positive rank and assume $xu = x$ whenever u has smaller rank then y. If y is odd it follows that $xy = xy_0 * xy_1 = x * x = x$, while if $y = \langle y', r \rangle$ is even, $xy = (xy')r = xr = x$.

The next claim provides a useful left distributive law, and the claim that follows it states a "skew" right distributivity for the element t.

Claim 2.2.2. $x(y * z) = xy * xz$ for all $x, y, z \in M$.

If $y = z$ the claim is immediate from the idempotency of $*$, so suppose $y \neq z$. Thus, if y and z are even $y * z$ is the odd element $\langle y, z \rangle$, whence the claim is simply the definition of $x\langle y, z \rangle$. In all other cases $x(y * z) = x(y_0 * z_1) = xy_0 * xz_1$ (since y_0 and z_1 are even). Because $*$ is a diagonal operation the last expression is equal to $(xy_0 * xy_1) * (xz_0 * xz_1)$, which is $xy * xz$.

Claim 2.2.3. $(x * y)t = yt * xt$ for all $x, y \in M$.

As above, the claim is obvious for $x = y$. If x and y are distinct even elements, $x * y$ is the odd element $\langle x, y\rangle$ and the claim is simply the definition of $\langle x, y\rangle t$. The other cases follow as in Claim 2.2.2.

Now we are ready to prove (1.3.2) and (1.3.3).

Proof of (1.3.2). For all $x \in M$, $xd_0 * xd_1 = x(d_0 * d_1) = x1 = x$.

Proof of (1.3.3). For all $x, y \in M$, $(x * y)d_0 = (x * y) * (x * y)t = x * y * yt * xt = x * xt = x(1 * t) = xd_0$. Similarly, $(x * y)d_1 = yd_1$.

In view of the remarks preceding Claim 2.2.1, the remaining points to be proved are the associativity of multiplication and the fact that the set of all invertible elements of M is precisely G. Associativity is verified by an inductive process employing a series of claims. Note that Claim 2.2.1 implies $(xy)z = x(yz)$ whenever $x \in W$.

Claim 2.2.4. $(xa)b = x(ab)$ for all $x \in M$ and $a, b \in G$.

We may assume $x \notin G \cup W$ and $a \neq 1 \neq b$.

Case 1. Suppose x is odd. If $a \in R$ then $(xa)b = \langle x, a\rangle b = x(ab)$. If $a = t = b$, we have $(xt)t = x\psi\psi = x = x(tt)$. It follows that $xt \in S$. Hence if $a = t$ and $b \in R$, we have $(xt)b = \langle xt, b\rangle = x(tb)$. If $a = t$ and $b \notin R \cup \{t\}$, then $tb \in R$. Thus, using the associativity just proved with xt in place of x, we have $(xt)b = (xt)(ttb) = (xtt)(tb) = x(tb)$. In sum, Case 1 is verified for $a \in R \cup \{t\}$.

The remaining possibility is that $ta \in R$, in which case, using the associativity proved above, we have

$$(xa)b = [x(tta)b] = [(xt)(ta)b] = (xt)(tab) = x(ttab) = x(ab) .$$

Case 2. Suppose x is even, $x = \langle x', r\rangle$. Then in light of Case 1,

$$x(ab) = x'(rab) = (x'(ra))b = ((x', r)a)b = (xa)b .$$

Claim 2.2.5. $(xy)a = x(ya)$ for all $x, y \in M$ and $a \in G$.

Fix $x \in M$ and $a \in G - \{1\}$. For $y \in G$ the claim reduces to the previous, so let y have positive rank and assume $(xu)b = x(ub)$ for all $b \in G$ and all u of smaller rank then y.

Case 1. Suppose y is odd. If $a = t$, then

$$\begin{aligned}(xy)t &= (xy_0 * xy_1)t = (xy_1)t * (xy_0)t = x(y_1t) * x(y_0t) \\ &= x(y_1t * y_0t) = x[(y_0 * y_1)t] = x(yt) .\end{aligned}$$

Before considering the other possibilities for a, note that for $y \in W$ the above implies $xy \in W$, since $(xy)t = x(yt) = xy$. Thus $y \in W$ implies $(xy)z = xy = x(yz)$ for all $z \in M$, so we now assume $y \in S$.

If $a \in R$ then $x(ya) = x\langle y, a\rangle = (xy)a$. The remaining possibility for a is that $ta \in R$, in which case, by the previous claim and the associativity just proved (which remains valid with yt in place of y, since they have the same rank), we have

$$\begin{aligned}x(ya) &= x[y(tta)] = x[(yt)(ta)] = [x(yt)](ta) \\ &= [(xy)t](ta) = (xy)(tta) = (xy)a .\end{aligned}$$

Case 2. Suppose y is even, $y = \langle y', r\rangle$. Then, by the previous claim and the induction hypothesis,

$$(xy)a = [(xy')r]a = (xy')(ra) = x[y'(ra)] = x[(y'r)a] = x(ya) .$$

The next claim concludes the proof of associativity.

Claim 2.2.6. $(xy)z = x(yz)$ for all $x, y, z \in M$.

Fix $x, y \in M$. For $z \in G$ the claim reduces to the previous, so let z have positive rank and assume $(xy)u = x(yu)$ for all u having smaller rank than z.

If z is odd then $(xy)z = (xy)z_0 * (xy)z_1 = x(yz_0) * x(yz_1) = x(yz_0 * yz_1) = x(yz)$.

If $z = \langle z', r\rangle$ is even, the induction hypothesis and the previous claim imply $(xy)z = [(xy)z']r = [x(yz')]r = x[(yz')r] = x(yz)$, whereupon associativity is established.

All that remains to be proved is that G is the set of invertibles of M. One preliminary claim is required.

Claim 2.2.7. Let x be a left cancelable odd element of M and let $y \in M$. If y is odd then xy is odd or $y \in \{d_0, d_1\}$. If y is even then xy has positive even rank or $y \in \{1, t\}$.

As the elements of W are left zeroes, we must have $x \in S$.

For $y \in G$ the claim is an immediate consequence of the definition of xy, so let y have positive rank and assume the claim holds whenever the rôle of y is played by an element of lower rank.

Case 1. Suppose y is odd. Then $xy = xy_0 * xy_1$. If xy_i is even for some $i \in \{0, 1\}$, then $xy_0 * xy_1$ is odd unless $xy = xy_i$. But $xy = xy_i$ would imply $y = y_i$, a contradiction. Thus xy is odd if either xy_0 or xy_1 is even.

Hence we now assume that both xy_0 and xy_1 are odd. By the induction hypothesis it follows that y_0 and y_1 are distinct elements of $\{1, t\}$, whence $y \in \{d_0, d_1\}$.

Case 2. Suppose y is even, $y = \langle y', r\rangle$. First note that xy' is not a left zero, since otherwise $xy = (xy')r = xy'$ would imply $y = y'$, a contradiction. Next, observe that xy' is odd, for the induction hypothesis would otherwise imply $y' \in \{d_0, d_1\}$, making xy' a left zero. Finally, as an odd element that is not a left zero, xy' must belong to S, whereupon $xy = (xy')r = \langle xy', r\rangle$, an element of positive even rank.

Since the elements of G are obviously invertible in M, the following claim completes the proof of the theorem.

Claim 2.2.8. No element of positive rank is invertible in M.

If M contains an odd invertible x, let y be its inverse. Clearly $y \notin \{1, t\}$, so the previous claim implies xy is either odd or a left zero or of positive even rank, contradicting $xy = 1$.

Suppose $x = \langle x', r\rangle$ is an even invertible of positive rank. Then $xr^{-1} = x'(rr^{-1}) = x'$, whence x' is invertible, a contradiction because x' is odd. The claim and the theorem are now proved.

COROLLARY 2.3. *For every universal algebra* $\mathfrak{A}$ *there is a rigid multi-unary algebra* $\mathfrak{B}$ *such that* $\operatorname{Aut}(\mathfrak{A} \times \mathfrak{A}) \cong \operatorname{Aut}(\mathfrak{B} \times \mathfrak{B})$.

3. **Automorphism groups of finite direct squares.** The construction employed in the proof of Theorem 2.2 is not adequate to characterize the automorphism groups of finite direct squares, since the algebra resulting from that construction is infinite whenever the group has more than two elements. An obvious first guess in that every finite group with an element of order two is the automorphism group of a finite direct square. The next theorem substantiates this

guess in a special case, and the theorem that follows it shows that every such group is embeddable in the automorphism group of a finite direct square in such a way that a prescribed element of order two corresponds to τ.

As infinite groups beget algebras of the same cardinality in Theorem 2.2, the infinite case of this next theorem is of interest only as a simpler alternative in a special case.

THEOREM 3.1. *Let G be a group containing an element t of order two, and suppose there is a retraction ψ of G onto* $\{1, t\}$. *Then there exist a rigid multi-unary algebra $\mathfrak{A}$, having the same cardinality as G, and an isomorphism φ of G onto* $\operatorname{Aut}(\mathfrak{A} \times \mathfrak{A})$ *such that $t\varphi = \tau$.*

Proof. To apply Theorem 1.3 we construct a monoid M satisfying (1.3.1)-(1.3.3) and having its group of invertibles isomorphic to G in such a way that t corresponds to $d_1 * d_0$. Moreover, the cardinality of G will be shared by Md_0, which is the set on which the multi-unary algebra of Theorem 1.3 is constructed. Every element of Md_0 will be a left zero, whereupon Lemma 2.1 will gurantee the rigidity of the resulting algebra.

First define a homomorphism $g \longrightarrow g'$ of G onto the symmetric group S_2 by setting g' equal to the identity permutation of $\{0, 1\}$ if $g\psi = 1$, and g' equal to the transposition (01) if $g\psi = t$. Next, set $M = G \times G$, let $\circ$ denote the usual component-wise multiplication on M, and let $\bar{\psi}$ denote the endomorphism of $\langle M; \circ \rangle$ defined by applying ψ component-wise.

To obviate the need for multiple-level subscripts, we adopt the notation $x[i]$ as an alternative to x_i in denoting the ith component of an element x of M. For $x, y \in M$ define an element x^y of M by setting $x^y[i]$ equal to $x[iy_i']$ for $i = 0, 1$. Finally, for each $g \in G$ let $\bar{g}$ denote the diagonal element $\langle g, g \rangle$ and set $\bar{G} = \{\bar{g} \mid g \in G\}$. Note that $x \in \bar{G}$ implies $x^y = x$ for all y.

A new multiplication is now defined on M by setting

$$xy = \begin{cases} x \circ y & \text{if } \ x \in \bar{G} \, , \\ x^y \circ (y\bar{\psi}) & \text{if } \ x \notin \bar{G} \, . \end{cases}$$

Clearly $\bar{G}$ is a submonoid of M and is isomorphic to G under the map $g \longrightarrow \bar{g}$.

The required operation $*$ is defined as the rectangular band operation (see [1]) on M, i.e., $x * y = \langle x_0, y_1 \rangle$ for all $x, y \in M$. The elements d_0 and d_1 are respectively defined as $\langle 1, t \rangle$ and $\langle t, 1 \rangle$; it is clear that $\bar{t} = d_1 * d_0$. Note that for all $x \in M$, $xd_0 = \langle x_0, x_0 t \rangle$ and $xd_1 = \langle x_1 t, x_1 \rangle$.

As the identities (1.3.1)-(1.3.3) are very easily demonstrated, their verifications are omitted. Also, the fact that M has no invertibles outside of $\bar{G}$ is immediate upon the observation that whenever $x \in M - \bar{G}$ and $y \in M$,

$$xy = \begin{cases} x & \text{if } \ y\bar{\psi} = \bar{1}\ , \\ \langle x_1 t, x_0 t \rangle & \text{if } \ y\bar{\psi} = \bar{t}\ , \\ \langle x_0, x_0 t \rangle & \text{if } \ y\bar{\psi} = d_0\ , \\ \langle x_1 t, x_1 \rangle & \text{if } \ y\bar{\psi} = d_1\ . \end{cases}$$

Indeed it is clear that a product of two elements lies in $\bar{G}$ only if both factors do. It is also clear from this description that the elements of Md_0 are left zeroes, as desired. Moreover, $Md_0 = \bar{G}d_0$, which is in one-to-one correspondence with G under the mapping $g \longrightarrow \bar{g}d_0 (g \in G)$. Thus Md_0 has the same cardinality as G, so all that remains to be proved is the associativity of multiplication. This is done with the aid of the following claim.

Claim. For all $x, y, z \in M$ the following hold:
(i) $(x \circ y)^z = x^z \circ y^z$;
(ii) $(x^y)^z = x^{z \circ y^z}$;
(iii) $(x^y)^z = x^{yz}$;
(iv) $(x\bar{\psi})^y = x^y \bar{\psi}$.

As (i) is immediate we begin with (ii). Let u denote the expression on the left side of (ii) and v the expression on the right. Then, for $i \in \{0, 1\}$,

$$u_i = x^y[iz_i'] = x[iz_i'(y[iz_i'])'] = x[i(z \circ y^z)_i'] = v_i, \text{ so } u = v\ .$$

To prove (iii) first note that commutativity of S_2 implies the identity $x^{y \circ z} = x^{z \circ y}$; then consider two cases.

Case 1. Suppose $y \in \bar{G}$. Then $y^z = y$, so (ii) implies $(x^y)^z = x^{z \circ y} = x^{y \circ z} = x^{yz}$.

Case 2. Suppose $y \notin \bar{G}$. Observe that $\psi^2 = \psi$ implies the identity $w^z = w^{z\bar{\psi}}$. Taking $u = x^y$ and $v = y^z = y^{z\bar{\psi}}$, we have by (ii):

$$u^z = u^{z\bar{\psi}} = x^{(z\bar{\psi}) \circ v} = x^{v \circ (z\bar{\psi})} = x^{yz}\ ,$$

as desired.

To prove (iv), let u denote the expression on the left side and v the expression on the right. Then, for $i \in \{0, 1\}$,

$$u_i = (x\bar{\psi})[iy'_i] = (x[iy'_i] = v_i ,$$

so $u = v$ and the claim is proved.

Associativity of multiplication can now be proved. Let $x, y, z \in M$. If both x and y belong to $\bar{G}$, the associativity of $\circ$ gives $(xy)z = x(yz)$, so three cases remain to be considered.

Case 1. Suppose $x \in \bar{G}$ and $y \notin \bar{G}$. Then $xy \notin \bar{G}$ and $x^z = x$, whereupon

$$(xy)z = (x \circ y)^z \circ (z\bar{\psi}) = x^z \circ y^z \circ (z\bar{\psi}) = x \circ (yz) = x(yz) .$$

Case 2. Suppose $x \notin \bar{G}$ and $y \in \bar{G}$. Then $xy \notin \bar{G}$ and $(y\bar{\psi})^z = y\bar{\psi}$, whereupon

$$\begin{aligned}(xy)z &= (x^y \circ (y\bar{\psi}))z = (x^y \circ y\bar{\psi})^z \circ (z\bar{\psi}) = (x^y)^z \circ (y\bar{\psi})^z \circ (z\bar{\psi}) \\ &= x^{yz} \circ (y\bar{\psi}) \circ (z\bar{\psi}) = x^{yz} \circ ((y \circ z)\bar{\psi}) = x^{yz} \circ (yz)\bar{\psi} = x(yz) .\end{aligned}$$

Case 3. Suppose neither x nor y belongs to $\bar{G}$. Then $xy \notin \bar{G}$ and

$$\begin{aligned}(xy)z &= (xy)^z \circ (z\bar{\psi}) = (x^y \circ (y\bar{\psi}))^z \circ (z\bar{\psi}) = x^{yz} \circ (y^z\bar{\psi}) \circ (z\bar{\psi}\bar{\psi}) \\ &= x^{yz} \circ ((y^z \circ z\bar{\psi})\bar{\psi}) = x^{yz} \circ (yz)\bar{\psi} = x(yz) ,\end{aligned}$$

completing the proof of the theorem.

COROLLARY 3.2. *Let G be a finite group containing an element t of order two, and suppose the order of G is not divisible by four. Then there is an algebra satisfying the conclusion of Theorem* 3.1.

Proof. Consider the right-regular representation, as given by Cayley's Theorem, of G as a subgroup $R(G)$ of the symmetric group $S(G)$ on the set G. Specifically, $G \cong R(G) = \{R(g) \mid g \in G\}$, where $R(g)$ denotes right-multiplication by g. It follows that for each $a \in G$, $R(t)$ interchanges the elements a and at. Thus $R(t)$ is the product of $(1/2) \mid G \mid$ disjoint transpositions. Since $(1/2) \mid G \mid$ is odd, $R(t)$ does not belong to the alternating group $A(G)$. Define a map of $S(G)$ into itself by sending $A(G)$ to the identity permutation and $S(G) - A(G)$ to $R(t)$. This map, when restricted to $R(G)$, is the retraction that permits the application of Theorem 3.1.

We conclude this section with a theorem showing that while a finite analogue of Theorem 2.2 may be very difficult to prove, the corresponding embedding question is rather easily settled. (The infinite analogue of the following theorem is also easily proved, but represents no advance over Theorem 2.2.)

THEOREM 3.3. *Let G be a finite group containing an element t of order two. Then there exist a rigid multi-unary algebra $\mathfrak{A}$, having the same cardinality as G, and an embedding φ of G into* $\operatorname{Aut}(\mathfrak{A} \times \mathfrak{A})$ *such that $t\varphi = \tau$.*

Proof. Express G as the disjoint union of sets H and K having the property that for all $g \in G$, g is a member of H if and only if gt is a member of K. Then let n be the cardinality of G and regard n as the set of all its predecessors, $n = \{0, 1, \cdots, n - 1\}$. Let Δ denote the diagonal in $n \times n$, i.e., $\Delta = \{x \in n \times n \mid x_0 = x_1\}$. Decompose $(n \times n) - \Delta$ into two sets U and V, defined as $U = \{x \in n \times n \mid x_0 < x_1\}$ and $V = \{x \in n \times n \mid x_0 > x_1\}$. Then U and V have the same number of elements, namely $(n/2)(n - 1)$, which is $n - 1$ times the cardinality of H.

Thus we can express U as the disjoint union of sets U_i, $i = 0, 1, \cdots, n - 2$, such that each U_i has the same cardinality as H. For each i choose a bijection ψ_i of H onto U_i, then extend ψ_i to a one-to-one map of G into $U \cup V$ by setting $k\psi_i = (kt)\psi_i\tau$ for all $k \in K$. It follows that $(n \times n) - \Delta$ is the disjoint union of the sets $G\psi_i$, $i = 0, 1, \cdots, n - 2$.

For each $g \in G$ define a permutation φ_g of $n \times n$ by setting

$$x\varphi_g = \begin{cases} x \text{ if } x \in \Delta \,, \\ (ag)\psi_i \text{ if } x = a\psi_i \text{ for some } a \in G \text{ and } i = 0, \cdots, n-2 \,. \end{cases}$$

It is routine to check that $\varphi_t = \tau$ and that the correspondence $g \longrightarrow \varphi_g$ defines an embedding of G into the symmetric group on $n \times n$. If for each $j \in n$ a unary operation f_j is defined on n by specifying that f_j takes the constant value j, then the multi-unary algebra $\mathfrak{A} = \langle n; \{f_j \mid j \in n\}\rangle$ has the required properties.

4. Endomorphism monoids of Ith direct powers.

Let I be a nonvoid set. Any set of the form A^I is mapped into itself by functions δ_i, $i \in I$, defined analogously to the δ_0 and δ_1 of § 1. That is, for any $x \in A^I$, $x\delta_i$ is that member of A^I whose jth co-ordinate, for every $j \in I$, is x_i. Moreover, if α_i, $i \in I$, are mappings of A^I into itself, another such map $\alpha = p(\alpha_i \mid i \in I)$ is defined by stipulating that for all $x \in A^I$ and all $i \in I$, the ith co-ordinate of $x\alpha$ is the ith coordinate of $x\alpha_i$.

All of the results of § 1, and the first result of § 2, have analogues for Ith powers. These analogues are formulated and proved in such precise analogy to their counterparts that only one will be stated here (without proof), namely the analogue of Theorem 1.3.

THEOREM 4.1. *Let I be a nonvoid set. A monoid M is isomorphic to the endomorphism monoid of an Ith direct power if and only if there exist elements $(d_i \mid i \in I)$ of M and a mapping $p\colon M^I \rightarrow M$ satisfying the identities*

$$d_i d_j = d_i \quad \text{for} \quad i, j \in I\,; \tag{4.1.1}$$

$$p(xd_i \mid i \in I) = x \quad \text{for all} \quad x \in M\,; \tag{4.1.2}$$

$$p(x_i \mid i \in I)d_j = x_j d_j \quad \text{whenever} \quad j \in I \text{ and } (x_i \mid i \in I) \in M^I\,. \tag{4.1.3}$$

Moreover, given a monoid M satisfying these conditions, there exist a multi-unary algebra $\mathfrak{A}$ and an isomorphism φ of M onto $\operatorname{End}(\mathfrak{A}^I)$ such that $d_i\varphi = \delta_i$ for $i \in I$ and $p(x_i \mid i \in I)\varphi = p(x_i\varphi \mid i \in I)$ whenever $(x_i \mid i \in I) \in M^I$.

The existence of these analogues suggests the problem of characterizing the automorphism groups of Ith powers. Given a set A of more than one element, for each member φ of the symmetric group S_I there is a permutation φ' of A^I defined by setting $\varphi' = p(\delta_{i\varphi} \mid i \in I)$. The map $\varphi \rightarrow \varphi'$ is a one-to-one anti-homomorphism of S_I into the symmetric group on A^I. Clearly, if A is the carrier-set of a universal algebra $\mathfrak{A}$, then each φ' is an automorphism of the direct power $\mathfrak{A}^I$. This suggests that a nontrivial group G is isomorphic to the automorphism group of an Ith direct power if and only if G contains a copy of S_I. Although this conjecture fails when I is infinite (in which case $\operatorname{Aut}(\mathfrak{A}^I)$ must contain copies of its own direct square), perhaps it can be verified for finite I by altering the techniques of this paper to reflect the n-dimensional die (see [3]) aspect of $\operatorname{End}(\mathfrak{A}^n)$. In any case it appears that no straightforward generalization of the present methods will suffice.

5. Acknowledgment. The author acknowledges with gratitude the benefit of several conversations with Professor G. Grätzer on the subject of this paper. Further, the author thanks Professor R. McKenzie for pointing out an error in an earlier version of the proof of Theorem 2.2.

REFERENCES

1. C. C. Chang, B. Jónsson and A. Tarski, *Refinement properties for relational systems,*

Fund. Math., **55** (1964), 249-281.
2. A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups*, A.M.S. Mathematical Surveys no. 7, vol. **I** (1961), vol. **II** (1967).
3. S. Fajtlowicz, *n-Dimensional dice*, Rend. di Mat. 4, series **VI** (1971), 1-11.
4. G. Grätzer, *Universal Algebra*, Van Nostrand Reinhold (1968).
5. G. Grätzer and W. A. Lampe, *On subalgebra lattices of universal algebras*, J. Algebra, **7** (1967), 263-270.
6. A. A. Iskander, *The lattice of correspondences of universal algebras* (Russian), Izv. Akad. Nauk. S.S.S.R., Ser. Mat., **29** (1965), 1357-1372.
7. J. Plonka, *Diagonal algebras*, Fund. Math., **58** (1966), 209-321.

Received January 9, 1975. This work was partially supported by a grant from the National Research Council of Canada.

UNIVERSITY OF MANITOBA

Current address: Department of Mathematics,
Vanderbilt University
Nashville, Tennessee, U.S.A. 37235