SOME APPLICATIONS OF THE WREATH PRODUCT CONSTRUCTION

WITH CORRECTIONS

BY Charles Wells, Professor Emeritus of Mathematics, Case Western Reserve University

Corrections and Additions to "Some Applications of the Wreath Product Construction"

Charles Wells

Department of Mathematics and Statistics
Case Western Reserve University
Cleveland, Ohio 44106, U.S.A.
November 29, 1976

1. There is one important systematic error. In the proof of Theorem 13.1, every occurrence (I count 7 of them) of the phrase "$s \in I^1$" should read "$s \in I$" (delete the superscript 1). By the way, I should have stated that the presentation of this proof closely follows Lallement [71].

2. The proof of the Krohn-Rhodes Theorem in §14 is (as far as I know) correct, but the inductive step is incorrectly described on p. 331. What is shown is that S is decomposable into a wreath product of semigroup actions, each of which has smaller measure or else is a group action dividing S.

3. Two books and an article relevant to the subject were published more or less simultaneously with the article. [1] is an exposition of the theory of characters of wreath products with applications to representations theory and to combinatorics. [2] constitutes a thorough reworking of the albegraic side of automaton theory and contains among other things two proofs of the Krohn-Rhodes Theorem, one a simpler version of the proof given in §14 of my article, and the other a reformulation of the Zeiger-Ginsburg proof which I mentioned on p. 330. This reformulation yields a stronger theorem [2, Theorem 7.1] which makes possible an efficient decomposition algorithm. [3] gives a new algebraic construction of the real numbers directly from the integers.

[1] A. Kerber, Representations of Permutation Groups II. Lecture Notes in Math 495, Springer-Verlag, 1975.

[2] S. Eilenberg, Automata, Languages and Machines, Vol. B. Academic Press, 1976.

[3] F. Faltin, N. Metropolis, B. Ross, and G.-C. Rota, The real numbers as a wreath product. Advances in Math. 16(1975), 278-304.

Reprinted from the AMERICAN MATHEMATICAL MONTHLY
Vol. 83, No. 5, May 1976
pp. 317–338

SOME APPLICATIONS OF THE WREATH PRODUCT CONSTRUCTION

CHARLES WELLS

1. Introduction. Any two semigroups can be combined, usually in more than one nonequivalent way, into a third semigroup known as a wreath product of the two semigroups. This construction has been used by group theorists for many years (see Section 16), and in the last fifteen years it has come to be used widely in the study of semigroups.

It is the aim of this article to state and prove a theorem of Krohn and Rhodes, which says that a semigroup action can be decomposed (in a certain technical sense) into the wreath product of simple groups and certain special semigroups. This theorem was motivated by the fact that putting two automata in series with no feedback corresponds roughly to taking the wreath product of certain semigroups associated with the automata. A number of other applications of the wreath product are also described in the course of the article.

Section 2 provides an introductory discussion giving a natural setting for the wreath product. A number of necessary facts about semigroups are given in Section 3. The wreath product involves semigroup actions in an intimate way; they are described in Section 4, and a brief description of the closely-related idea of an automaton is in Section 5.

The wreath product is defined in Section 6, and in a more general way in Section 7. After some necessary preliminaries in the next two sections, the structure of the wreath product is described explicitly as a semi-direct product in Section 10. The following three sections provide a number of ways of embedding (in a sense more general than usual) a semigroup action in a wreath product. In one of these sections (Section 12), the important Kaloujnine-Krasner Theorem for groups is proved. These results are then used to prove the Krohn-Rhodes Theorem in Section 14. The last two sections are occupied with descriptions of other applications of the wreath product and with historical remarks.

The Bibliography is fairly extensive. A reference to Rumpelstiltskin [64] means the article written in 1964 by Rumpelstiltskin. Two articles written in the same year are distinguished by letters; e.g., [64a], [64b].

2. Triangular actions. The kind of situation to be studied involves a set X and a set S of operators on X: for each $s \in S$, there corresponds a function $s\phi: X \to X$. In group character theory, X is a complex vector space and S is a group, so that $s\phi$ may be regarded as an invertible matrix. In many applications to abstract group theory, X is the underlying set of a group S and $s\phi$ is right multiplication by s. In combinatorics, X is often a combinatorial structure (e.g., a graph) and S its group of automorphisms. For automaton theorists, X is a set of states and S an input alphabet. A scientific theory can often be cast in this mold, too, as observed by Krohn, Langer and Rhodes [67] (from which interesting article I have drawn the discussion in this section): X is the set of possible states allowed by the theory and S is the set of possible inputs (perturbations). An ambitious working out of this idea is in Rhodes [71].

To study such a system, it is desirable to parametrize the set X in such a way that the action by S is analyzed into simpler actions on the parameters. Another way of saying this is: Regard X as a set of vectors, in the broad sense of n-tuples from some Cartesian product of sets, and describe the action of S via the changes it makes in the coordinates.

It is too much to hope that S would act coordinatewise: that is, that for $s \in S$, the effect of $s\phi$ on a coordinate would depend only on that coordinate. In general, it will depend on some or all of the other coordinates. What can frequently be done is that coordinates can be found which are ordered so that the effect on a given coordinate depends *only on that coordinate and the coordinates following it.* The action is then said to be **triangular**.

In most applications, it is convenient to take S to be a semigroup. If it is not already a semigroup, S is usually replaced by the free semigroup on the elements of S (the set of finite strings of elements of S

with concatenation as operation) or sometimes by the semigroup generated by the set of functions $s\phi$ with functional composition as operation. Moreover, one usually wants the property that the successive action of two elements of S is the same as the action of the product of those elements.

These considerations mean that the proper objects to study are "semigroup actions"; these are described in succeeding sections, and the wreath product is defined in terms of them.

3. Semigroups. A **semigroup** is a set S together with an associative multiplication on S. A **unity** in S is a (necessarily unique) element $1 \in S$ satisfying $1s = s1 = s$ for all $s \in S$. A semigroup with unity is a **monoid**. A **subsemigroup** of a semigroup S is a subset of S closed under multiplication. T is a **subgroup** of S if T is a subsemigroup of S which is a group. Warning: The unity of T may not be the unity of S; S may not even have a unity. T is a **unitary subgroup** of a monoid S if T is a subgroup of S and its unity is the same as that of S.

If S has no unity, a unity may be adjoined: let 1 be an element not in S, and define $S^1 = S \cup \{1\}$ to be the semigroup with S as a subsemigroup and $1s = s1 = s$ for $s \in S$. If S has a unity, S^1 denotes S.

If X is a set, Trans$X$ is the set of all functions from X to X, together with the binary operation, composition of functions. A function in Trans$X$ is called a **transformation** of X. Sym$X$ is the unitary subgroup of Trans$X$ of all **permutations** of X (bijections from X to X). Trans$X$ is contained in the larger monoid PF(X) of all **partial functions** from X to X. An element $f \in \mathrm{PF}(X)$ is by definition a function from a subset of X to X. If $f, g \in \mathrm{PF}(X)$, $f \circ g$ is the function with domain $\{x \in \mathrm{dom}\, f \mid xf \in \mathrm{dom}\, g\}$ (which may be empty), with $x(f \circ g) = (xf)g$. (Observe that I write functions on the right and compositions from left to right. This is undoubtedly the Wave of the Future. It makes functional diagrams easier to read and corresponds to the natural order of doing things on a pocket calculator.)

Let S be a semigroup. If $z \in S$ satisfies $zs = sz = z$ for all $s \in S$, then z is a **zero** of S. PF(X) has a zero (the empty function), but not Trans$X$. If $e \in S$ satisfies $e^2 = e$, e is **idempotent**. A unity of a semigroup is idempotent; so is a zero. A function $f \in \mathrm{Trans}X$ is idempotent if and only if its image is contained in its set of fixed points.

If V is a subset of S and $s \in S$, then $sV = \{sv \mid v \in V\}$. Vs and more complicated symbols like sVt are defined analogously.

A subset I of a semigroup S is a *right ideal* if $is \in I$ for every $i \in I$ and $s \in S$. *Left ideal* is defined similarly. A right or left ideal is necessarily a subsemigroup. If $h \in S$, then hS is a right ideal of S. S is a left and right ideal in S^1. A group has only the empty set and the whole group as ideals. Some authors do not count the empty set as an ideal or subsemigroup.

If S and T are semigroups, a function $\phi\colon S \to T$ is a **homomorphism** if $(ss')\phi = (s\phi)(s'\phi)$ for all $s, s' \in S$. If e is idempotent, then $e\phi$ is idempotent. If ϕ is surjective and 1 is a unity of S, then 1ϕ is a unity of T; the same statement is true of zeroes. T is a **homomorphic image** of S if $S\phi = T$; i.e., if ϕ is surjective.

If S and T are semigroups, $S \mid T$ (S "divides" T) if S is a homomorphic image of a subsemigroup of T. "Divides" is a reflexive, transitive relation. Two *finite* semigroups divide each other if and only if they are isomorphic.

The following technical lemmas will be used in the proof of the Krohn-Rhodes Theorem and may be skipped on first reading. The reader unfamiliar with semigroups will find their proofs a good illustration of elementary semigroup-theoretic proof techniques.

LEMMA 3.1. *Let S be a finite semigroup, and let $x \in S$. Then some power of x is an idempotent.*

Proof. Let k and n be the minimal integers such that $0 < k < n$ and $x^k = x^n$. Then $x^{k+n-k} = x^k$, so by induction $x^{k+m(n-k)} = x^k$ for all integers $m \geqq 0$. Let s be a positive integer for which $k + s = m(n-k)$ for some m. Then it is easy to see that $(x^{k+s})^2 = x^{k+s}$.

LEMMA 3.2. *Let S be a finite semigroup, ϕ a semigroup homomorphism with domain S, and $S\phi$ a group. Then there is a subgroup G of S such that $G\phi = S\phi$.*

Proof. Let G be a minimal subsemigroup of S with the property that $G\phi = S\phi$. Let $e \in G$ be an arbitrary idempotent. Then $e\phi$ is idempotent in $S\phi$, hence is the unity of $S\phi$ since the only idempotent in a group is its unity. It follows that $(eGe)\phi = G\phi = S\phi$, so by the minimality of G, $eGe = G$: in other words, every element of G is of the form ege for some $g \in G$. But $e(ege) = (ege)e = ege$, so that G is in fact a monoid with unity e. We started with an arbitrary idempotent e; hence e is the unique idempotent of G.

Now if $x \in G$, $x^k = e$ for some k by Lemma 3.1. Then $x \cdot x^{k-1} = x^{k-1} \cdot x = e$, so x has an inverse. This proves Lemma 3.2.

4. Semigroup actions. An **action on the right** by a semigroup S on a set X is a function $(x, s) \mapsto xs$ from $X \times S$ to X satisfying

$$s(st) = (xs)t \qquad (x \in X, s, t \in S). \tag{4.1}$$

Such an action determines a homomorphism $\phi: S \to \mathrm{Trans}X$ defined by

$$x(s\phi) = xs \qquad (x \in X, s \in S). \tag{4.2}$$

Conversely, any homomorphism from S to $\mathrm{Trans}X$ determines an action on X by S. Actions will be denoted by boldface capitals (usually by the boldface form of the letter which denotes the semigroup) or, when necessary, by the ordered triple (S, ϕ, X) with $\phi: S \to \mathrm{Trans}X$. $\mathbf{Trans}X$ and $\mathbf{Sym}X$ denote the actions by $\mathrm{Trans}X$ and $\mathrm{Sym}X$ respectively on X. (In their case ϕ is an inclusion function and (4.1) is just the definition of composition of functions.)

An **action on the left** of S on X is a function $(s, x) \mapsto sx$ satisfying

$$(st)x = s(tx) \qquad (s, t \in S, x \in X). \tag{4.3}$$

An action on the left determines and is determined by an *antihomomorphism* $\phi: S \to \mathrm{Trans}X$. If functions were written on the left and composition from right to left then a left action would determine a homomorphism, but then a right action would determine an antihomomorphism. This difficulty is not avoidable!

Actions in this article are on the right except where specified.

Actions are called by many other names in the literature. If $\boldsymbol{S} = (S, \phi, X)$ is an action, $\boldsymbol{S}$ is also called a **semi-automaton** or **machine** and X may be called an $\boldsymbol{S}$**-set** or $\boldsymbol{S}$**-operand.**

I have already given $\mathbf{Trans}X$ and $\mathbf{Sym}X$ as examples of actions. Here are some other examples.

Example 4.1. Any semigroup of transformations of a set X acts on X; in particular, any permutation group on X is an example of an action. Thus the automorphism group of a structure (algebraic structure, graph, topological space, etc.) acts on the underlying set of the structure.

Example 4.2. Any semigroup S acts on its own underlying set by right multiplication. This action will be denoted $\boldsymbol{S}_S$. More generally, if I is a right ideal of S, then S acts on I by right multiplication; this action is denoted $\boldsymbol{S}_I$.

Example 4.3. A group G with normal subgroup N acts on N on the right by setting

$$n^g = g^{-1}ng \qquad (g \in G, n \in N), \tag{4.4}$$

where the action is written as exponentiation to avoid confusion with multiplication in G. There is also an action on the left taking $n \mapsto gng^{-1}$ which is best denoted by writing G additively and setting

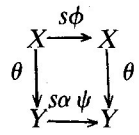
$$gn = g + n - g \qquad (g \in G, n \in N). \tag{4.5}$$

This notation will be used in Section 9.

Automata, discussed in the next section, provide another example of actions.

A pair (X, θ) is a **morphism of actions** from $S = (S, \phi, X)$ to $T = (T, \psi, Y)$ if $\alpha: S \to T$ is a homomorphism, $\theta: X \to Y$ is a function, and, for every $s \in S$,

(4.6)



commutes: in other words, $(x\theta)(s\alpha) = (xs)\theta$ for $x \in X$ and $s \in S$. Notice that then $(S, \alpha\psi, X\theta)$ is an action by S on $X\theta$. The category of actions and morphisms of actions is called Act. The analogous category for left actions is Act_L.

The morphism (α, θ) is **injective** (resp. **surjective**) if α and θ are both injective (resp. surjective). $\boldsymbol{S}$ is a **subaction** of $\boldsymbol{T}$ if α and θ are inclusions. The morphism (α, θ) is an isomorphism (= invertible in Act) if and only if α and θ are both bijective. (This is a theorem, not a definition!)

If $\boldsymbol{S} = (S, \phi, X)$ and $\boldsymbol{T} = (T, \psi, Y)$ are actions, and there is a surjective morphism of actions from a subaction of $\boldsymbol{S}$ onto $\boldsymbol{T}$, then $\boldsymbol{T}$ **divides** $\boldsymbol{S}$. In that case, T divides S in the sense of Section 3.

Of special importance is the case when $\alpha = id_S$. An $\boldsymbol{S}$**-morphism** or **equivariant map** from (S, ϕ, X) to (S, ψ, Y) (*same* S) is a function $\theta: X \to Y$ for which

$$(xs)\theta = (x\theta)s \qquad (x \in X, s \in S) \tag{4.7}$$

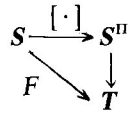
(it looks like commutativity).

In the case of left actions, this becomes $(sx)\theta = s(x\theta)$ (it looks like associativity). The category of actions by S and S-morphisms is denoted S-Act. S-Act is a much better-understood category than Act; it is a topos, which means that in many ways it resembles the category of sets. See Wraith [**75**].

If the action $\boldsymbol{G}$ is a permutation group G on a set X, the group of G-automorphisms of $\boldsymbol{G}$ is traditionally called the **centralizer of** G in Sym$X$. The group of automorphisms in Act of $\boldsymbol{G}$ is the **normalizer of** G in Sym X.

If $\boldsymbol{S} = (S, \phi, X)$ is an action, an $\boldsymbol{S}$**-partition** is a partition Π of X with the property that, if $x \equiv x' \pmod{\Pi}$ and $s \in S$, then $xs \equiv x's \pmod{\Pi}$. Any $\boldsymbol{S}$**-partition** Π gives rise to a natural S-action on the set Π by setting $[x]s = [xs]$, where $[x]$ denotes the block of Π containing x. This action is denoted $\boldsymbol{S}^{\Pi}$.

The fact just mentioned has a converse. The **quotient** of a function is the partition of its domain whose blocks are the inverse images of elements of the image of the function. The quotient Π of an S-homomorphism $F: \boldsymbol{S} \to \boldsymbol{T}$ is then an S-partition. Furthermore, the class map $x \to [x]$ is a surjective S-morphism from $\boldsymbol{S}$ to $\boldsymbol{S}^{\Pi}$, and there is a unique injective S-morphism from $\boldsymbol{S}^{\Pi}$ to $\boldsymbol{T}$ so that



commutes.

Dual to the notion of action on an S-partition is the idea of a **stable subset**: a subset $Y \subset X$ for which $ys \in Y$ for all $y \in Y$ and $s \in S$. The induced action is denoted $\boldsymbol{S}_Y$ (cf. $\boldsymbol{S}_I$ in example 4.2).

If a semigroup S is regarded as a category with one object, an action $\phi: S \to \mathrm{Trans}X$ is just a functor from S to the category of sets. Some of the embedding theorems below hold in this more general case. See Elkins and Zilber [**73**] and Wells [tbp].

5. Automata. An automaton is a semigroup action with certain additional structure. A definition suited to our use is:

Definition 5.1. An **automaton** is a septuple $(X, A, B, \phi, \mu, i, C)$, where X, A and B are sets, (FA, ϕ, X) is an action (FA denoting the free semigroup on the set A), $\mu: A \times X \to B$ is a function, $i \in A$ and $C \subset B$. X is the set of **states**, A the **input alphabet**, B the **output alphabet**, i the **initial state**, and C the set of **acceptor states**.

The part of the automaton of interest to us is the action (FA, ϕ, X); in this context, the action is often called a **semiautomaton** or **machine** (sometimes a machine has an output alphabet). There are variations on the definition in the literature, as for example in Arbib [68b], Ginzburg [68], Hopcroft and Ullman [69], and Eilenberg [74]. Davis [70] gives a neat categorical description of machines. (Note: I object to the nearly universal use of the phrase "automata theory"; after all, one does not say "groups theory.")

Both computer programs and computers themselves can be thought of as automata, but this requires care to spell out precisely. See Scott [71] and Eilenberg [74].

Although this article focuses on semigroup actions, I want to emphasize that the major concerns of automaton theorists do not lie in that direction. The major emphasis in automaton theory may be described this way: Say a subset L (a "language") of FA is **accepted** by the automaton $(X, A, B, \phi, \mu, i, C)$ if $w \in L$ if and only if $iw \in C$. The problem is to describe connections between properties of an automaton and properties of the language which it accepts.

6. Wreath products. It is now possible to define the basic object of study of this article. Let $\boldsymbol{S} = (S, \phi, X)$ and $\boldsymbol{T} = (T, \psi, Y)$ be actions. The **wreath product** $\boldsymbol{S}$ wr $\boldsymbol{T}$ of S by T (in that order) is a semigroup action of a certain semigroup $S\mathrm{wr}T$ on the set $X \times Y$. To define it, let S^Y denote the set of all functions from Y to S. The underlying set of $S\mathrm{wr}T$ is $S^Y \times T$ and the action is given by

$$(x, y)(F, t) = (x(yF), yt) \qquad (x \in X, y \in Y, F \in S^Y, t \in T). \tag{6.1}$$

Thus the action on the first coordinate depends on both coordinates, whereas the action on the second coordinate depends only on the second coordinate.

To calculate the composition of two such functions, some notation is needed. For $F, G \in S^Y$, let $F + G$ be defined by

$$y(F + G) = yF \cdot yG \qquad (y \in Y), \tag{6.2}$$

the product on the right side taking place in S. This is fairly common notation, and one of only a few places in mathematics where $+$ denotes a not necessarily commutative operation. It will fit with the notation of (4.5).

Now suppose $(G, u) \in S^Y \times T$ also. Then

$$\begin{aligned}[(x, y)(F, t)](G, u) &= (x(yF), yT)(G, u) \\ &= ([x(yF)](ytG), (yt)u) \\ &= (x, y)(F + tG), tu),\end{aligned}$$

where $tG \in S^Y$ is defined by

$$y(tG) = (yt)G. \tag{6.3}$$

Thus multiplication in $S\mathrm{wr}T$ is given by the formula

$$(F, t) \circ (G, u) = ((F + tG), tu) \qquad (F, G \in S^Y; t, u \in T), \tag{6.4}$$

which incidentally shows that $S\mathrm{wr}T$ is closed under composition. It is straightforward to show that multiplication is associative. It is apparent from (6.4) that the semigroup $S\mathrm{wr}T$ depends on S, T, and the action of T on Y, but not on the action of S on X. $S\mathrm{wr}T$ will sometimes be written "$S\mathrm{wr}(\psi)T$" to emphasize this. It is the **abstract wreath product** corresponding to $\boldsymbol{S}\mathrm{wr}\boldsymbol{T}$.

Because of the independence of $S\mathrm{wr}(\psi)T$ from ϕ, many authors define $S\mathrm{wr}(\psi)T$ given only S, T, and $\boldsymbol{T}$, without reference to an action by S. Such authors then define an action of $S\mathrm{wr}(\psi)T$ on $X \times Y$ by (6.1).

NOTE 1. If Y is finite, $S\mathrm{wr}T$ can be represented as a semigroup of matrices. Let $Y = \{1, \cdots, n\}$. If

$(F, t) \in S \mathrm{wr} T$, define the $n \times n$ matrix $M(F, t)$ by

$$M(F,t)_{ij} = \begin{cases} iF & \text{if } j = it \\ 0 & \text{otherwise.} \end{cases} \tag{6.5}$$

These matrices have exactly one entry in a given row. The mapping $(F, t) \to M(F, t)$ is a semigroup homomorphism which is an isomorphism when the action by T is faithful. (Two matrices $M(F, t)$ are multiplied in the obvious way.) Furthermore, if $\boldsymbol{x} = (x_1, \cdots, x_n)$ is any list of n elements of X, then the list $\boldsymbol{x}' = \boldsymbol{x}[M(F, t)^T]$ obtaining by "multiplying" (in the obvious way) $\boldsymbol{x}$ by the transpose of $M(F, t)$ has the property

$$(\boldsymbol{x}')_{it} = (\boldsymbol{x}_i)(iF). \tag{6.6}$$

Because of the transpose, this defines an action *on the left* of $S \mathrm{wr} T$ on X^n. A special case of this action is described by Ore [42]; the general case (not in matrix-theoretic terms) by Harary [59b]. Another special case appears in Section 10 below, preparatory to describing the structure of $S \mathrm{wr} T$ as a semigroup. A nice application of wreath products as matrix groups appears in Wiegold [63].

NOTE 2. Let $\mathscr{A}_1 = (Y, A, B, \psi, \lambda, i, D)$ and $\mathscr{A}_2 = (X, B, C, \phi, \mu, j, E)$ be automata, with the output alphabet of the first equal to the input alphabet of the second. If they are hooked up in series:

$$\text{input} \to \mathscr{A}_1 \to \mathscr{A}_2 \to \text{output}, \tag{6.7}$$

then a word w in the input acts on Y by ψ, and it also causes $\mathscr{A}_2$ to change state; but this latter action *depends on the state $\mathscr{A}_1$ was in*, because the output from $\mathscr{A}_1$ depends on that state. In other words, w acts on X by a function yF: $X \to X$ depending on $y \in Y$. Regarding (6.7) as one big automaton with state set $X \times Y$, we have that w induces

$$(x, y) \to (x\,(yF), yw)$$

(compare (6.1)); whence the connection between automata and wreath products.

7. The wreath product of an ordered set of actions. In this section, I shall describe how to construct the wreath product of a set of semigroup actions indexed by an ordered set I. The construction is a special case of a construction of Holland [69]. When I has two elements, the construction reduces to that given in section 6. If the reader follows through the discussion below with $I = \{1, 2, 3\}$ (usual ordering), he will discover that the action given on X is triangular in the sense of section 2.

Let I be a partially ordered set, and $(\boldsymbol{S}_i)_{i \in I}$ a set of actions indexed by i; let $\boldsymbol{S}_i = (S_i, \phi_i, X_i)$. Define:

(a) $X = \Pi_{i \in I} X_i$.

(b) For each $i \in I$, $M_i = \Pi_{j > i} X_i$. (If there are no $j > i$, take M_i to be a one-element set.)

(c) $W = \Pi_{i \in I} S_i^{M_i}$.

(d) The ith coordinate of $x \in X$, $m \in M$, $w \in W$ to be x_i, m_i, w_i respectively.

(e) If $x \in X$, x^i is the element of M_i which agrees with x (the projection of x on M_i). Thus, if $x \in X$, $(x^i)_j = x_j$ for all $j > i$. (If there are no $j > i$, x^i is the unique element of M_i.)

W acts on X by an action ω defined this way:

$$(xw)_i = x_i(x^i w_i) \qquad (i \in I, x \in X, w \in W). \tag{7.1}$$

If $v, w \in W$, then $[x(vw)]_i = x_i(x^i v_i)[(xv)^i w_i]$ so that

$$(vw)_i = v_i + v^i w_i, \tag{7.2}$$

where $v^i w_i$: $M_i \to S_i$ is defined by

$$u(v^i w_i) = (uv)^i w_i \qquad (i \in I, U \in M_i, v, w \in W). \tag{7.3}$$

(W, ω, X) is then the **wreath product of the system** $\{\boldsymbol{S}_i\}_{i\in I}$.

If $I = \{1, \cdots, n\}$ with the usual ordering, (W, ω, X) is denoted $\mathrm{Wr}_{i=1}^{n}\boldsymbol{S}_i$.

PROPOSITION 7.1. *Let* $\boldsymbol{S}_i$, $i = 1,2,3$, *be actions. Then* $(\boldsymbol{S}_1\mathrm{wr}\boldsymbol{S}_2)\mathrm{wr}\boldsymbol{S}_3 \cong \boldsymbol{S}_1\mathrm{wr}(\boldsymbol{S}_2\mathrm{wr}\boldsymbol{S}_3) \cong \mathrm{wr}_{i=1}^{3}\boldsymbol{S}_i$.

The proof is straightforward.

8. Some constructions. In this section and the next, some properties which semigroup actions may have, are defined, and some constructions are made. These will then be used in Section 10 to describe the abstract wreath product as a semigroup.

Let $\boldsymbol{S} = (S, \phi, X)$ be a semigroup action. Then $S\phi$ is a semigroup of transformations on X called the **constituent** of $\boldsymbol{S}$.

If Y is a stable subset of X, there is a natural S-morphism res (for "restriction") from the constituent of $\boldsymbol{S}$ to that of $\boldsymbol{S}_Y$ such that $\phi_Y = \phi \circ \mathrm{res}$, where ϕ_Y is the action of S on Y.

If S is a monoid with unity 1_S, then (S, ϕ, X) is **unitary** if

$$x1_S = x \qquad (x \in X). \tag{8.1}$$

Then $1_S\phi = \mathrm{id}_X$, where id_X denotes the identity function from X to X.

It will be assumed throughout this article that, if S is a group, then the action by S is unitary.

A semigroup action $\boldsymbol{S} = (S, \phi, X)$ is **faithful** if ϕ is injective; thus

$$(xs = xt \text{ for all } x \in X) \Rightarrow s = t. \tag{8.2}$$

In this case, S is isomorphic to the constituent of $\boldsymbol{S}$. Observe that if Y is a stable subset of X, then $\boldsymbol{S}_Y$ may not be faithful even if $\boldsymbol{S}$ is, since two elements of S may agree on Y without agreeing on all of X.

Any transformation semigroup acts faithfully. If S is any monoid, S acts faithfully on itself by right multiplication.

$\boldsymbol{S}$ is **transitive** if for every ordered pair $(x, x') \in X \times X$, there is $s \in S$ for which $xs = x'$. If $x \in X$, write

$$xS = \{xs \mid s \in S\}. \tag{8.3}$$

Then $\boldsymbol{S}$ is transitive if and only if $xS = X$ for every $x \in X$.

Warning: It is not necessary that $x \in xS$ if S is not a monoid.

If X is a set and $z \in X$, the **constant function** $c_z\colon X \to X$ satisfies

$$xc_z = z \qquad (x \in X). \tag{8.3}$$

If $\boldsymbol{S} = (S, \phi, X)$ is a faithful action, S_X^c denotes the semigroup $S\phi \cup CX$, where CX is the semigroup of constant functions on X. S will be regarded as a subsemigroup of S_X^c by the obvious identification between elements of S and $S\phi$. The natural action of S_X^c on X is denoted $\boldsymbol{S}^c$.

Similarly, S_X^{-c} denotes the subsemigroup of $S\phi$ generated by the nonconstant functions in $S\phi$, and $\boldsymbol{S}^{-c}$ the corresponding action. If every function in $S\phi$ is constant, S_X^{-c} will be $\{\mathrm{id}_X\}$ by convention.

The proof given in Section 14 of the Krohn-Rhodes theorem requires some delicate maneuvering among $\boldsymbol{S}$, $\boldsymbol{S}^c$, and $\boldsymbol{S}^{-c}$.

The following facts are useful and easy to prove.

PROPOSITION 8.1. *If S is a group and* $\boldsymbol{S} = (S, \phi, X)$ *an action, then*

(a) $\boldsymbol{S}$ *is faithful if and only if the only element of S fixing everything in X is the unity of S.*

(b) $\boldsymbol{S}$ *is transitive if and only if* $xS = X$ *for at least one* $x \in X$.

PROPOSITION 8.2. *If S is a semigroup, then*

(a) *S acts faithfully on* S^1 *by right multiplication.*

(b) *Right multiplication is transitive if and only if S is a group.*

PROPOSITION 8.3. *For P any of the four words below, if* $\boldsymbol{S}$ *and* $\boldsymbol{T}$ *are both P, then so is* $\boldsymbol{S}\mathrm{wr}\boldsymbol{T}$:

(a) *unitary* (b) *faithful*

(c) *transitive* (d) *group.*

9. Semidirect products. It is natural to consider semigroup actions $\boldsymbol{S} = (S, \phi, E)$ where E has additional structure and each map in the constituent of $\boldsymbol{S}$ is an endomorphism of the structure. For example, S is a semigroup of matrices and E is a vector space, or S is a group acting continuously on a topological space E. Here, one special case is needed, that where E is also a semigroup and S acts on the left.

This causes notational difficulties; the device of Example 4.3 will be followed here. A semigroup S **acts** on a semigroup E **on the left** if there is a function $(s, e) \mapsto se$ from $S \times E$ to E for which

$$(st)e = s(te) \qquad (s, t \in S, e \in E), \text{ and} \tag{9.1}$$

$$s(e + f) = se + sf \qquad (s \in S, e, f \in E), \tag{9.2}$$

where E is written additively.

Such an action gives rise to an antihomomorphism $\phi\colon S \to \mathrm{End}\, E$ ($\mathrm{End}\, E$ is the endomorphism monoid of the semigroup E), and conversely any such antihomomorphism yields an action of S on the left on E.

Morphisms are defined as in Act, yielding a category Sem-Act.

If the semigroup S acts on the semigroup E on the left, a new semigroup $E\mathrm{sd}S$, the **semidirect product of** E **by** S, may be constructed. (Some authors would say: "The semidirect product of S by E".) The underlying set of $E\mathrm{sd}S$ is $E \times X$, and multiplication satisfies

$$(e, s)(f, t) = (e + sf, st) \qquad (e, f \in E, s, t \in S). \tag{9.3}$$

(One must check associativity.) Mapping the action of S on E to $E\mathrm{sd}S$ is the object map of a functor SD from Sem-Act to the category of semigroups; the definition of the morphism map is left to the reader.

When S and E are monoids with unities 1_S and 0_E respectively, and the action of S on E is unitary, then $(0_E, 1_S)$ is a unity for $E\mathrm{sd}S$ which is therefore a monoid. Then $E\mathrm{sd}S$ has submonoids $E \times \{1_S\}$ and $\{0_E\} \times S$ which are isomorphic to E and S respectively, and it is easy to check that if s is invertible in S, then it has $(0_E, s^{-1})$ as inverse in $E\mathrm{sd}S$, and that for $e \in E$, conjugating $(e, 1_S)$ by $(0_E, s)$ yields $(se, 1_S)$. (That is conjugating as in (4.5), not as in (4.4).) Thus any left action by a monoid on a monoid can be embedded in a bigger monoid in which the invertible elements act by conjugation. In particular, the semidirect product of groups $N\mathrm{sd}G$ with G acting on N contains a copy of N as a normal subgroup, a copy of G as a subgroup, and the action of the copy of G on the copy of N by conjugation is the same as the given action of G on N. Thus group actions on groups can always be internalized in a semidirect product.

10. The structure of the abstract wreath product. Let Y be a set, S a semigroup. Then S^Y is a semigroup under the operation $+$ defined by (6.2). If (T, ψ, Y) is a right semigroup action, there is a canonical left semigroup action of T on S^Y defined this way: If $t \in T$, $G \in S^Y$, then tG is defined as in Section 6 by

$$s(tG) = (st)G \qquad (s \in S). \tag{10.1}$$

To show that this gives a semigroup action, it is necessary to check that $(tt')G = t(t'G)$ for $t, t' \in T$ and $G \in S^Y$, and that $t(G + G') = tG + tG'$ for $t \in T$ and $G, G' \in S^Y$. Both are easy.

For a fixed T, the map which associates the action (T, ψ, Y) and the semigroup S to the action defined above is the object map of a bifunctor $E(Y, S)$: $\boldsymbol{T}$**-Act** $\times$ **Sem** $\to$ **Sem-Act** which is contravariant in (T, ψ, Y) and covariant in S. The definitions of the morphism maps are again left to the reader (copy the definitions of the morphism maps of a hom-functor).

If $Y = \{1, 2, \cdots, n\}$, S^Y may be identified with the Cartesian power S^n by regarding $F: Y \to S$ as the n-tuple $(1F, 2F, \cdots, nF)$. The action of T on S^Y can be written this way:

$$t(s_1, \cdots, s_n) = (s_{1t}, \cdots, s_{nt}) \qquad (s_1, \cdots, s_n \in S, t \in T). \tag{10.2}$$

Then

$$(tt')(s_1, \cdots, s_n) = (s_{1tt'}, \cdots, s_{ntt'}) = t(s_{1t'}, \cdots, s_{nt'}).$$

It is tempting, but mistaken, to think that

$$t(s_{1t'}, \cdots, s_{nt'}) = (s_{1t't}, \cdots, s_{nt't}).$$

The action is on the positions the elements occupy (alibi) rather than the elements themselves (alias). I recall two days of bafflement when reading the paper by Ore [42] before I caught onto this.

The structure of the abstract wreath product can now be described.

THEOREM 10.1. *Let (S, ϕ, X) and (T, ψ, Y) be actions. Then $S\mathrm{wr}(\psi)T \cong S^Y \mathrm{sd} T$.*

Proof. This follows immediately from (6.4), the definition of semidirect product in Section 10, and the definition of S^Y.

S is called the **bottom semigroup** of $S\mathrm{wr}T$, and T the **top semigroup**. S^Y is the **basis semigroup**. When S and T are monoids, S^Y and T are canonically subsemigroups of $S\mathrm{wr}T$, and S is embedded in $S\mathrm{wr}T$ in many ways. One embedding in particular is the **diagonal embedding**, taking $s \in S$ onto (c_s, id_T). The diagonal embedding takes S onto the scalar matrices when $S\mathrm{wr}T$ is written as a matrix semigroup. S^Y corresponds to the diagonal matrices.

When S and T are groups, then S^Y is a normal subgroup of $S\mathrm{wr}T$, and the action ψ is conjugation of S^Y by the canonical copy of T in $S\mathrm{wr}T$, as described in Section 9.

The functor which takes (S, ϕ, X) and (T, ψ, Y) to $S\mathrm{wr}T$ is $A \circ SD$, where A and SD are described at the beginning of this section and in Section 9 respectively. Since $S\mathrm{wr}T$ does not depend on ϕ and X, this functor factors through a functor from **Sem** $\times$ T-**Act** to **Sem** which takes S and (T, ψ, Y) to S wr T.

When Y is the underlying set of T *and* T acts by left multiplication, $S\mathrm{wr}T$ is called the **standard wreath product**. A good deal is known about the structure of standard wreath products of groups (P. Neumann [64]). Kerber [68] studied representations of standard wreath products, and Houghton [63] their automorphisms. See also Kappe and Parker [70] and Huppert [67], pp. 94 ff and 101. *Warning*: If S, T and U are semigroups, then $(S\mathrm{wr}T)\mathrm{wr}U$ and $S\mathrm{wr}(T\mathrm{wr}U)$ (standard wreath products) are both defined, but are *not* isomorphic, except in trivial cases. This does not contradict Proposition 7.1!

When S is a group and T is **Sym** $\boldsymbol{X}$, where $X = \{1, 2, \cdots, n\}$, then $S\mathrm{wr}T$ is the **complete monomial group of degree n over S**. The properties of this group have been studied by Ore [42]. See also Crouch [55] and [60]. There are important differences between complete monomial groups and standard wreath products of groups. For example, all the complements of the basis subgroup are conjugate in the standard wreath product, but not necessarily in a complete monomial group.

When Y is infinite and S is a monoid, the semigroup S^Y has a subsemigroup $S^{(Y)}$ consisting of all those functions $F: Y \to S$ for which $yF = 1$ for all but a finite number of $y \in Y$. It is easy to see that $S^{(Y)}$ is taken into itself as a set by any $t \in T$ under the action of T on S^Y defined by (10.1); the corresponding semidirect product is the **restricted wreath product** of S by T. Taking the restricted wreath product preserves various properties. For example, if G and H are solvable groups, so is $G\mathrm{wr}H$ for any action of H. This is not true of nilpotence, however (Baumslag [59]).

11. A decomposition schema. Let $\boldsymbol{S} = (S, \phi, X)$ be a semigroup action. Parametrizing $\boldsymbol{S}$ so that the action becomes triangular means precisely to find actions $\boldsymbol{M} = (M, \psi, Y)$ and $\boldsymbol{N} = (N, \rho, P)$ so that $\boldsymbol{S}$ divides $\boldsymbol{M}\mathrm{wr}\boldsymbol{N}$; that is, so that there is a surjective morphism (α, θ): $T \to S$ where $\boldsymbol{T}$ is some subaction of $\boldsymbol{M}\mathrm{wr}\boldsymbol{N}$. This is called a **decomposition** of $\boldsymbol{S}$, or an **embedding** of $\boldsymbol{S}$ in $\boldsymbol{M}\mathrm{wr}\boldsymbol{N}$.

The latter word, although common in the literature, can be misleading; it need not happen that (α, θ) has a right inverse in Act. If it does, then $\boldsymbol{S}$ is isomorphic to a subaction of $\boldsymbol{M}\mathrm{wr}\boldsymbol{N}$; we say $\boldsymbol{S}$ is **homomorphically embedded** in $\boldsymbol{M}\mathrm{wr}\boldsymbol{N}$. Even if (α, θ) does not have a right inverse, however, it is still true (because (α, θ) is surjective) that each $x \in X$ and $s \in S$ corresponds to $(y, p) \in Y \times P$ and $(F, n) \in M\mathrm{wr}N$ respectively in such a way that $(y, p)\theta = x$, $(F, n)\alpha = s$, and (*a fortiori*) $[(y, p)(F, n)]\theta = xs$. The point is that it might happen that $x's' = xs$, yet no choice of (y', p') and (F', n') yields $(y', p')(F', n') = (y, p)(F, n)$. In other words, the "embedding" may be multivalent as well as nonhomomorphic. This should not bother the automaton theorist, who can filter out the multivalence with the output map. He will be more concerned with keeping Y and P a reasonable size, and with ensuring that M and N bear some reasonable relation to S.

In the next three sections, I shall describe a number of ways of decomposing semigroup actions into wreath products. These methods will then be used to give a proof of the Krohn-Rhodes Theorem (Section 14) and more briefly in some other applications. Some of the methods will give a homomorphic embedding of the action into the wreath product; others only an embedding or decomposition in the weaker sense just discussed.

In this section a general Schema for such decompositions is described. It includes many but not all of the methods described below. It is a Schema rather than a Theorem because it gives a general way for decomposing an action into a wreath product, but provides no control over the sizes or properties of the semigroups or sets involved in the wreath product.

DEFINITION. Let $\boldsymbol{S} = (S, \phi, X)$ be a semigroup action and Π an S-partition of X. A **coordinate system** for Π is an ordered pair $(\boldsymbol{M}, \{\beta_B\}_{B \in \Pi})$ where $\boldsymbol{M}$ is an action by a semigroup M on a set Y, and for each block $B \in \Pi$, $\beta_B : B \to Y$ is an injection satisfying the following requirement: For each $s \in S$ and $B \in \Pi$ there is $m_B^s \in M$ such that for all $x \in B$,

$$(x\beta_B)m_B^s = (xs)\beta_C, \tag{11.1}$$

where C is the block of Π to which s takes elements of B; i.e., $C = Bs$. In other words, *the partial function induced on Y by β_B and s extends in at least one way to an action by an element of M.*

THEOREM 11.1 (Decomposition Schema). *Let $\boldsymbol{S} = (S, \phi, X)$ be a faithful semigroup action with an S-partition Π and coordinate system $(\boldsymbol{M}, \{\beta_B\}_{B \in \Pi})$. Then $\boldsymbol{S}$ divides $\boldsymbol{M}\mathrm{wr}\boldsymbol{S}^{\Pi}$.*

Proof. Let $\lambda : X \to Y \times \Pi$ be defined by

$$x\lambda = (x\beta_B, B) \qquad (x \in B \in \Pi) \tag{11.2}$$

and let $\theta = \lambda^{-1} : \mathrm{Im}\lambda \to X$ (observe that λ is injective). For each $s \in S$, let $F_s : \Pi \to M$ be defined by

$$BF_s = m_B^s \qquad (B \in \Pi), \tag{11.3}$$

where m_B^s is an element of M satisfying (11.1). Let $\bar{\phi}$ be the action of S on Π. Then for all $x \in B$, $B \in \Pi$,

$$[(x\beta_B, B)(F_s, s\bar{\phi})]\theta = (xs, (x\beta_B m_B^s, Bs\bar{\phi})\theta) \tag{11.4}$$

by (11.1) and definition of the action $\boldsymbol{M}\,\mathrm{wr}\,\boldsymbol{\Pi}$. Since $\boldsymbol{S}$ is a faithful, s is determined uniquely by (11.4), so defines $(F, s\bar{\phi})\alpha = s$, for all elements $(F, s\phi)$ with F satisfying (11.3). This set of elements $(F, s\phi)$ is clearly a subsemigroup of the semigroup of $\boldsymbol{M}\,\mathrm{wr}\,S^{\Pi}$, and (α, θ) is a surjective morphism of actions by (11.4). This proves the Theorem.

NOTE. Given a set Y and injections $\beta_B : B \to Y$ for each $B \in \Pi$, one can always find a semigroup action $\boldsymbol{M}$ of a semigroup M on Y making $(\boldsymbol{M}, \{\beta_B\}_{B \in \Pi})$ a coordinate system, even in such a way that the covering (α, θ) has a right inverse. For example, take an element $e \notin Y$ and let $\tilde{Y} = Y \cup \{e\}$. For

$s \in S$ and $B \in \Pi$, define a transformation $m_B^s \in \operatorname{Trans} \tilde{Y}$ by

$$ym_B^s = \begin{cases} xs\beta_{Bs} & \text{if } y = x\beta_B,\ x \in B \\ e & \text{otherwise.} \end{cases}$$

Let $BF = m_B^s$ for $B \in \Pi$. Then $(s \mapsto (F_s, s\bar{\phi}), x \mapsto (x\beta_B, B))$ for $s \in S$, $x \in B \in \Pi$, is an injective morphism from $\boldsymbol{S}$ to a wreath product of **Trans** $\tilde{Y}$ by N acting on $\tilde{Y} \times X$. The trouble is that **Trans** $\tilde{Y}$ is so large.

COROLLARY 11.2. *Let $\boldsymbol{S}$ and $\boldsymbol{M}$ be as in Theorem* 11.1, *and suppose that $\boldsymbol{M}$ is faithful and all the β_B are bijections. Then there is a homomorphic embedding $\boldsymbol{S} \to \boldsymbol{M}\mathrm{wr}\boldsymbol{\Pi}$.*

Proof. The conditions of the corollary force m_B^s to be uniquely determined by (11.1), and hence $(F_S, s\bar{\phi})$ to be uniquely determined by s. Hence (α, θ) is not only surjective, but injective as required.

If $\boldsymbol{S}$ is transitive, $\mathrm{Aut}_s X$ satisfies the requirements on $\boldsymbol{M}$ in this corollary, with Π the set of orbits of $\mathrm{Aut}_S X$ and Y one of the orbits. (Krohn, Langer and Rhodes [67].) This corollary will be used to prove the Kaloujnine-Krasner Theorem in Section 12.

COROLLARY 11.3. *Let S be a faithful semigroup action with a stable subset Y. Then the set $\Pi = \{Y\} \cup \{\{x\}, x \in X - Y\}$ is an S-partition, and $\boldsymbol{S}$ divides $(\boldsymbol{S}_Y)^c \mathrm{wr} S^{\Pi}$.*

Proof. Let $y_0 \in Y$ and let $\beta_Y = id_Y$, $x\beta_{\{x\}} = y_0$ for $x \in X - Y$. If $s \in S$, let

$$m_B^s = \begin{cases} s\phi_Y & \text{if } B = Y \\ C_{xs} & \text{if } B = \{x\},\ x \in X - Y,\ xs \in Y \\ C_{y_0} & \text{if } B = \{x\},\ x \in X - Y,\ xs \in X - Y, \end{cases}$$

where ϕ_Y is the action of S on Y.

Then $m_B^s \in S_{\phi_Y}^c$ and it satisfies (11.1). The corollary thus follows from the decomposition schema.

This lemma will be needed later:

LEMMA 11.4. *If $\boldsymbol{S} = (S, \phi, X)$ has an S-partition Π and coordinate system $(\boldsymbol{M}, \{\beta_B\}_{B \in \Pi})$, then $(\boldsymbol{M}^c, \{\beta_B\}_{B \in \Pi})$ is a coordinate system for $\boldsymbol{S}^c$. Hence $\boldsymbol{S}^c$ divides $\boldsymbol{M}^c \mathrm{wr}(\boldsymbol{S}^{\Pi})^c$.*

Proof. Easy.

12. Decomposition of group actions. In this section a sequence of propositions will be given which culminate in the important Kaloujnine-Krasner Theorem, which says roughly that a finite group can be homomorphically embedded in an iterated wreath product of the simple groups which occur as factors in a composition series of the group. Enroute, a brief look will be taken at an application to character theory.

PROPOSITION 12.1. *Let $\boldsymbol{G} = (G, \phi, X)$ be a faithful group action and Π a G-partition. Suppose that the induced action of G on Π is transitive, let $Y \in \Pi$ and let G_Y denote the constituent on Y of the subgroup of G which fixes Y setwise. Then $\boldsymbol{G}$ is homomorphically embedded in $\boldsymbol{G}_Y \mathrm{wr} \boldsymbol{G}^{\Pi}$.*

Proof. Let $B \in \Pi$, and let $g_B \in G$ carry B to Y. Define $\beta_B : B \to Y$ by

$$x\beta_B = xg_B \qquad (x \in B).$$

Then β_B is a bijection. Now let $h \in G$, $x \in B \in \Pi$, $xh \in C \in \Pi$. Then

$$(xh)\beta_C = xhg_C = xg_B g_B^{-1} hg_C = (x\beta_B) g_B^{-1} hg_C.$$

But if $y \in Y$, then $yg_B^{-1} hg_C \in Y$. Hence by (11.1), $\boldsymbol{G}_Y$, together with the set $\{\beta_B\}_{B \in \Pi}$, forms a coordinate system for $\boldsymbol{G}$ which satisfies the requirements of Corollary 11.2.

If $\boldsymbol{G}$ is transitive, then certainly the action of G on Π is transitive. Thus the proposition applies in particular to any G-partition of any transitive group action.

If G is a group with subgroup H, then G acts transitively on the set of right cosets Hg of H by

$$(Hg)g' = Hgg' \qquad (g, g' \in G). \tag{12.1}$$

(This is clearly well-defined.) Indeed, every transitive action by G is G-isomorphic to an action of this form (take H to be the subgroup fixing an element). Let G^H denote the constituent of G on the set of cosets of H.

COROLLARY 12.2. *Let G be a group with subgroup H and G/H the set of right cosets of H in G. Then $\boldsymbol{G}_G$ is homomorphically embedded in $\boldsymbol{H}_H \mathrm{wr} \boldsymbol{G}^H$.*

Proof. $\boldsymbol{G}_G$ (G acting on its own underlying set by right multiplication) is faithful and transitive, and G/H is a G-partition. Let $Y = H$ (which is a block of G/H). The subgroup of G which fixes H setwise is H itself. The corollary then follows from Prop. 12.1 (see Wells [69]).

Observe that Cor. 12.2 embeds G in a wreath product of H by the constituent of G on G/H. If any action of H on a set X is given, then G acts on $X \times (G/H)$ via this embedding (see Section 6).

Now suppose a k-dimensional complex representation τ (a homomorphism into a multiplicative group of $k \times k$ matrices with complex entries) of H is given, and suppose H has finite index n in G. By using the construction in Corollary 12.2 and the matrix representation in Section 6, G may be represented by $n \times n$ monomial matrices whose entries are $k \times k$ complex matrices. By what may best be described as erasing parentheses, an nk-dimensional complex representations of G is obtained; it is the representation of G *induced* by the given representation of H. Because of the relative ease of calculating the character of such a representations, this construction is a fundamental tool used by finite group theorists in constructing character tables. See Gorenstein [68], chapter 4, section 4, or Lang [65], chapter VIII, section 6. Of special interest in this connection is the study of "M-groups"; see Huppert and Wielandt [62], Kerber [70], and the references therein. This construction is a special case of the left adjoint construction in Wraith [75] 53, example (iii).

COROLLARY 12.3. *Let G be a group with normal subgroup H. Then G is isomorphic to a subgroup of the standard wreath product $H \mathrm{wr}(G/H)$.*

Proof. Observe that the assumption that H is normal means that G/H is a group. The corollary will follow from Corollary 12.2 if it is shown that $\boldsymbol{G}^H$ is Act-isomorphic to $(\boldsymbol{G}/\boldsymbol{H})_{G/H}$. But that is immediate from (12.1).

A direct proof of Cor. 12.3 is in H. Neumann [67], p. 46.

A group G is an **extension of $\boldsymbol{H}$ by $\boldsymbol{B}$** if there is an exact sequence

$$1 \to H \to G \to B \to 1.$$

(This means that there is a monomorphism from H into G and an epimorphism from G onto B such that the image of the monomorphism is exactly the kernel of the epimorphism.) The preceding corollary says that *every extension of H by B is embedded in the standard wreath product of H by B.*

Now let G be a finite group. It is well known that there is a sequence (not necessarily unique) of subgroups $1 = N_0, N_1, N_2, \cdots, N_k = G$ of G with the property that for $i = 0, 1, \cdots, k-1$, N_i is a normal subgroup of N_{i+1} and N_{i+1}/N_i is simple (has no nontrivial normal subgroups). Furthermore, the number of simple groups of a given isomorphism type is determined uniquely. This sequence is called a *composition series* for G.

Thus G is an extension of N_{k-1} by N_k/N_{k-1}. Furthermore, N_{k-1} is an extension of N_{k-2} by N_{k-1}/N_{k-2}, and in general N_i is an extension of N_{i-1} by N_i/N_{i-1} for $i = 1, \cdots, k$. The following theorem then follows from Corollary 12.3 by induction.

THEOREM 12.4. (Kaloujnine-Krasner [51a], p. 47). *A finite group can be embedded in an iterated standard wreath product of the simple groups occurring in a composition series of the group.*

REMARKS. (1) In the notation preceding the statement of Theorem 12.4, let N_1 act on X, and let

$E_i = N_{i+1}/N_i$ for $i \geqq 1$. Then the embedding of the theorem gives a triangular action of G on the set $X \times E_1 \times \cdots \times E_n$. This fact will be used in the proof of the Krohn-Rhodes Theorem.

(2) Observe that the simple groups in the theorem divide the given group.

(3) "Kaloujnine" is frequently transliterated "Kalužnin".

(4) Actually, Kaloujnine and Krasner proved a more general theorem, allowing any tower of subgroups instead of a composition series — but then the wreath product may not be standard. See also Marchionna-Tibiletti [57].

13. Other decomposition theorems. In this section, two related decomposition techniques are given which are needed for the proof of the Krohn-Rhodes Theorem. These two techniques are in a way dual to the Schema of Section 11, since they decompose (S, ϕ, X) by breaking up S instead of breaking up X.

THEOREM 13.1. *Let $\boldsymbol{S}$ be a monoid and $S = (S, \phi, X)$ be a faithful unitary action, and suppose $S = I \cup T$, where I is a left ideal and T a unitary submonoid. Let $\boldsymbol{I}^1$ denote the induced unitary action by I^1 on X, where $I^1 = I \cup \{1_S\}$ even if I has a unity. Let $\boldsymbol{T}$ be the action by right multiplication of T on itself. Then $\boldsymbol{S}$ divides $\boldsymbol{I}^1 \mathrm{wr} \boldsymbol{T}^c$.*

Proof. Let $W = I^1 \mathrm{wr} T^c$, and define mappings $E: T \to I^1$, $F_s: T \to I^1$ (for $s \in I^1$) by

$$tE = id_X \qquad (t \in T) \tag{13.1}$$

and

$$tF_s = ts \qquad (t \in T, s \in I^1). \tag{13.2}$$

Let $\bar{S}$ denote the subsemigroup of W consisting of elements of the form (E, t) $(t \in T)$ and (F_s, c_t) $(s \in I^1,\ t \in T)$. One checks that $\bar{S}$ is indeed a subsemigroup:

$$(E, t)(E, t') = (E, tt') \qquad (t, t' \in T)$$

$$(E, t)(F_s, c_{t'}) = (F_{ts}, c_{t'}) \qquad (s \in I^1, t, t' \in T)$$

$$(F_s, c_t)(E, t') = (F_s, c_{tt'}) \qquad (s \in I^1, t, t' \in T)$$

and

$$(F_s, c_t)(F_{s'}, c_{t'}) = (F_{sts'}, c_{t'}) \qquad (s, s' \in I^1, t, t' \in T).$$

Define $\alpha: \bar{S} \to S$ by

$$(E, t)\alpha = t, \quad (F_s, c_t)\alpha = st \qquad (t \in T, s \in I^1), \tag{13.3}$$

and $\theta: X \times T \to X$ by

$$(x, t)\theta = xt \qquad (t \in T, x \in X). \tag{13.4}$$

Then α and θ are surjective, and

$$[(x, t)\theta](E, t')\alpha = xtt' = [(x, t)(E, t')]\theta$$

by (6.1), (13.1), (13.3), and (13.4), and

$$[(x, t)\theta](F_s, c_{t'})\alpha = xtst' = [(x, t)(F_s, c_{t'})]\theta$$

by (6.1), (13.2), (13.3) and (13.4). By (4.6), this proves Theorem 13.1.

THEOREM 13.2. *Let M be a finite monoid and $\boldsymbol{M} = (M, \phi, X)$ a unitary faithful action. Let G be the group of units of M. Then $I = M - G$ is a two-sided ideal of M, and $\boldsymbol{M}$ divides $\boldsymbol{I} \mathrm{wr} \boldsymbol{G}_G$, where $\boldsymbol{I}$ is the induced action of I on X.*

Proof. First a proof that I is a two-sided ideal: If $h \in I$ then by right multiplication h induces a mapping from M to M which is neither injective nor surjective, because if it were one it would have to

be the other (M is finite!) and an element inducing a bijection is invertible. But then if $m \in M$, neither mh nor hm can induce bijections, so neither is in G.

Now the remainder of the proof is sketched; it is similar to that of Theorem 13.1.

Define $E: G \to I$ and $F_s: G \to I$ for $s \in I$ by

$$gE = id_X \qquad (g \in G)$$

and

$$gF_s = gsg^{-1} \qquad (g \in G, s \in I).$$

The subset $\bar{S}$ of elements (E, g) and (F_s, g) for $g \in G$ and $s \in I$ is then a submonoid of $I \mathrm{wr} G$. Define $\alpha: \bar{S} \to S$ by

$$(E, g)\alpha = g, \qquad (F_s, g)\alpha = sg$$

and $\theta: X \times G \to X$ by

$$(x, g)\theta = xg.$$

Then (α, θ) is a surjective morphism of actions onto (S, ϕ, X).

14. The Krohn-Rhodes Theorem. The Krohn-Rhodes Theorem says that simple groups and certain semigroups U_1, U_2 and U_3 are the fundamental semigroups into which finite semigroup actions may be decomposed. U_3 is the transformation semigroup on a two-element set consisting of the two constant functions, and the identity function. U_1 is the subsemigroup of constant functions, and U_2 is a subsemigroup (either one of them) consisting of one constant function and the identity function.

THEOREM (Krohn-Rhodes [65]). *Let $\boldsymbol{S} = (S, \phi, X)$ be a faithful semigroup action with S and X finite. Then $\boldsymbol{S}$ divides an iterated wreath product of a finite number of semigroup actions $\boldsymbol{T} = (T_i, \Psi_i, Y_i)$, where T_i is either U_1, U_2 or U_3 or a finite simple group dividing S.*

NOTE: It can happen that the decomposition require U_3 even though U_3 does not divide S (Meyer-Thompson [69], section 4). On the other hand, it is obvious that any occurrence of U_1 or U_2 in the covering can be replaced by U_3. Much more is known about the role the semigroups U_1, U_2 and U_3 play in the Krohn-Rhodes Theorem. For example, finite simple groups and U_1, U_2, U_3 are exactly the **irreducible** semigroups: T is irreducible if whenever $T | A \mathrm{wr} B$ then $T | A$ or $T | B$. This was included by Krohn and Rhodes [65] in their statement of the theorem. More recent information about this is in Stiffler [73].

Every cyclic group of prime order is simple. An automaton whose constituent is a cyclic group is called a **counter.** The famous result of Feit-Thompson [63] thus implies that a group action by a group of odd order can be decomposed into counters. There are many other finite simple groups, of course; the discovery of finite simple groups is an active area of research (Carter [72], Gorenstein [68]).

The least number of groups needed in a covering of $\boldsymbol{S}$ by a wreath product is called the **group complexity** of the actions. This has been the subject of active research lately. See Rhodes and Tilson [72], Rhodes [74], Rhodes [to appear] and Tilson [to appear], the articles in *Advances in Mathematics* Vol. 11 (1973), and the references therein.

The proof below is in essence due to Meyer and Thompson [69]. A very different proof is that of Ginzburg [68] based on a proof by Zeiger which contained errors.

Proof of Krohn-Rhodes Theorem. The proof is by transfinite induction on a measure $\|\boldsymbol{S}\|$ of $\boldsymbol{S}$ defined this way:

$$\|\boldsymbol{S}\| = (|S_X^c|, |X|, |S|). \tag{14.1}$$

Thus $\|\boldsymbol{S}\|$ is an ordered triple of positive integers; note that $|S_X^c| > 0$ by convention (Section 8).

The set of measures is lexicographically ordered.

$$(m_1, m_2, m_3) < (n_1, n_2, n_3) \Leftrightarrow \begin{cases} m_1 < n_1 \text{ or} \\ m_1 = n_1 \text{ and } m_2 < n_2 \text{ or} \\ m_1 = n_1,\ m_2 = n_2 \text{ and } m_3 < n_3. \end{cases}$$

This is a well-ordering.

The smallest measure is $(1,1,1)$, which makes S the one-element group, for which the Theorem is true (if we take the one-element group to be simple, which not all authors do). Because of the faithfulness assumption, the next occurring measure is $(1,2,1)$, for which the same comment applies. The next two measures are $(1,2,2)$ and $(1,2,3)$, which correspond to the actions defined above for U_1, U_2 or U_3.

If (S, ϕ, X) is a group, the Theorem is true by the Kaloujnine-Krasner Theorem. (Note that the latter theorem is a bit stronger, since it says that the simple groups occurring in the wreath covering are factors in a composition series for the group, rather than merely dividing the group. That is a genuine distinction; for example, every alternating group on more than 4 letters is simple and contains every smaller alternating group.)

I shall now show that if $\boldsymbol{S}$ is not a group and has measure larger than $(1,2,3)$, then it divides a wreath product $\boldsymbol{T}_1 \mathrm{wr} \boldsymbol{T}_2$ such that for $i = 1,2, |\boldsymbol{T}_i| < |\boldsymbol{S}|$ and $\boldsymbol{T}_i^{-c}$ divides $\boldsymbol{S}$. The theorem will then follow by transfinite induction: Suppose the theorem is true of all actions with measure strictly less than that of $\boldsymbol{S}$. Then $\boldsymbol{T}_i$ is covered by a wreath product of semigroup actions T_{ij} where T_{ij} is either U_1, U_2 or U_3 or a finite simple group dividing T_i. Then $\boldsymbol{S}$ is covered by $\boldsymbol{T}_{11} \mathrm{wr} \cdots \mathrm{wr} \boldsymbol{T}_{21} \mathrm{wr} \cdots$. Furthermore, if T_{ij} is a finite simple group, it divides T_i and hence T_i^{-c} (Lemma 3.1), and hence S.

CASE 1. $\boldsymbol{S}^{-c}$ has a proper nontrivial S_X^{-c}-subaction. That is a subset $Y \subset X$ closed under action by any nonconstant element of $\boldsymbol{S}$. "Nontrivial" means that Y has more than one element.

Then by Corollary 11.3 and Lemma 11.4. $\boldsymbol{S}^c$, and hence $\boldsymbol{S}$ divides $(\boldsymbol{S}_Y)^c \mathrm{wr}(\boldsymbol{S}^\Pi)^c$, where Π is the congruence on X which has Y as the only class with more than one element. Observe that $(\boldsymbol{S}_Y)^c \mathrm{wr}(\boldsymbol{S}^\Pi)^c$ is an action on the set $Y \times \Pi$.

It is easy to verify that S_Y^{-c} divides S_X^{-c}, so $|S_Y^{-c}| \leqq |S_X^{-c}|$. Since $|Y| < |X|$, it follows that $\|\boldsymbol{S}_Y^c\| < \|\boldsymbol{S}\|$. (Implicitly used here is the fact that $(S_X^c)^{-c} = S_X^{-c}$.)

Similarly, $(\boldsymbol{S}^\Pi)^{-c}$ divides $\boldsymbol{S}^{-c}$, and $|\Pi| < |X|$, so that $\|(\boldsymbol{S}^\Pi)^c\| < \|\boldsymbol{S}\|$.

CASE 2. S is a monoid, $\boldsymbol{S}$ is unitary, and the subgroup G of invertible elements of S satisfies $1 < |G| < |S|$. By Theorem 13.2, $\boldsymbol{S}$ divides $\boldsymbol{I} \mathrm{wr} \boldsymbol{G}_G$ acting on $X \times G$, where $I = S - G$.

Clearly $|I^{-c}| \leqq |S^{-c}|$ and $|I| < |S|$, so $\|I\| < \|S\|$. Moreover, I^{-c} divides S. On the other hand, $\boldsymbol{G}_G$ is a group action and G divides S.

CASE 3. S is not a group and does not satisfy Case 1 or Case 2. I also assume that S is a monoid and $\boldsymbol{S}$ is unitary, because if the Krohn-Rhodes Theorem is true for finite unitary monoid actions it is necessarily true for all finite semigroup actions. (If G is a nontrivial group, S a finite semigroup, and $G | S^1$, then certainly $G | S$.)

$S - \{1_S\}$ has no permutations, so is an ideal of S (no non-permutation times any element of S can be a permutation, but 1_S is a permutation). $S - \{1_S\}$ cannot consist entirely of constant functions, for then $S^{-c} = \{id_X\}$, $\boldsymbol{S}^{-c}$ has a nontrivial subaction, and Case 1 holds (unless $|X| = 2$, but then $\|\boldsymbol{S}\| \leqq (1,2,3)$).

Thus there is $t \in S$ with $t \neq 1_S$, t nonconstant. Then $1 < |Xt| < |X|$. Then St is a proper subset of $S - \{1_S\}$ or else Xt would be a subaction making Case 1 hold. Hence St is a proper left ideal of $S - \{1_S\}$.

Let I be a maximal proper left ideal of $S - \{1_S\}$. Let $x \in S - I^1$ and let $T = Sx \cup \{1_S\}$. Then $I \cup Sx$ is a left ideal properly containing I, so $I \cup T = S$. T is a unitary submonoid, so Theorem 13.1 implies that S divides $\boldsymbol{I}^1 \mathrm{wr} \boldsymbol{T}^c$, where $\boldsymbol{I}^1$ acts on X and $\boldsymbol{T}^c$ on T.

Clearly $(I^1)^{-c}$ and $(T^c)^{-c} = T^{-c}$ both divide S. It follows from the facts that $\boldsymbol{I}^1$ acts on X and that $|I^1| < |S|$ that $\|\boldsymbol{I}^1\| < \|\boldsymbol{S}\|$. To show that $\|\boldsymbol{T}\| < \|\boldsymbol{S}\|$ it is necessary to show that $|T^{-c}| < |S^{-c}|$ since

we have no control over the relative sizes of the sets T and X being acted on. Since $|S^{-c}| \geqq 2$, if $T-\{1_S\}$ consists entirely of constant functions, we are done. Otherwise, $T-\{1_S\}$ contains a nonconstant element x, so by the same argument as for t, Sx is a proper subset of S and $XSx = Xx$ is a proper subset of X. If $S-T$ consisted only of constants, this would imply that Xx is a proper nontrivial Sx^{-c} subaction, so Case 1 would hold. Hence $S-T$ contains a nonconstant, so $|T^{-c}| < |S^{-c}|$, which completes the proof of the Krohn-Rhodes Theorem.

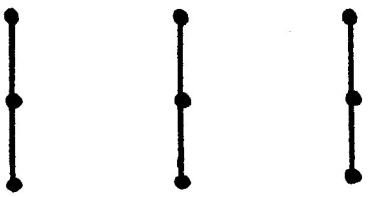


FIG. 15.1

15. Applications to automorphism groups and combinatorics. An automorphism of the disconnected graph G in Fig. 15.1 must take one of the three connected components into the same one or another one. Thus Aut G has a G-partition Π consisting of the three components. It follows easily from Prop. 12.1 that Aut$G$ is the wreath product of the cyclic group of order 2 (the automorphism group of one component) by the symmetric group of degree 3 (the action of Aut$G$ on the components). (Observe that Aut$G$ is not transitive.)

This is an instance of a general theorem known to graph-theorists which dates back at least to Frucht [49]:

THEOREM 15.1. *Let a finite graph G be the disjoint union $\cup_{i=1}^{m} \cup_{j=1}^{n_i} A_{ij}$, with A_{ij} connected and $A_{ij} \cong A_{rs}$ if and only if $j = s$. Then*

$$\mathrm{Aut}G \cong \prod_{i=1}^{m} (\mathrm{Aut}A_{i1} \times \mathrm{Sym}(n_i)).$$

It is necessary that the components to be connected, and the theorem won't work for infinite graphs unless each component has no proper subgraph isomorphic to it.

An analogous theorem is true of partially ordered sets and of other kinds of structures for which the disjoint union of two instances of that kind of structure is another structure of that kind.

Going back to a graph G, Aut$G$ sometimes has a fixed point which, when removed, puts one in the situation of Theorem 15.1. Thus the graph G in Fig. 15.2. has Aut $G \cong C_2 \mathrm{wr} \mathrm{Sym}4$. Erasing the edges e and f would yield a graph with automorphism group $C_2 \mathrm{wr}(C_2 \times C_2)$.

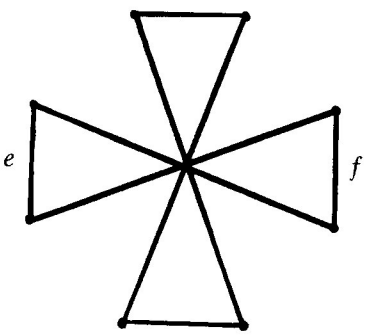


FIG. 15.2

See Harary [59] for another situation in which the automorphism group of a graph decomposes as a wreath product.

This is a useful device for studying rooted trees, the automorphism groups of which are direct products of wreath products of symmetric groups, if one insists that the automorphisms preserve roots and levels (distances from roots). Thus the automorphism group of the tree in Fig. 15.3 is (Sym2wrSym3) × (Sym2wrSym3wrSym2).

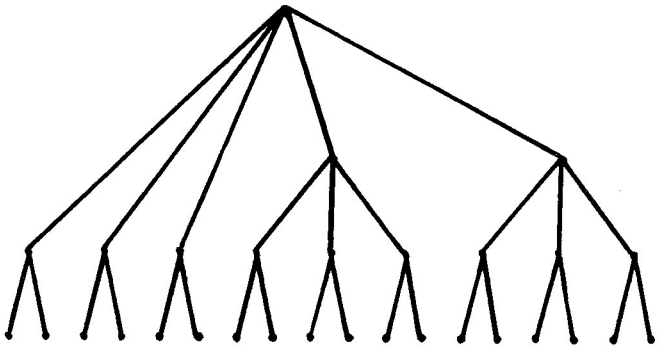


FIG. 15.3

For more on this, see McCarthy [tbp]. The opposite, synthetic problem of constructing a graph with a given wreath product as automorphism has been studied by Frucht and Harary [70] and Uebelacker [tbp].

This sort of analysis can be made for certain structures that appear in counting-problems.

Thus suppose one wants to segregate 8 distant objects into two groups of 3 and a group of 2. If the two groups of 3 were to be kept distinct, so that for example (naming the objects by the first eight digits) $\{\{1,2,3\},\{4,5,6\},\{7,8\}\}$ were different from $\{\{4,5,6\},\{1,2,3\},\{7,8\}\}$, the number of ways to do this is the well-known multinomial coefficient

$$m(2,3,3) = \frac{8!}{2!3!3!} = 560. \tag{15.5}$$

But suppose the two groups of 3 are indistinguishable. How many ways can the objects be arranged now? There are 8! ways to permute the objects, but some permutations do not yield a new arrangement. For example, the permutation (1 4) (2 5 3 6) (7 8) applied to the arrangement $\{\{1,2,3\}\ \{4,5,6\},\ \{7,8\}\}$ leaves the arrangement unchanged.

Formally, define an **arrangement** as a partition of the set of integers from 1 to 8 into a set of two and two sets of three integers. An **automorphism** of the arrangement is a permutation of the set which leaves the partition unchanged. By the same sort of argument as for the graphs and trees before, the automorphism group of any arrangement is $(\mathrm{Sym}(3)\mathrm{wr}C_2) \times C_2$, which has $6^2 \cdot 2 \cdot 2 = 144$ elements. Thus there are $8!/144 = 280$ possible arrangements. In this simple case, one could have deduced this directly from (15.5), but it is clear that the method is quite general. This problem is treated by Pólya [37], in the paper in which he gave the wreath product its name.

In that paper, he introduced his general theory of counting which is a fundamental tool in combinatorial theory. Many of its applications involve the wreath product. Good recent expositions of his theory and generalizations are in Beckenbach [64] and Read [68].

A particular application which dates back to the turn of the century (see Burnside [55]) is to centralizers of permutations.

THEOREM 15.2. *Let ϕ be a permutation of a finite set, and suppose ϕ has n_i cycles of length r_i, for*

$i = 1, 2, \cdots, m$. Then the permutations which commute with ϕ form a group isomorphic to

$$\prod_{i=1}^{m} (C_{n_i} \text{wrSym}(n_i)).$$

The formal similarity between Theorems 15.1 and 15.2 is no accident. One can represent a permutation as a directed graph; for example as in Fig. 15.4, which represents the permutation (1 2) (3 4 5) (6 7 8).

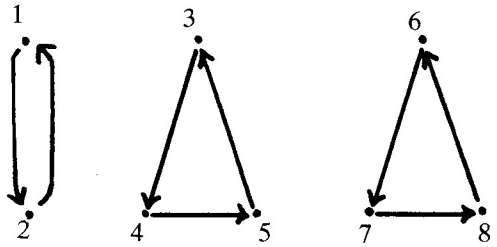


FIG. 15.4

A permutation commutes with this permutation if and only if it is an automorphism of the directed graph, and the automorphisms of an n-cycle form a group isomorphic to C_n. Theorem 15.2 then becomes a special case of Theorem 15.1.

The more difficult task of constructing the centralizer in Sym(n) of a permutation group G on n letters can be simplified by using Theorem 15.2 and a theorem of Kuhn [04]. The normalizer of G can be described as a "twisted wreath product" (see Section 16). Certain sets of polynomials over finite fields appear as wreath products; see Carlitz and Hayes [72], Lausch and Nöbauer [73, Section 4.9] (and the references there in), and Wells [74].

16. History, other applications and generalizations. Group actions with nontrivial G-partitions (called **imprimitive** by group theorists) have been understood as long as groups have been known. The earliest reference I have is Ruffini, *Teoria generale delle equazioni*, published in Bologna in 1799; but I only know of it secondhand (Kuhn [04]). Other works in which the concept appeared include Cayley [78], and Miller [01].

The wreath product in something like its present form appears in Loewy [29]. This apparently came to the attention of I. Schur, who suggested questions related to it to his students B. H. Neumann and W. Specht (see Specht [33]). The name *Kranzgruppe* is due to Pólya [37] in a long and influential paper already mentioned in Section 15. P. Hall developed the standard wreath product as a tool for studying abstract groups, a technique continued by the Neumanns and many other group theorists and in wide use today. This line of development has been ignored almost completely here, a lack I have tried to make up for by including a sizeable selection of relevant papers in the Bibliography. Two excellent expositions in specific areas are H. Neumann [67] and Kerber [71].

The abstract wreath product construction was extended to semigroups by B. H. Neumann [60]. The automaton theorists began studying wreath product decomposition of semigroups in the early sixties, their initial major result being the Krohn-Rhodes Theorem (Section 14).

The wreath product is also used in other studies of semigroups not connected with the Krohn-Rhodes Theorem, particularly in the work of Petrich [73a], [73b], [74] (and the references therein).

The wreath product has been generalized in various ways. The wreath product of ordered groups is discussed by B. H. Neumann [49], [60]. The **verbal wreath product** (where the basis group is a verbal product rather than a direct product) is introduced by Smelkin [64]; see also Burns [66] and H. Neumann [67]. Petrich [73a, V. 3], and [73b, Section 2] (and in other papers referred to there) allows the functions in S^Y to be defined only partly, yielding the **partial-mapping wreath product.** B. H. Neumann [56, Section 8] constructs the **crown product** by amalgamating subgroups in the basis group.

Various related constructions by B. H. Neumann [63], H. Neumann [67, p. 65], and Wong [67] have been called the **twisted wreath product**. Krohn, Mateosian and Rhodes [67] used this construction (they called it the # product) to characterize the concatenate of two "generalized machines", and Altinger [70] used a version almost identical with that of H. Neumann [67] just mentioned to describe the normalizer of a subgroup of a symmetric group.

The wreath product construction has been extended to groupoids by Houghton [74b] and to categories by Wells [tbp].

The author would like to thank C. Houghton, D. McCarthy, B. H. Neumann, J. Wiegold and the referee for suggestions and corrections made to an earlier version of this paper, for historical backgrounds, and for suggesting items to include in the Bibliography.

Bibliography

This Bibliography is selective. I have included fundamental papers, papers referred to in the article, and papers published in obscure places of which the reader might never otherwise become aware. I have included a good many recent papers in which the wreath product is applied to problems in group theory in an effort to remedy the lack of attention given these areas in the body of the article. I have excluded many papers referred to in the following articles and books, which have extensive bibliographies of their own: H. Neumann [67], Kerber [71], Petrich [73a] and Rhodes and Allen [73].

S. Ahmad, Split dilations of finite cyclic groups with application to finite fields, Duke Math. J., 38 (1970) 547–554.

J. Altinger, Normalizers of permutation groups, Ph.D. thesis, Case Western Reserve Univ., 1970.

M. Arbib, The automata theory of semigroup embeddings, J. Austral. Math. Soc., 8 (1968a) 568–570.

———, ed. Algebraic Theory of Machines, Languages, and Semigroups, Academic Press, 1968b.

L. Babai, Automorphism groups of graphs and edge-contractions, Discr. Math., 9 (1974) 13–20.

J. M. Bateman, R. Phillips, and L. Sonneborn, Wreath products and representations of degree one or two, Trans AMS 181 (1973), 143–155.

G. Baumslag, Wreath products and p groups, Proc. Cam. Phil. Soc., 55 (1959) 224–231.

———, Roots and wreath products, Proc. Cam. Phil. Soc. 56 (1960) 109–117.

———, Wreath products and extensions, Math. Z., 81 (1963) 286–299.

E. F. Beckenbach (ed), Applied Combinatorial Mathematics, Wiley, 1964.

V. O. Bélickov, The automorphism group of a wreath product of finite groups, Doponde Akda. Nauk. Ukrain. RSR, Ser. A, (1971) 489–492. MR 45 (1973) 6931. (Generalized by Segal [72]).

E. H. Bird, Automorphism groups of partial orders, Bull. A.M.S., 79 (1973) 1011–1015.

N. Blackburn, Some homology groups of wreath products, Ill. J. Math., 16 (1972) 116–129.

J. Buckley, Polynomial functions and wreath products, Ill. J. Math., 14 (1970) 274–282.

A. Bunt, On the automorphism group of a generalized wreath product, Latv. Math. Yearbook, 3 (1968), 81–88. MR 39, 2881. (Contains error corrected in Houghton [74b].)

R. G. Burns, A wreath tower construction of countably infinite, locally finite groups, Math. Z., 105 (1968) 367–386.

———, Verbal wreath products and certain product varieties of groups, J. Austral. Math. Soc., (1966).

W. Burnside, Theory of groups of finite order, Reprint of second edition, Dover, New York, 1955.

L. Carlitz and D. Hayes, Permutations with coefficients in a subfield, Acta Arith., 21 (1972) 131–135.

R. Carter, Simple groups of Lie type, Wiley, New York, 1972.

R. Carter and P. Fong, The Sylow 2-subgroups of the finite classical groups, J. Algebra, 1 (1964) 13–151.

J. Cossey, K. Gruenberg and L. G. Kovács, The presentation rank of a direct product of finite groups, J. Algebra, 28 (1974) 597–603.

A. Cayley, A theorem on groups, Math. Ann., 13 (1878) 561–565 = Coll. works 10, no. 659, 149–152.

R. Crouch, Monomial groups, Trans. Amer. Math. Soc., 80 (1955) 187–215.

———, Characteristic subgroups of monomial groups, Pac. J. Math., 10 (1960) 85–89.

R. Davis, Universal coalgebra and categories of transition systems, Math. Sys. Th., 4 (1970) 91–95.

J. Dixon, Complements of normal subgroups in infinite groups, Proc. Lon. Math. Soc., (3) 17 (1967) 431–446.

S. Eilenberg, Automata, Languages and Machines, Volumes A and B, Academic Press, vol. A, 1974, vol. B, 1975.

T. Evans, Embedding systems for multiplicative systems and projective geometries, Proc. Amer. Math. Soc., 3 (1952) 614–620.

K. Krohn, R. Mateosian, and J. Rhodes, Methods of the algebraic theory of machines, I, Decomposition theorem for generalized machines; properties preserved under series and parallel compositions of machines, J. Comput. System Sci., 1 (1967) 55–85.

E. M. Kublanova, Triangular polynomial groups, Latvijas Valsts Univ. Zinatn. Raksti, 151 (1971) 79–103. MR 46, 7393.

H. W. Kuhn, On imprimitive substitution groups, Amer. J. Math., 26 (1904) 45–102.

W. Kuyk, An algebraic application of the wreath product, Math. Centrum Amsterdam ZW, 1964–007 (1964).

———, Certain representations of the wreath product and of a certain type of its subgroups, Math. Centrum Amsterdam ZW, 1964–013, (1964).

G. Lallement, On the prime decomposition theorem for finite monoids, Math. Systems Theory, 5 (1971) 8–12.

S. Lang, Algebra, Prentice-Hall, Englewood Cliffs, N. J., 1965.

H. Lausch and W. Nöbauer, Algebra of Polynomials, North Holland, 1973.

A. Loewy, Über abstrakt definierte Transmutationssysteme oder Mischgruppen, J. Reine Angew. Math., 157 (1927) 239–254.

C. Marchionna-Tibiletti, Sul prodotto di gruppi permutabili, Ann-Mat. Pura Appl., (4) 43 (1957), 341–356. MR 21 (1960), No. 1336. MR 21 also reviews a number of other articles by Marchionna-Tibiletti on the wreath product.

D. J. McCarthy, Automorphism groups of separable graphs, To be published.

J. D. McKnight, Jr., and E. Sadowski, The kernel of the wreath product of semigroups, Semigroup Forum, 4 (1972) 232–236.

J. O. P. Meldrum, Central series in wreath products, Proc. Cambridge Philos. Soc., 63 (1967) 551–567.

A. R. Meyer and C. Thompson, Remarks on algebraic decompositions of automata, Math. Systems Theory, 3 (69) 110–118.

G. Miller, On the transitive substitution groups whose order is a power of a prime number, Amer. J. Math, 23 (1901) 173–178. Coll. works 2, 114–118.

B. H. Neumann, On ordered groups, Amer. J. Math., 71 (1949) 1–18.

———, Ascending derived series, Comp. Math., 13 (1956) 47–64.

———, Embedding theorems for semigroups, J. London Math. Soc., 35 (1960a) 184–192.

———, Embedding theorems for ordered groups, J. London Math. Soc., 35 (1960b) 503–512.

———, Lectures on topics in the theory of infinite groups, Tata Inst. for Fundamental Research, Bombay, (1961). Ch. V has a good exposition of the wreath product of groups.

———, Twisted wreath products of groups, Arch. Math., 14 (1963) 1–6.

———, Some remarks on semigroup presentations, Canad. J. Math., 19 (1967) 1018–1026.

B. H. and H. Neumann, Embedding theorems for groups, J. London Math. Soc., 34 (1959) 465–479.

B. H. Neumann, H. Neumann and P. Neumann, Wreath products and varieties of groups, Math. Z., 80 (1962) 44–62.

H. Neumann, Varieties of Groups, Springer, New York, 1967.

H. Neumann and J. Wiegold, Linked products and linked embeddings of groups, Math. Z., 73 (1960) 1–19.

P. Neumann, On the structure of standard wreath products of groups, Math. Z., 84 (1964) 343–373.

O. Ore, Theory of monomial groups, Trans. Amer. Math. Soc., 51 (1942) 15–64.

M. Osima, Some remarks on the characters of S_n, II, Canad. J. Math., 6 (1954) 511–521.

M. Petrich, Introduction to Semigroups, Merrill Publ., Columbus, Ohio, 1973a.

———, Dense extensions of completely 0-simple semigroups I, J. Reine Angew. Math., 258 (1973b) 103–125.

———, The structure of completely regular semigroups, Trans. Amer. Math. Soc., 189 (1974) 211–236.

G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, Acta Math., 68 (1937) 145–254.

R. C. Read, The use of S-functions in combinatorial analysis, Canad. J. Math., 20 (1968) 808–841.

N. Reilly, Some applications of wreath products and ultraproducts in the theory of lattice ordered groups, Duke Math. J., 36 (1969) 825–834.

J. Rhodes, Application of automata theory and algebra to biology, physics, psychology, games, codes. Department of Math., Univ. of Calif., Berkeley, 1971.

———, Axioms for complexity for all finite semigroups, Advances in Math., 11 (1973) 159–209.

———, Finite binary relations have no more complexity than finite functions, Semigroup Forum, 7 (1974) 92–103.

———, A proof of the fundamental lemma of complexity (strong version) for arbitrary finite semigroups, J. Combinatorial Theory (to appear).

J. Rhodes and D. Allen, Jr., Synthesis of the classical and modern theory of finite semigroups, Advances in Math., 11 (1973) 238–266.

J. Rhodes and B. R. Tilson, Improved lower bounds for the complexity of finite semigroups, J. Pure Appl. Algebra, 2 (1972) 13–71.

D. Scott, The Lattice of flow diagrams, Symposium on Semantics of Algorithmic Languages, 310–366. Springer Lecture Notes No. 188, 1971.

T. Scruton, Bounds for the class of nilpotent wreath products, Proc. Cambridge Philos. Soc., 62 (1966) 165–169.

D. Segal, Ph.D. thesis, Univ. of London, Dec. 1972 (investigates the automorphism group of certain restricted standard wreath products).

K. Seksenbaev, On the anticenter of bands of groups, Izv. Akad. Nauk Kazah SSR Ser. Fiz.-Mat., (1966) 20–34.

———, On the group of automorphisms of the wreath product of two groups, Vestnik Akad. Nauk Kazah SSR, (1969) 43–45. (Contains error corrected in Houghton [72].)

———, The Hopficity of a wreath product of two groups, Izv. Akad. Nauk Kazah SSR Ser. Fiz.-Mat., (1971) 50–54. Mr 45 (1973) 6932.

A. Smel'kin, Wreath products and varieties of groups, Dokl. Akad. Nauk, SSSR, 157 (1964) 149–170.

———, A note to my paper "Wreath products and varieties of groups", Izv. Akad. Nauk, SSSR Ser. Mat., 31 (1967) 433.

W. Specht, Eine Verallgemeinerung der Permutationsgruppen, Math. Z., 37 (1933) 321–341.

P. Stiffler, Jr., Extension of the fundamental theory of finite semigroups, Advances in Math., 11 (1973) 159–209.

M. Tainiter, A characterization of idempotents in semigroups, J. Combinatorial Theory, 5 (1968) 370–373.

B. R. Tilson, Complexity of two-J-class semigroups, Advances in Math., 11 (1973) 215–237.

———, On the complexity of finite semigroups, J. Pure. Appl. Algebra, (to appear).

J. W. Uebelacker, Product graphs for subgroups of the wreath product of two groups, I and II, to be published.

J. W. Wamsley, The deficiency of wreath products of groups, J. Algebra, 27 (1973) 48–56.

B. A. F. Wehrfritz, Wreath products and chief factors of linear groups, J. London Math. Soc., (2) 4 (1972) 671–681.

E. Weiner, Permutations of finite abelian groups: some counting theorems, Ph.D. thesis, Case Western Reserve Univ., 1970.

C. Wells, Groups of permutation polynomials, Monatsh. Math., 71 (1967) 248–262.

———, H-split translations of groups, J. Algebra, 12 (1969) 195–206.

———, Functions which commute with translations of a finite field, Proc. Amer. Math. Soc., 46 (1974) 347–50.

———, The wreath product of categories (to be published).

J. Wiegold, Embedding group amalgams in wreath products, Math. Z., 80 (1962) 148–153.

———, Adjunction of elements to nilpotent groups, J. London Math. Soc., 38 (1963) 17–26.

J. Wilson, Groups with every proper quotient finite, Proc. Cambridge Math. Soc., 69 (1971) 373–391.

W. Wong, Twisted wreath products and Sylow 2-subgroups of the classical simple groups, Math. Z., 97 (1967) 406–424.

G. C. Wraith, Lectures on elementary topoi, in Model theory and topoi, Springer Lecture Notes 445, 1975.

Department of Mathematics, Case Western Reserve University, Cleveland, OH 44106.