Internat. J. Math. & Math. Sci.
VOL. 20 NO. 4 (1997) 803-812

COMULTIPLICATION ON MONOIDS

MARTIN ARKOWITZ
Mathematics Department
Dartmouth College
Hanover, NH 03755
E-mail address: Martin.Arkowitz@Dartmouth.edu

MAURICIO GUTIERREZ
Mathematics Department
Tufts University
Medford, MA 02155
E-mail address: mgutierr@tufts.edu

(Received April 14, 1997)

ABSTRACT. A comultiplication on a monoid S is a homomorphism $m : S \to S * S$ (the free product of S with itself) whose composition with each projection is the identity homomorphism. We investigate how the existence of a comultiplication on S restricts the structure of S. We show that a monoid which satisfies the inverse property and has a comultiplication is cancellative and equidivisible. Our main result is that a monoid S which satisfies the inverse property admits a comultiplication if and only if S is the free product of a free monoid and a free group. We call these monoids semi-free and we study different comultiplications on them.

KEY WORDS AND PHRASES: Monoid, free product, comultiplication, inverse property, cancellative monoid, equidivisibility, semi-free monoid.

1991 AMS SUBJECT CLASSIFICATION CODES: Primary: 20M05, 20M10 Secondary: 20M99, 20N99.

1. INTRODUCTION

Comultiplications can be defined for objects in any category with coproducts and zero morphisms. Given such an object X, a comultiplication is a morphism $m : X \to X \sqcup X$ (the coproduct of X with itself), such that the composition of m with either projection $X \sqcup X \to X$ is the identity morphism. The general theory has been surveyed in [1], and in [3] it is specialized to algebraic systems. In [2], [5] and [6], comultiplications on groups have been studied. In this paper we extend some of these results to the category of monoids. We are interested in the following kind of question: given a monoid with a comultiplication, what restrictions does this place on the structure of the monoid? This question has been answered for groups by Kan who showed that a group admits a comultiplication if and only if it is free [6]. For monoids, Bergman and Hausknecht have shown that the existence of an *associative* comultiplication yields a presentation of the monoid by generators and relations [3, Thm. 20.16]. Here we study arbitrary comultiplications on a monoid which satisfies an additional condition (the inverse property). We show that these monoids are semi-free, i.e., the free product of a free group and a free monoid. In order to prove this result, we establish along the way, several results for monoids with the inverse property which may be of independent interest. In particular, we show that if such a monoid has a comultiplication, then it is cancellative (Theorem 3.5) and equidivisible (Theorem 4.2). In addition, we study the possible comultiplications on semi-free monoids in §5.

2. BASIC FACTS AND DEFINITIONS

A **monoid** is a set S with an associative, binary operation and an identity element. The operation is usually called multiplication and denoted by juxtaposition and the identity element is denoted by 1. The notions of **submonoid** and **homomorphism** of monoids are analogous to the corresponding notions in group theory. There is also the notion of a **free monoid** defined by the usual universal property. A good general reference on monoids is [4]. Every free monoid has a basis in which each element can be expressed as a word. Moreover, it is proved in [7, 5.1] that a free monoid has a *unique* basis which we call the **canonical basis**.

If S and T are monoids, then one can form the **free product** $S * T$ in analogy to the free product of groups. A typical element of $S*T$ is $\alpha = s_1t_1s_2t_2\cdots s_nt_n$, where $s_i \in S$ and $t_j \in T$. A product of the first k factors of α, $1 \leq k \leq 2n$, is called an **initial segment** of α. If some factor, say $s_i = 1$, then the expression $t_{i-1}\,1\,t_i$ in α can be replaced by $t_{i-1}t_i$. If $s_2, \dots, s_n, t_1, \dots, t_{n-1}$ are all $\neq 1$, then α is said to be **reduced**. If $\alpha \in S * T$, then the number of non-trivial factors of α in reduced form, is denoted $|\alpha|$ and called the **length** of α. If $f : S \to S'$ and $g : T \to T'$ are homomorphisms, then a homomorphism $f * g : S * T \to S' * T'$ is defined by

$$(f * g)(s_1t_1\cdots s_nt_n) = f(s_1)g(t_1)\cdots f(s_n)g(t_n).$$

We also have injection homomorphisms $i_1 : S \to S * T$ and $i_2 : T \to S * T$ defined by $i_1(s) = s$ and $i_2(t) = t$ and projection homomorphisms $p_1 : S * T \to S$ and $p_2 : S * T \to T$ defined by $p_1(\alpha) = \prod s_i$ and $p_2(\alpha) = \prod t_j$. If $S = T$, we write $i_1(s) = s'$ and $i_2(t) = t''$ so that a typical element α of $S * S$ can be expressed

$$\alpha = s_1't_1''\cdots s_n't_n'', \quad s_i, t_j \in S. \tag{2.1}$$

The **equalizer** E_S of S is the submonoid $\{\alpha | \alpha \in S * S, p_1(\alpha) = p_2(\alpha)\}$ of $S * S$. Then $p_1|_{E_S} = p_2|_{E_S}$ and we denote this homomorphism by $p : E_S \to S$. A **comultiplication** m on S is a homomorphism $m : S \to S * S$ such that $p_1m = p_2m = id : S \to S$. The comultiplication m is called **associative** if $(id*m)m = (m*id)m : S \to S*S*S$. A **section** of p is a homomorphism $\mu : S \to E_S$ such that $p\mu = id : S \to S$. Clearly comultiplications of S correspond to sections of p. In particular, if S admits a comultiplication, then S can be embedded in E_S.

Given a monoid S, let $\{z_s \mid s \in S\}$ be a set in one-to-one correspondence with S. The **free group in** S, [4, 12.1], is the group $\overline{S}$ with presentation $\langle z_s \mid z_sz_t = z_{st},\ s, t \in S\rangle$. Then a homomorphism $\nu : S \to \overline{S}$ is defined by $\nu(s) = z_s$. Moreover, if G is a group and $f : S \to G$ is a homomorphism of monoids, then there is a uniquely defined group homomorphism $\overline{f} : \overline{S} \to G$ with $\overline{f}\nu = f$. Thus, if S admits a comultiplication m, then $\overline{S}$ admits a comultiplication $\overline{m}$ with $\overline{m}\nu = (\nu * \nu)m$. Finally, by [4, Thm. 12.4], S embeds in a group if and only if $\nu : S \to \overline{S}$ is an embedding.

If S is a monoid and a, $b \in S$ with $ab = 1$, then b is called a **right inverse** of a and a is called a **left inverse** of b. If $a \in S$ has a left inverse and a right inverse, then they are unique and equal. We then say that a is **invertible** with inverse a^{-1}. The set U_S of invertible elements of S is a submonoid of S which is a group.

Definition 2.2. Let S be a monoid.

(1) S has the **inverse property** if whenever a, $b \in S$ and $ab = 1$, then $ba = 1$.

(2) S is **cancellative** or a **cancellation monoid** if $ab = ac$ or $ba = ca$ implies $b = c$, for all $a, b, c \in S$.

In verifying cancellation, we usually establish one of the two implications. The other is proved analogously. We note that if a monoid satisfies either property of Definition 2.2, so does every submonoid.

Clearly every cancellation monoid has the inverse property: For if $ab = 1$, then $(ba)(ba) = (ba)1$, and so $ba = 1$. However, the converse is not true since the monoid $S = \{1, a, a^2\}$ with $a^3 = a$ has the inverse property but is not cancellative.

3. THE INVERSE PROPERTY AND CANCELLATION

In this section we show that a monoid with a comultiplication which has the inverse property is cancellative. We begin with some simple lemmas.

Lemma 3.1. *If S and T have the inverse property and $\alpha, \xi \in S * T$ are in reduced form, then there exists $\alpha_1, \xi_1, \delta \in S * T$ such that δ is invertible, $\alpha = \alpha_1\delta^{-1}$, $\xi = \delta\xi_1$ and $\alpha_1\xi_1$ is in reduced form. Furthermore, $\delta = 1$ or is an initial segment of ξ.*

Proof. Express α and ξ in reduced form as

$$\alpha = \prod_{i=1}^{n} s_i' t_i'', \quad \xi = \prod_{j=1}^{p} x_j' y_j'', \tag{3.2}$$

where $s_i, x_j \in S$ and $t_i, y_j \in T$ and consider

$$\alpha\xi = s_1' t_1'' \cdots s_n' t_n'' x_1' y_1'' \cdots x_p' y_p''.$$

We list several cases.

Case 1: t_n and x_1 are both $\neq 1$. Then $\alpha\xi$ is in reduced form and so we set $\delta = 1$.

Case 2: $t_n = 1$. Then $\alpha\xi = s_1' t_1'' \cdots t_{n-1}''(s_n x_1)' y_1'' \cdots x_p' y_p''$. Let l be the smallest integer ≥ 0 such that either (i) $s_{n-l}x_{l+1} \neq 1$ or (ii) $t_{n-l-1}y_{l+1} \neq 1$. We only consider (i) since (ii) is analogous. We have

$$s_n x_1 = 1, \quad t_{n-1}y_1 = 1, \quad \ldots, \quad t_{n-l}y_l = 1 \quad \text{and}$$
$$\alpha\xi = s_1' t_1'' \cdots t_{n-l-1}''(s_{n-l}x_{l+1})' y_{l+1}'' \cdots x_p' y_p''.$$

By the inverse property for S and T, $x_1^{-1} = s_n$, $y_1^{-1} = t_{n-1}$, $\ldots$, $y_l^{-1} = t_{n-l}$. Thus $\delta = x_1' y_1'' \cdots x_l' y_l''$ is invertible with $\delta^{-1} = t_{n-l}'' s_{n-l+1}' \cdots s_n'$ and we set $\alpha_1 = s_1' t_1'' \cdots s_{n-l}'$ and $\xi_1 = x_{l+1}' y_{l+1}'' \cdots y_p''$.

Case 3: $x_n = 1$. This is similar to Case 2, and hence omitted. □

Lemma 3.3. *Let S and T be monoids.*

(1) *If S and T have the inverse property, then $S * T$ has the inverse property.*

(2) *If S and T are cancellative, then $S * T$ is cancellative.*

Proof. (1) Suppose $\alpha, \xi \in S * T$ with $\alpha\xi = 1$. By Lemma 3.1, there exists $\delta, \alpha_1, \xi_1 \in S * T$ such that δ is invertible, $\alpha = \alpha_1\delta^{-1}$, $\xi = \delta\xi_1$ and $\alpha_1\xi_1$ is in reduced form. Since $\alpha_1\xi_1 = \alpha\xi = 1$, it follows that either $\alpha_1 = \xi_1$ or $\alpha_1 = 1 = \xi_1$. In either case $\xi\alpha = 1$.

(2) Suppose $\alpha\xi = \beta\xi$, where $\alpha, \beta, \xi \in S * T$ are all reduced. By Lemma 3.1, there exists $\delta_1, \alpha_1, \xi_1, \delta_2, \beta_2, \xi_2 \in S * T$ such that δ_1, δ_2 are invertible, $\alpha = \alpha_1\delta_1^{-1}$, $\xi = \delta_1\xi_1$, $\beta = \beta_2\delta_2^{-1}$, $\xi = \delta_2\xi_2$ and $\alpha_1\xi_1$ and $\beta_2\xi_2$ are reduced. By Lemma 3.1, δ_1 and δ_2 are either 1 or an initial segment of ξ. We distinguish two cases: (i) $|\delta_1| \leq |\delta_2|$ and (ii) $|\delta_2| \leq |\delta_1|$ and only treat (i).

If $|\delta_1| \le |\delta_2|$, then $\delta_2 = \delta_1\gamma$ for some invertible γ. Hence $\delta_1\xi_1 = \xi = \delta_2\xi_2 = \delta_1\gamma\xi_2$. Thus $\xi_1 = \gamma\xi_2$. Therefore $\alpha_1\gamma\xi_2 = \alpha_1\xi_1 = \beta_2\xi_2$. There are now several cases to consider depending on whether $\alpha_1\gamma$ and β_2 end with a primed or double-primed term and ξ_2 begins with a primed or double-primed term. For example, suppose that $\alpha_1\gamma$ and β_2 end with primed terms (say s'_i and u'_j, respectively) and ξ_2 begins with a primed term (say x'_k). Then $s_i x_k = u_j x_k$. By cancellation we obtain $s_i = u_j$ and so $\alpha_1\gamma = \beta_2$. All other cases are treated similarly. Thus $\alpha = \alpha_1\delta_1^{-1} = \alpha_1\gamma\delta_2^{-1} = \beta_2\delta_2^{-1} = \beta$. □

Corollary 3.4. *Let S be a monoid.*

(1) *If S has the inverse property, then E_S has the inverse property. If S is cancellative, then E_S is cancellative.*

(2) *Let S have a comultiplication. If E_S has the inverse property, then S has the inverse property. If E_S is cancellative, then S is cancellative.*

Theorem 3.5. *If S is a monoid with the inverse property and S admits a comultiplication, then S and E_S are cancellative.*

Proof. We first show that if $\xi \in E_S$ and $\xi \ne 1$, then $|\xi^2| > |\xi|$. Suppose $|\xi^2| \le |\xi|$. We write ξ as $\gamma s'\delta$ or $\gamma t''\delta$ for some $\gamma, \delta \in S*S$ and s, t non-trivial elements of S. If $\xi = \gamma s'\delta$, then $\xi^2 = \gamma s'\delta\gamma s'\delta$ and so $\delta\gamma = 1$. By 2.2, $\delta = \gamma^{-1}$ and hence $\xi = \gamma s'\gamma^{-1}$. Therefore $p_2(\xi) = p_2(\gamma)p_2(\gamma^{-1}) = 1$. Hence $1 = p_1(\xi) = p_1(\gamma)s(p_1(\gamma))^{-1}$ and so $s = 1$. This contradicts $\xi \ne 1$. A similar argument holds if $\xi = \gamma t''\delta$.

Next we show that E_S has the following weak cancellation property: $\alpha\xi = \alpha$ or $\xi\alpha = \alpha$ implies $\xi = 1$ for $\alpha, \xi \in E_S$. Suppose $\alpha\xi = \alpha$ and $\xi \ne 1$. Then $|\xi^2| > |\xi|$. Then $\alpha\xi^k = \alpha$, for all $k \ge 1$, and we choose N such that $|\xi^N| > 2|\alpha|$. Then $\alpha\xi^N$ cannot equal α since their lengths are different. This contradicts $\xi \ne 1$. The other implication is proved similarly.

It now follows that S has this same weak cancellation property: $ax = a$ or $xa = a$ implies $x = 1$. This is because the comultiplication m on S provides an embedding of S into E_S and the weak cancellation property is inherited by submonoids.

Now we prove that S is cancellative. Suppose $ax = bx$ in S. Then $\alpha\xi = \beta\xi$, where $\alpha = m(a)$, $\beta = m(b)$ and $\xi = m(x)$. We represent α and ξ by (3.2) and

$$\beta = \prod_{k=1}^{q} u'_k v''_k \tag{3.6}$$

which are all assumed to be reduced. Again we consider cases.

Case 1: t_n, v_q, x_1 are all $\ne 1$. Clearly $\alpha = \beta$ and so $a = b$.

Case 2: $x_1 = 1$. Then

$$s'_1 \cdots s'_n (t_n y_1)'' x'_2 \cdots y''_p = u'_1 \cdots u'_q (v_q y_1)'' x'_2 \cdots y''_p.$$

If $t_n y_1 = 1$ and $v_q y_1 \ne 1$, then, comparing both sides of the above equation from the right, we obtain $s_n x_2 = x_2$. This implies that $s_n = 1$, contradicting the fact that α is reduced. Thus $v_q y_1 = 1$. We continue in this manner and conclude that if k cancellations are required to write $\alpha\xi$ in reduced form, then exactly k cancellations are needed to put $\beta\xi$ into reduced form. Therefore by Lemma 3.1, there exists $\alpha_1, \beta_1, \xi_1, \delta \in S * S$ with δ invertible such that $\alpha = \alpha_1\delta^{-1}$, $\beta = \beta_1\delta^{-1}$, $\xi = \delta\xi_1$ and $\alpha_1\xi_1$ and $\beta_1\xi_1$ are reduced. Assume that α_1 ends in an s'_k (a similar argument holds if α_1 ends in a t''_k). Then ξ_1 begins with some x'_l and β_1 ends with some u'_r. Furthermore $s_k x_l \ne 1$ and $u_r x_l \ne 1$. We can further factor

$$\alpha = \alpha_2 s'_k \delta^{-1}, \quad \beta = \beta_2 u'_r \delta^{-1}, \quad \xi = \delta x'_l \xi_2$$

for some $\alpha_2, \beta_2, \xi_2 \in S * S$. Thus $\alpha_2(s_k x_l)'\xi_2 = \beta_2(u_r x_l)'\xi_2$. Since these are reduced, we cancel ξ_2 from both sides and then multiply on the right by δ^{-1}, getting $\alpha_2(s_k x_l)'\delta^{-1} = \beta_2(u_r x_l)'\delta^{-1}$. Applying p_2, we have

$$a = p_2(\alpha) = p_2(\alpha_2(s_k x_l)'\delta^{-1}) = p_2(\beta_2(u_r x_l)'\delta^{-1}) = p_2(\beta) = b.$$

Case 3: $x_1 \neq 1$ and t_n or $v_n = 1$. This case is like Case 2, and hence omitted.

This proves that S is cancellative. By Corollary 3.4, E_S is cancellative. □

4. EQUIDIVISIBILITY

We have need of the following definition [7, p. 103].

Definition 4.1. A monoid S is **equidivisible** if the equation $ax = by$ in S implies that either there exists a $c \in S$ such that $a = bc$ and $cx = y$ or there exists a $d \in S$ such that $b = ad$ and $x = dy$.

Note that if S is cancellative, then S is equidivisible if $ax = by$ implies that either there exists a $c \in S$ such that $a = bc$ or there exists a $d \in S$ such that $b = ad$.

Theorem 4.2. *If the monoid S has the inverse property and admits a comultiplication, then S is equidivisible.*

Proof. We assume $ax = by$ in S and apply m to obtain $\alpha\xi = \beta\eta$, where $\alpha = m(a)$, $\beta = m(b)$, $\xi = m(x)$ and $\eta = m(y)$. By Lemma 3.1, there are elements $\delta, \theta, \alpha_1, \xi_1, \beta_1, \eta_1 \in S * S$ such that δ and θ are invertible, $\alpha = \alpha_1\delta^{-1}$, $\xi = \delta\xi_1$, $\beta = \beta_1\theta^{-1}$, $\eta = \theta\eta_1$ and $\alpha_1\xi_1$ and $\beta_1\eta_1$ are reduced.
Case 1: $|\alpha_1| < |\beta_1|$. Since $\alpha_1\xi_1 = \beta_1\eta_1$ is an equality of reduced expressions, $\alpha_1\lambda = \beta_1$ for some $\lambda \in S * S$. Then

$$\alpha(\delta\lambda\theta^{-1}) = \alpha_1\delta^{-1}\delta\lambda\theta^{-1} = \beta_1\theta^{-1} = \beta.$$

We apply p_1 to this and get $ad = b$, where $d = p_1(\delta\lambda\theta^{-1})$.
Case 2: $|\beta_1| < |\alpha_1|$. This is similar to Case 1.
Case 3: $|\alpha_1| = |\beta_1|$. Let us assume that α_1 ends with s_k' (a similar argument holds when α_1 ends with t_k'') and so ξ_1 begins with some x_l'. We write $\alpha_1 = \widetilde{\alpha}_1 s_k'$ and $\xi_1 = x_l'\widetilde{\xi}_1$. Since $|\alpha_1| = |\beta_1|$, β_1 ends with some u_r' and so η_1 begins with some w_t'. We write $\beta_1 = \widetilde{\beta}_1 u_r'$ and $\eta_1 = w_t'\widetilde{\eta}_1$. Then $\widetilde{\alpha}_1(s_k x_l)'\widetilde{\xi}_1 = \widetilde{\beta}_1(u_r w_t)'\widetilde{\eta}_1$ yields $\widetilde{\alpha}_1 = \widetilde{\beta}_1$. Now

$$a = p_2(\alpha) = p_2(\widetilde{\alpha}_1 s_k'\delta^{-1}) = p_2(\widetilde{\alpha}_1)p_2(\delta^{-1}) \quad \text{and}$$
$$b = p_2(\beta) = p_2(\widetilde{\beta}_1 u_r'\theta^{-1}) = p_2(\widetilde{\beta}_1)p_2(\theta^{-1}).$$

Thus $a = cu$ and $b = cv$, where u and v are invertible, and so $a = b(v^{-1}u)$. □

Corollary 4.3. *If a monoid S admits a comultiplication m and has the inverse property, then $S * S$ and E_S are equidivisible.*

Proof. First note that m induces a comultiplication on $S * S$ given by

$$S * S \xrightarrow{m*m} S * S * S * S \xrightarrow{id*T*id} S * S * S * S,$$

where $T : S * S \to S * S$ interchanges the two factors. By 3.3, $S * S$ has the inverse property. By 4.2, $S * S$ is equidivisible.

Now suppose $\alpha\xi = \beta\eta$ in E_S. Since $E_S \subseteq S * S$ and $S * S$ is equidivisible, there exists $\gamma \in S * S$ such that $\alpha = \beta\gamma$ or there exists a $\delta \in S * S$ such that $\beta = \alpha\delta$. In the former case, $p_1(\beta)p_1(\gamma) = p_1(\alpha) = p_2(\alpha) = p_2(\beta)p_2(\gamma)$. Since $p_1(\beta) = p_2(\beta)$ and S is cancellative, $p_1(\gamma) = p_2(\gamma)$. Thus $\gamma \in E_S$. The other case is similar. Equidivisibility for E_S now follows by 3.4. □

The following proposition will be generalized in §6.

Proposition 4.4. *Let S be a monoid. Then the following are equivalent:*

(1) *S admits a comultiplication, S has the inverse property and the group of invertible elements $U_S = 1$.*

(2) *S is a free monoid.*

In this case, any comultiplication of S is associative.

Proof. We first show (1) implies (2). If $x \neq 1$ and we can write $x = uv$ for $u \neq 1$ and $v \neq 1$, then u is called a **left factor** of x. By [7, Cor. 5.1.7], it suffices to show that every non-trivial $x \in S$ has finitely many left factors. Suppose u is a left factor of x. Then $\xi = m(x) = m(u)m(v)$. There can be no cancellation between the last factor of $m(u)$ and the first factor of $m(v)$ because S has the inverse property and $U_S = 1$. Thus $m(u)m(v)$ is in reduced form. If we write $\xi = \prod_{i=1}^{p} x_i' y_i''$, then for some l, $0 \leq l < p$,

$$m(u) = \left(\prod_{i=1}^{l} x_i' y_i''\right) x_{l+1}' r'' \quad \text{or} \quad m(u) = \left(\prod_{i=1}^{l} x_i' y_i''\right) s',$$

where $r = 1$ or is a left factor of y_{l+1} and where $s = 1$ or is a left factor of x_{l+1}. In the first case $u = p_1 m(u) = \prod_{i=1}^{l+1} x_i$ and in the second case $u = p_2 m(u) = \prod_{i=1}^{l} y_i$. Thus every left factor u of x has the form $u = \prod_{i=1}^{l+1} x_i$ or $u = \prod_{i=1}^{l} y_i$. Since there are only finitely many of these, x has finitely many left factors. This proves (2).

For (2) implies (1) it is clear that if S is free, then S has the inverse property and $U_S = 1$. If $Y \subseteq S$ is a basis, then a comultiplication of S is defined by $m(y) = y'y''$ for $y \in Y$. This proves (1).

If S is a free monoid with basis Y, then $m(y) = s_1' t_1'' \cdots s_n' t_n''$ for each $y \in Y$. Hence $s_1 \cdots s_n = t_1 \cdots t_n = y$, and this implies some $s_i = y$, some $t_j = y$ and all other factors are trivial. Therefore $m(y) = y'y''$ or $m(y) = y''y'$, and so m is associative. $\square$

5. SEMIFREE MONOIDS

In this section we study comultiplications on certain monoids (called semi-free). We shall see in §6 that a large class of monoids with comultiplication (namely those with the inverse property) are semi-free. We begin with some preliminaries.

We recall from [2] some basic facts about comultiplications on groups. Let F be a group with comultiplication n. We know that E_F is a free group with basis $\xi_a = a'a''$, for all $a \neq 1$ in F, and so F is a free group [5]. If X is a basis for F, then for every $x \in X$, $n(x)$ can be expressed as a reduced word in finitely many of the generators $\xi_{\delta_i(x)}$, where $\delta_i(x) \in F$, and $i = 1, \ldots, k$. (We have in fact given an algorithm in [2] for finding the $\delta_i(x)$.) Then the set $\Delta_n = \{\delta_i(x) \mid x \in X\}$ is the **quasi-diagonal set** of n and is essential to our study of comultiplications on groups in [2]. For example, if $D_n = \{d \mid d \in F,\, d \neq 1,\, n(d) = d'd''\}$ is the **diagonal set** of n, then $D_n \subseteq \Delta_n$, and n is associative if and only if $D_n = \Delta_n$.

We next consider analogues of these sets for monoids. Let S be a monoid with comultiplication m. We define the **diagonal set** D_m and **antidiagonal set** D_m^* of m by

$$D_m = \{d \mid d \in S,\, d \neq 1,\, m(d) = d'd''\} \quad \text{and}$$

$$D_m^* = \{d \mid d \in S,\, d \text{ not a unit},\, m(d) = d''d'\}.$$

Recall from §2 that we can associate to S the free group $\overline{S}$ in S and a natural homomorphism $\nu : S \to \overline{S}$. Then m induces a comultiplication $\overline{m} : \overline{S} \to \overline{S} * \overline{S}$ such that $\overline{m}\nu = (\nu * \nu)m$.

Definition 5.1. A monoid S is **semifree** if $S = U * M$, where U is a free group and M is a free monoid.

Hence if S is semifree, the group of invertible elements $U_S = U$ and M has a canonical basis Y (§2). If X is any basis of U, we say that (X, Y) is a **basis** for S. The cardinality of $X \cup Y$ is called the **rank** of S. Clearly $\overline{S} = U * \overline{M}$, and $\overline{M}$ is the free group with basis Y. If m is a comultiplication on S and $\overline{m}$ is the induced comultiplication on $\overline{S}$, then $\overline{m}|_U = m|_U : U \to U * U$. Moreover, for each $y \in Y$, $m(y) = \prod s_i' t_i'' \in S * S$ which we assume is reduced. Since $\prod s_i = \prod t_i = y$, it follows that for precisely one index j (resp., k) $s_j = u_j y v_j$ and $u_j, v_j, s_i \in U$ for all $i \neq j$ (resp., $t_k = w_k y z_k$ and $w_k, z_k, t_i \in U$ for all $i \neq k$). Moreover, $s_1 \cdots s_{j-1} u_j = v_j s_{j+1} \cdots s_n = 1$ and similar equations hold for the t_i, w_k, z_k. Now we proceed to compute the quasi-diagonal set $\Delta_{\overline{m}}$ of $\overline{m}$. Clearly $\Delta_{\overline{m}} = \Delta_{m|U} \cup \Delta$, where $\Delta = \{\delta_i(y) \mid y \in Y\}$. By the above remarks, if $j \leq k$ and $y \in Y$, then $\delta_i(y) \in U$ for all $i \notin [2j-1, 2k-1]$ and $\delta_i(y)$ is of the form $u_i y v_i$ for all $i \in [2j-1, 2k-1]$, where $u_i, v_i \in U$. If $k \leq j$ and $y \in Y$, then $\delta_i(y) \in U$ for all $i \notin [2k-1, 2j-1]$ and $\delta_i(y) = u_i y^{-1} v_i$ for all $i \in [2k-1, 2j-1]$, where $u_i, v_i \in U$.

Thus the expressions for the $\delta_i(y) \in \Delta$ which are not in U are all of the form uyv or all of the form $uy^{-1}v$, where $u, v \in U$. If $\delta \in \Delta_{\overline{m}}$ lies in S we say that δ is a **quasidiagonal** element of m and denote the set of quasidiagonal elements by Δ_m. If $\delta^{-1} \in \Delta \cap S$ and δ is not a unit, then we say that δ^{-1} is a **quasi-antidiagonal** element of m and denote the set of such elements by Δ_m^*. Thus Δ_m is the union of $\Delta_{m|U}$, the units in Δ and all elements of the form uyv in Δ, and Δ_m^* consists of all elements of the form $v^{-1} y u^{-1}$, where $uy^{-1}v \in \Delta$. Clearly $D_m \subseteq \Delta_m$ and $D_m^* \subseteq \Delta_m^*$.

We illustrate all of this with a concrete example. For ease of notation we write $\overline{s}$ for the inverse of a group element s and ξ_a for $a'a'' \in E_S$. We use the algorithm of [2] to express an element of E_S as a word in the ξ_a's.

Example 5.2. Let S be a semifree monoid of rank 4 with basis $X \cup Y$, where $X = \{x_1, x_2\}$ and $Y = \{y_1, y_2\}$, and define a comultiplication m by

$$\begin{aligned} m(x_1) &= x_1' x_1'' = \xi_{x_1}, \\ m(x_2) &= x_2' x_2'' \overline{x}_2' \overline{x}_1'' x_2' x_1'' = \xi_{x_2} \xi_{\overline{x}_2} \overline{\xi}_{x_1 \overline{x}_2} \xi_{x_1}, \\ m(y_1) &= \overline{x}_1'' \overline{x}_2' x_1'' x_2' \overline{x}_2'' \overline{x}_2' x_2'' y_1'' x_1'' x_2' y_1' x_1' \overline{x}_1'' \overline{x}_1' = \overline{\xi}_{x_1} \xi_{x_1 \overline{x}_2} \overline{\xi}_{\overline{x}_2} \overline{\xi}_{x_2} \overline{\xi}_{\overline{x}_1 \overline{y}_1 \overline{x}_2} \overline{\xi}_{x_1}, \\ m(y_2) &= x_1' x_2' y_2'' \overline{x}_2' \overline{x}_1' y_2' = \xi_{x_1 x_2} \overline{\xi}_{\overline{y}_2 x_1 x_2}. \end{aligned}$$

Note that the comultiplication $m|_U$ is Example 3.7(2) of [2]. Then we have

$$\Delta_{\overline{m}} = \{x_1,\, x_2,\, \overline{x}_2,\, x_1\overline{x}_2,\, \overline{x}_1\overline{y}_1\overline{x}_2,\, x_1x_2,\, \overline{y}_2x_1x_2\} \quad \text{and} \quad D_{\overline{m}} = \{x_1,\, \overline{x}_1\overline{y}_1\overline{x}_2\},$$

$$\text{and so} \quad \Delta_m = \{x_1,\, x_2,\, \overline{x}_2,\, x_1\overline{x}_2,\, x_1x_2\}, \quad D_m = \{x_1\},$$

$$\Delta_m^* = \{x_2y_1x_1,\, \overline{x}_2\overline{x}_1y_2\} \quad \text{and} \quad D_m^* = \{x_2y_1x_1\}.$$

The following theorem is then proved analogously to [2, (3.6) and (4.5)].

Theorem 5.3. *If S is a finite rank semifree monoid with comultiplication m, then*

(1) *The set Δ_m is a finite set of generators of U_S and $\Delta_m \cup \Delta_m^*$ is a finite set of generators of S.*

(2) *The comultiplication m is associative if and only if $\Delta_m = D_m$ and $\Delta_m^* = D_m^*$.*

6. THE MAIN THEOREM

In this section we prove the main result of the paper (Theorem 6.3). If a and b are elements of a monoid S, then a and b are said to be **associate** if $a = bu$ for some $u \in U_S$. Clearly this is an equivalence relation on S. We denote by $\langle a \rangle$ the equivalence class of $a \in S$.

Definition 6.1. *Let S be a monoid and $a \in S$. If the set $\{\langle u \rangle \mid u \text{ a left factor of } a\}$ is finite, then a is called* **finitely decomposable**. *If $\{\langle u \rangle \mid u \text{ a left factor of } a\}$ has one element, then a is called* **indecomposable**.

The following is a generalization of [4, Thm. 9.6].

Lemma 6.2. *A monoid S is semi-free if and only if*

(1) *S is cancellative,*
(2) *U_S is a free group,*
(3) *S is equidivisible and*
(4) *each element of S is finitely decomposable.*

Proof. These are clearly necessary conditions. To show sufficiency, let Y be the set of non-units of S which are indecomposable. As in [4, Thm. 9.6], Y generates a free monoid M with $U_M = 1$ and $U_S \cap M = 1$. We show now that U_S and Y generate S. If a is indecomposable, then either $a \in U_S$ or $a \in Y$. If not, $a = a_1 a_2$, where a_2 is not a unit. If a_1 and a_2 are indecomposable, then we are done. Otherwise we continue this process and obtain for each n a product $a = a_1 \cdots a_n$ with $a_1 \cdots a_i$ not associate to $a_1 \cdots a_{i+1}$. We claim that $\langle a_1 \rangle, \langle a_1 a_2 \rangle, \ldots, \langle a_1 \cdots a_n \rangle$ are distinct classes. For if $a_1 \cdots a_i$ is equivalent to $a_1 \cdots a_j$, $j > i$, then by cancellation, $a_{i+1} \cdots a_j$ is a unit. Thus $a_{i+1}, \ldots, a_j$ are units. This contradicts our previous assumption. Thus for any n, we obtain n distinct equivalence classes of left factors of a. This contradicts (4).

Finally, to show that each element of S can be uniquely represented in terms of U_S and Y, see [4, Thm. 9.6]. □

We now prove our main theorem. The result is in the spirit of Kan's work on groups with a comultiplication [6]. Its prototype is the result of Bergman-Hausknecht [3, Thm. 20.16] which classifies all monoids which admit an associative comultiplication. For such monoids, Theorem 6.3 follows from [3, Thm. 20.16].

Theorem 6.3. *If S is a monoid with the inverse property, then S admits a comultiplication if and only if S is semi-free.*

Proof. Clearly if S is semi-free, S admits a comultiplication (see §5). Now suppose that S admits a comultiplication m. Then by Theorem 3.5, S is cancellative and by Theorem 4.5, S is equidivisible. Also m induces a comultiplication on U_S, and so U_S is a free group [6]. Thus it suffices to show that S has property (4) of Lemma 6.2. We do this in a similar way to the proof of Proposition 4.4. Suppose $x \in S$ and u is a left factor of x. Then $x = uv$ for some $v \in S$, where $u \neq 1$ and $v \neq 1$, and so $m(x) = m(u)m(v)$. Suppose $\xi = m(x) = x_1' y_1'' \cdots x_p' y_p''$ is reduced. By Lemma 3.1, $m(u) = \alpha\delta$ and $m(v) = \delta^{-1}\beta$, where $\xi = \alpha\beta$, for $\alpha, \beta, \delta \in S * S$. Thus $u = p_i m(u)$ is a product of the form $\left(\prod_1^l x_j\right) d$ or $\left(\prod_1^l y_j\right) e$, where $d, e \in U_S$ is the image of p_1 or p_2 of δ and $1 \leq l \leq p$.

Thus there are only finitely many equivalence classes of left factors of x. This completes the proof. □

We conclude with two corollaries of Theorem 6.3.

Corollary 6.4. *If S is a cancellative and equidivisible monoid, then E_S is semi-free.*

Corollary 6.5. *If S is a commutative monoid with comultiplication, then $S \approx \mathbb{N}^0$, the free monoid on one generator, or $S \approx \mathbb{Z}$, the free group on one generator.*

Note that there are exactly two comultiplications on $\mathbb{N}^0$ (see the proof of Proposition 4.4) and that the comultiplications on $\mathbb{Z}$ have been classified in [2, Lem. 6.9].

ACKNOWLEDGEMENT. We would like to thank J. M. Howie and G. Lallement for valuable clarifications. Part of this work was done while the second-named author was a visiting scholar at Dartmouth College.

REFERENCES

1. M. Arkowitz, *Comultiplications in algebra and topology*, Rend. del Sem. Mat. e Fisico di Milano (to appear).
2. M. Arkowitz and M. Gutierrez, *Comultiplications on free groups and wedges of circles*, Trans. Amer. Math. Soc. (to appear).
3. G. Bergman and A. Hausknecht, *Co-groups and Co-rings in Categories of Associative Rings*, Mem. Amer. Math. Soc., 1996.
4. A.H. Clifford and G.B. Preston, *The Algebraic Theory of Semigroups*, vol. I and II, Amer. Math. Soc., 1967.
5. B. Eckmann and P. Hilton, *Structure maps in group theory*, Fund. Math. **50** (1961), 207–221.
6. D. Kan, *Monoids and their duals*, Bol. Soc. Math. Mex. **3** (1958), 52–61.
7. G. Lallement, *Semigroups and Combinatorial Applications*, Wiley, 1979.